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

№ 4 (квітень)

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. – №4 (квітень) . – 66 с.

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

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

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

© Науково-дослідний інститут інформатики і права Національної академії правових наук України,
© Національна бібліотека України імені В.І. Вернадського, 2019

ЗМІСТ

«…До заходу [всеукраїнська науково-практична конференція «Безпека соціально-економічних процесів у кіберпросторі] долучилися майже тисяча учасників. Серед них – практикуючі спеціалісти Департаменту кіберполіції, студенти та представники кафедр з кібербезпеки 24 вищих навчальних закладів України, а також представники найбільших приватних організацій, які спеціалізуються на кібербезпеці…

Зокрема, у рамках конференції начальник Департаменту кіберполіції Сергій Демедюк та ректор Київського національного торговельно-економічного університету Анатолій Мазаракі підписали меморандум про взаємодію.

Відтак, Департамент кіберполіції надаватиме практичний досвід та можливість студентам вишу щотижнево отримувати навички з кібербезпеки на базі Департаменту кіберполіції.

Вже сьогодні на базі університету створено кіберлабораторію, за допомогою якої спеціалісти зможуть детально вивчати шкідливе програмне забезпечення за допомогою найсучаснішого обладнання. Також, в університеті створено сучасну Smart-бібліотеку. Їх презентація відбулася сьогодні у рамках проведення конференції.

Крім того, сьогодні було проведено ряд науково-практичних дискусійних панелей на тему боротьби з кіберзлочинністю, кіберзахисту на підприємствах та щодо основних напрямків забезпечення кібербезпеки в Україні.» ***(Ми повинні навчати наших дітей та молодь основам кібербезпеки. Сьогодні для нас це ключове завдання — Сергій Демедюк // Деловой Славянск (https://slavdelo.dn.ua/2019/04/03/mi-povinni-navchati-nashih-ditej-ta-molod-osnovam-kiberbezpeki-sogodni-dlya-nas-tse-klyuchove-zavdannya-sergij-demedyuk/). 03.04.2019).***

***

Кібервійна проти України

«Україна зараз знаходиться в епіцентрі війн різних видів. Росія здійснює гібридну війну, не тільки проводить бойові дії на сході України, а й намагається впливати на нашу державу в економічній, інформаційній галузях і сфері кібербезпеки.

Про те, як наша країна протистоїть російським хакерам, і як РФ намагається відпрацювати на нашій державі методи, які збирається використовувати в інших країнах, …розповіла голова ГО “Рада інформаційної безпеки і кібернетичного захисту України” Еліна Шнурко-Табакова…

Є два великих пласта кібернетичних небезпек: перша і найбільш відома – хакери, друга – інформаційно-психологічний вплив на населення. Останньому, за словами гості студії, наші співгромадяни ще не можуть твердо протистояти. Але відбити атаку хакерів українські фахівці готові в будь-який момент.

“З точки зору можливості зламу різних систем і заміни якихось результатів, наприклад, під час виборів, ситуація досить спокійна. Ми мобілізували всіх, кого могли, фахівці на сторожі. Вони моніторять простір і знають свої уразливі сторони. Але, з моєї точки зору, агресорові зараз немає сенсу здійснювати пряме втручання, тому що він домігся набагато більше на рівні інформаційно-психологічного впливу, який також можна віднести до кібернебезпек”, – зазначила голова ГО” Рада інформаційної безпеки і кібернетичного захисту України”.

Вона заявила, що всі види війн завжди присутні в комбінаціях. “Наприклад, коли відбувається конфлікт, миттєво починають працювати хакери, намагаючись порушити наші ресурси, що стосуються, наприклад, Збройних сил України. Після цього додається вплив в інформаційній сфері”, – розповіла Еліна Шнурко-Табакова.

За її словами, вже п’ять років Росія намагається відпрацювати на прикладі України той інструментарій, який згодом використовує для кібернетичних атак в інших державах світу, наприклад, в ситуації з Brexit.

“Країна-агресор моніторить всі негативи, які зараз існують в нашому суспільстві, потім обробляє їх і вносить знову в інформаційний простір в зміненому вигляді. В результаті наші люди стають до них сприйнятливі”, – пояснила експерт.

Еліна Шнурко-Табакова зазначила, що головним інструментом для протистояння діям РФ є навчання населення медіаграмотності…» ***(Альона Воробйова. Українські кіберспеціалісти готові відбивати будь-які атаки РФ, – Еліна Шнурко-Табакова // UA\|TV (https://uatv.ua/ukrayinski-kiberspetsialisty-gotovi-vidbyvaty-bud-yaki-ataky-rf-elina-shnurko-tabakova/). 11.04.2019).***

***

«Кіберполіція не зафіксувала жодної кібератаки на системи Центральної виборчої комісії під час проведення другого туру президентських виборів в Україні.

Відстежували ситуацію в цілодобовому режимі, повідомили у кіберполіції.

Там нагадали, що під час першого туру виборів зафіксували кілька спроб сканування систем ЦВК задля виявлення вразливостей. Сканування здійснювали з IP-адрес, розташованих в Росії і в Києві…» ***(Кіберполіція не зафіксувала жодної кібератаки на ЦВК під час другого туру виборів // iPress (https://ipress.ua/news/kiberpolitsiya_ne_zafiksuvala_zhodnoi_kiberataky_na_tsvk_pid_chas_drugogo_turu_vyboriv_288838.html). 24.04.2019).***

***

«У ніч підрахунку голосів системи Центральної виборчої комісії зазнали атаки з боку російських хакерів, повідомив міністр внутрішніх справ Арсен Аваков…

"Ми дали нашим сусідам не так багато можливостей з технічного боку втручатися у виборчий процес. Разом з тим, в ніч підрахунку голосів ми фіксували спроби втручання в нашу систему через кіберзагрози. Це були не масові атаки. Вони розвідували можливості наших систем", - сказав Аваков.» ***(У ніч підрахунку голосів хакери РФ намагались атакувати системи ЦВК, - МВС // ТОВ***

«УКРАЇНСЬКА ПРЕС-ГРУПА» (http://day.kyiv.ua/uk/news/110419-u-nich-pidrahunku-golosiv-hakery-rf-namagalys-atakuvaty-systemy-cvk-mvs). 11.04.2019).

***

«Програмне забезпечення, розроблене в Росії, може містити шкідливі вірусні програми та інструменти для прихованого доступу до інформації, що продемонстрували численні кібернетичні атаки на Україну та її державні установи.

Таке переконання сьогодні у Брюсселі в ході дискусії під назвою "Досвід України у кібернетичній безпеці: захищаючи демократію" висловив експерт київської громадської організації "Міжнародна академія інформації" Анатолій Марущак, доктор юридичних наук, професор, лауреат Державної премії України в галузі науки і техніки 2012 року, повідомляє кореспондент Укрінформу.

"У контексті гібридних засобів ведення війни Росія використовує шкідливе програмне забезпечення, а також соціальну інженерію та приховані засоби дистанційного доступу до інформації, які закладаються у програмне забезпечення російського виробництва. Наприклад, антивірус "Dr.Web" не розпізнає шкідливий "софт", розроблений розвідувальними службами Російської Федерації. Більш того, як ви знаєте, Лабораторія Касперського була прямо звинувачена компетентними правоохоронними органами Сполучених Штатів у причетності до витоку чутливої інформації", — сказав Марущак…

Він зауважив, що після того, як російські спецслужби переконалися у низькій ефективності інформаційних впливів на населення України, вони приступили до здійснення кібернетичних атак на технологічну, економічну та адміністративну інфраструктури в Україні. Перша з найпотужніших атак відбулася у 2014 році під час позачергових президентських виборів в Україні з метою дискредитації їх результату. У 2015 році кібератака агресора була спрямована проти енергетичних компаній у центральних та західних регіонах України, а у 2016 році кібернетичним загрозам довелося протистояти українським фінансовим установам та транспортним компаніям…» ***(Експерт: російський "софт" може містити приховані програми-шпигуни // Goodnews.ua (http://goodnews.ua/technologies/ekspert-rosijskij-soft-mozhe-mistiti-prixovani-programi-shpiguni/). 10.04.2019).***

***

«…Поступили комментарии главы миссии наблюдателей Европарламента по поводу проведения президентских выборов в Украине. Ситуацию озвучила Ребекка Хармс.

Наблюдатели со стороны Европарламента проверяют ход выборов в Украине. Выясняется, в частности, уровень влияния России. По заявлению Хармс, он сводится к минимуму.

По словам наблюдателей, влияние России сводится к публикациям на соответствующую тематику в ведущих СМИ. Украина была подготовлена к кибератакам. По словам Хармс, Украиной применяются не все инструменты оцифровки, в сравнении с другими странами. Есть опасность взлома

компьютеров…» ***(Европарламент не нашел доказательств российского вмешательства в выборы // AOinform (https://www.aoinform.com/news/evroparlament_ne_nashel_dokazatelstv_rossijskogo_vmeshatelstva_v_vybory/2019-04-22-29334). 22.04.2019).***

***

«Министр внутренних дел Арсен Аваков заявляет, что полиция обезвредила 2 террористические группы и остановила кибератаки России во время выборов Президента.

Об этом говорится в сообщении пресс-службы МВД.

"Мы рассчитывали на такую ситуацию, учитывая весь гибридный арсенал РФ, который она использует для дискредитации выборов. Обезвредили две террористические группы, которые имели связь с РФ. Наша киберполиция провела хорошую работу, поэтому противник не имеет доступа к нашей системе и прекратил атаки", - заявил министр.

По его словам, во время выборов и в предыдущие 2 дня наблюдается рекордное количество недостоверных сообщений о минировании крупных государственных объектов и атаки на украинские системы с VPN-адресами якобы в США, Гонконге и Китае, которые на самом деле поступали из РФ…» ***(Во время выборов обезвредили 2 террористические группы – Аваков // АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/299438-vo_vremja_vyborov_obezvredili_2_terroristicheskie_gruppy_-_avakov). 22.04.2019).***

***

Боротьба з кіберзлочинністю в Україні

«Полицейские вышли на след злоумышленников, которым удалось с помощью вмешательства в работу компьютера бухгалтера одной из украинских компаний вывести больше 3,3 миллионов гривен налогового кредита…

Как стало известно, в производстве следственного отдела Староконстантиновского ОП ГУНП в Хмельницкой области находится уголовное производство от 14 февраля 2017 года по факту совершения уголовного правонарушения, предусмотренного ч.1 ст.361 (несанкционированное вмешательство в работу автоматизированных систем), ч.3 ст.191 (присвоение, растрата имущества или завладение им путем злоупотребления служебным положением) и ч.1 ст.366 Уголовного кодекса Украины (служебный подлог).

В ходе досудебного расследования и проведения оперативно-розыскных мероприятий установлено, что с помощью компьютерной программы «Anyplace Control», позволяющей удаленно работать с компьютером, и предварительно установленной на ПК для ведения бухгалтерского учета ООО «Старокостянтинивцукор» (при неизвестных органом досудебного расследования обстоятельствах), с помощью электронной подписи в программном обеспечении

«M.E.Doc», в режиме реального времени через Интернет было проведено несанкционированное вмешательство в работу автоматизированной системы регистрации налоговых накладных в Едином государственном реестре налоговых накладных.

Злоумышленники от имени ООО «Старокостянтинивцукор» за 12 минут 10 февраля 2017 года зарегистрировали восемь налоговых накладных о предоставлении строительно-монтажных работ ООО «Легал Фин групп» на общую сумму 20 миллионов гривен, в результате чего произошло уменьшение регистрационного лимита НДС в ООО «Старокостянтинивцукор» на общую сумму 3 миллиона 333 тысячи 333 гривны 33 копейки.

– При этом во время вмешательства в программное обеспечение использовался российский IP-адрес 188.64.171.181 (Москва, Россия), провайдера ООО «H1», – говорится в материалах дела.

Следствие также установило цепочку, по которой накопленный налоговый кредит выводился на три юридических лица. По версии правоохранителей, деньги ушли на ООО «Апт-Украина» – порядка 2 миллионов 516 тысяч гривен, ООО «Евро Инвест плюс» – 560,7 тыс грн, ООО «Спецтрансбуд-1» – 272,6 тыс.

Полицейские также вышли на мужчину, который, возможно, причастен к регистрации некоторых компаний из схемы выведения денег и был основателем и руководителем одной из фигурирующих в деле фирм – ООО «Шеваль гранд». Именно от этой фирмы, спустя минуту после оформления налоговых накладных от ООО «Старокостянтинивцукор», было зарегистрировано налоговые накладные на сумму 20 миллионов гривен о предоставлении ООО "Билгороденерго" (ещё один предполагаемый участник схемы).

21 сентября прошлого года полицейские провели обыск в квартире основателя и руководителя (на момент проведения схемы) ООО «Шеваль гранд». Последним из имеющихся в судебном реестре решений по этому делу суд удовлетворил ходатайство следствие о доступе к информации о движении средств по счету мужчины в «ОТП Банк». Решение действует до 18 апреля.» ***(Владимир Кондрашов. Хакеры"тихо" украли у украинского предприятия более трех миллионов гривен // Internetua (http://internetua.com/hakery-tiho-ukrali-u-ukrainskogo-predpriyatiya-bolee-treh-millionov-griven-1). 11.04.2019).***

***

«Два года ограничения свободы с испытательным сроком в один год получил бывший инженер компьютерных систем одного из украинских охранных предприятий. Мужчина, чтобы вернуть себе работу, организовал серию DDoS-атак на ресурсы своих бывших работодателей.

…обвиняемый с октября 2016 по март 2018 года работал в ООО «Днепровская охранная компания «Профессиональная защита» в должности инженера компьютерных систем и на основании договора постоянно находился на ООО «Вневедомственная охрана» в Запорожье. 5 марта прошлого года его уволили. Однако после увольнения из указанного предприятия, «желая вернуться на прежнюю работу и продемонстрировать руководству «Днепровской охранной компании «Профессиональная защита» необходимость его возвращения на пост»,

мужчина, используя уязвимость ограничения настроек маршрутизаторов, решил заблокировать работу предприятия ООО «Вневедомственная охрана»путем осуществления DDoS-атаки, зная, что прекращение действия атаки требует перенастройки оборудования абонентов и предприятия, которое потребует много времени.

– Реализуя свой преступный умысел, обвиняемый загрузил и скопировал на жесткий диск своего ноутбука из всемирной сети Интернет программное обеспечение, необходимое для организации и проведения DDoS-атак под названием «LOIC», что дало ему возможность осуществлять DDoS-атаки на избранные им серверы и IP- адреса, – говорится в приговоре. – Также он установил на свой мобильный телефон приложение «DDOS», которое может выполнять распределенную атаку вида «отказ в обслуживании» (ddos-атака), путем постоянных передач на нужные сайты или IP-адреса, и приложение «Ping», которое также может отправлять постоянные запросы на нужные IP-адреса.

Всего следствию удалось доказать 8 эпизодов DDoS-атак на мощности ООО «Вневедомственная охрана». Благодаря атакам в апреле и мае 2018 года была нарушена и временно прекращена работа охранной компании, что «делало невозможным мониторинг и не позволяло управлять удаленным оборудованием абонентов предприятия (обработка информации от оборудования абонентов не давала результатов вообще, или давала только часть тех результатов, которые можно было получить до вмешательства)».

В судебном заседании обвиняемый свою вину по всем эпизодам признал полностью. Вместе с обвинительным актом в суд поступило соглашение о примирении, заключенное между представителем потерпевшего ООО «Вневедомственная охрана» и подозреваемым, согласно которому стороны договорились о формулировки обвинения и его правовой квалификации по ч. 1 ст. 363-1 УК Украины.

Также были согласованы все существенные для данного уголовного производства обстоятельства, согласованно наказание в виде ограничения свободы сроком на 2 года с освобождением от отбывания наказания с испытанием, и с испытательным сроком в 1 год.

Суд соглашение утвердил.» ***(Владимир Кондрашов. Инженер организовал серию DDoS-атак, чтобы вернуть себе работу, но получил срок // Internetua (https://internetua.com/inzgener-organizoval-seriua-ddos-atak-cstoby-vernut-sebe-rabotu-no-poluchil-srok). 10.04.2019).***

***

«До двух лет лишения свободы грозит украинцу, которого подозревают в создании и распространении вредоносного программного обеспечения, взломе компьютеров и администрировании сайта по продаже логов…

16 марта полиция открыла уголовное дело по признакам уголовного преступления, предусмотренного ч.1 ст.361-1 УК Украины (Создание с целью использования, распространения или сбыта вредных программных или технических средств, а также их распространение или сбыт).

Досудебным расследованием установлена информацию в отношении лица, известного на «хакерском» форуме «bhf.io» под никнеймами «kr3wka», «naf4nya» и «Nafanya». Пользователь, по версии следствия, осуществляет распространение вредоносного программного обеспечения и непосредственно занимается несанкционированным вмешательством в работу электронно-вычислительных машин (компьютеров). В результате аналитически-розыскных мероприятий работниками отдела противодействия киберпреступности в Запорожской области удалось даенонимизировать хакера. Им оказался житель Запорожья, который зарегистрирован в социальной сети «Вконтакте» под именем «Олег Хаджийский».

Также было установлено, что данный гражданин является администратором веб-ресурса «stealacc.store», с помощью которого осуществляется продажа логов (конфиденциальная информация пользователей всемирной сети Интернет по электронным платежным системам, пароли от почтовых ящиков, ключи от электронных кошельков криптовалют и прочее), которые были получены им в результате использования вредоносного программного обеспечения.

Кроме этого установлено, что для получения денежных средств за продажу вредоносного программного обеспечения мужчина использует собственную банковскую карточку Приватбанка. Следствие уже получило разрешение на доступ к сведениям о движении денежных средств на счет.» ***(Владимир Кондрашов. Полиция вышла на след хакера известного как "Nafanya" // Internetua (https://internetua.com/policiya-vyshla-na-sled-hakera-izvestnogo-kak-nafanya). 09.04.2019).***

***

«Главное следственное управление Нацполиции Украины осуществляет досудебное расследование в уголовном производстве, открытом ещё в начале ноября 2017 года, по факту реализации группой лиц похищенных данных серверов. Более того, данная группа собиралась создать некую онлайн-платформу для продажи краденой информации…

Известно, что уголовное дело открыто «по факту реализации группой лиц похищенных данных серверов вследствие несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров), автоматизированных систем и компьютерных сетей, а также о приготовлении группой лиц к созданию онлайн-платформы для продажи похищенных с помощью специально разработанного программного обеспечения с ОС Windows прав доступа к украинским и иностранным серверам по результатам несанкционированного вмешательства в их работу»…

Дело открыто по признакам уголовного преступления, предусмотренного ч. 2 ст. 361 УК Украины – несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи, совершенные повторно или по предварительному сговору группой лиц, или если они причинили существенный вред. Следствие продолжается.» ***(Владимир Кондрашов. Полиция: продавцы похищенных персональных данных попались "на горячем" // Internetua***

(https://internetua.com/policiya-prodavcy-pohisxennyh-personalnyh-dannyh-popalis-na-goryacsem). 05.04.2019).

***

«Сотрудники Департамента киберполиции Национальной полиции Украины выявили группу лиц, специализирующуюся на создании вредоносного программного обеспечения, его распространении за денежные средства, несанкционированном вмешательстве в работу ЭВМ и автоматизированных систем финансовых организаций…

Полицейские установили, что участники преступной группы в период с июня по август 2018 года на территории города Черкассы снимали жилье, где организовали схему создания и сбыта вредоносных программ. В данный период злоумышленники, благодаря сотрудничеству с одним из бывших работников банковского учреждения, разработали основные составляющие части вредоносного программного обеспечения.

Вредоносное ПО, в создании и продаже которого и подозревают группу, состоит из трех исполняющих файлов: программы для сканирования кассет банкомата, программы выдачи денежных средств и программы генерации кодов для работы программы. Первые два файла (cm17F.exe, Stimulator22.exe) продавцы ПО пересылают до оплаты, а программу генерации кодов - после оплаты за «товар».

– По результатам изучения двух указанных файлов (cm17F.exe, Stimulator22.exe) установлено, что исследуемые файлы зашифрованы утилитой «VMProtect». В ходе анализа выявлено, что файл с названием «Stimulator22.exe» является генератором кода доступа. Файл «cm17F.exe» содержит логику и команды для работы с кассовым модулем банкоматов Wincor Nixdorf, – говорится в материалах дела. – Установлено, что логика работы программы «cm17F.exe» предназначена для несанкционированной выдачи наличных из банкомата, а поэтому оно может считаться вредоносным программным обеспечением…

Правоохранители установили не только адрес проживания продавца, IP-адрес и профили в социальных сетях, но и то, что помощь в шифровании файлов ему предоставляет пользователь различных хакерских форумов - «раздает данные из стиллера, продает данные аккаунтов граждан и тому подобное»…

Уголовное дело по признакам уголовного преступления, предусмотренного ч. 2 ст. 361 УК Украины, было открыто 31 января. Участникам группы грозит до шести лет лишения свободы.

Следствие продолжается.» ***(Владимир Кондрашов. Киберполиция вышла на след создателей ПО для взлома банкоматов // Internetua (https://internetua.com/kiberpoliciya-vyshla-na-sled-sozdatelei-po-dlya-vzloma-bankomatov). 04.04.2019).***

***

«Зловмисники самостійно створювали, а також купували та модифіковували шкідливе програмне забезпечення. Ці програмні засоби вони поширювали в мережі інтернет на спеціалізованих форумах та чатах бірж

криптовалют під виглядом ліцензійного програмного забезпечення. Насправді ж, користувачі завантажували на свій пристрій вірус. Зазвичай це були віруси типу «stealer» або «keylogger».

Працівники Подільського управління та Управління інформаційних технологій та програмування в західному регіоні Департаменту кіберполіції, спільно зі слідчими поліції Хмельниччини, за процесуального керівництва Шепетівської місцевої прокуратури, встановили причетність до цього правопорушення двох 28-ми річних мешканців Хмельниччини.

Робота цих вірусів була налаштована так, що на інфікованих комп'ютерах відбувався збір інформації, в тому числі і конфіденційної. Серед такої – паролі, логіни до різних ресурсів, інформація про гаманці криптовалют, файли з персональною інформацією тощо.

У подальшому зібрана інформація направлялась зловмисникам на спеціально налаштований сервер. Частина розповсюдженого шкідливого програмного забезпечення дозволяла їм віддалено керувати інфікованими пристроями на правах адміністратора, в тому числі спостерігати за жертвами та прослуховувати їх розмови.

Викрадена особиста інформація зазвичай використовувалась для подальших протиправних дій та частково продавалася на відповідних форумах. Сума збитків наразі встановлюється…

Триває досудове розслідування розпочате за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України…» ***(Кіберполіція викрила групу осіб у поширенні вірусів для викрадення конфіденційної інформації // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-grupu-osib-u-poshyrenni-virusiv-dlya-vykradennya-konfidenczijnoyi-informacziyi-8899/). 02.04.2019).***

***

«В интернете уже начали продавать базы данных клиентов ПриватБанка, а мошенники обзванивают его клиентов, выпрашивая номера банковских карт.

Тенденция опасна: личными данными могут воспользоваться не только маркетологи различных компаний для рассылки рекламы и обзвона, но и преступники.

В Сети появились объявления, где мошенники продают свежие данные о клиентах ПриватБанка. «Продам телефонную базу клиентов ПриватБанка», «Продам базы ВИП-клиентов ПриватБанка», — говорится в таких объявлениях. В них предлагают паспортные данные клиентов с пропиской, идентификационные коды, телефоны, данные об автомобилях. Цены стартуют от 900 гривен за несколько тысяч клиентов.

«Цена зависит от того, для чего вам нужна база. Если для рассылки рекламы, то достаточно телефонов и имен. Если хотите данные посерьезнее, адреса узнать или еще что-то, то это будет подороже», — рассказал один из продавцов.

Приватовская база — одна из крупнейших в стране. Тут собрано самое большое количество клиентов с их скриншотами паспортов, кодов, точными адресами и телефонами. Поэтому это очень лакомый кусок как для тех, кто занимается рекламой, так и для мошенников и воришек.

Уже сейчас мошенники активизировались — они обзванивают клиентов и предлагают перейти им в Ощадбанк, выманивая данные карточек… В самом ПриватБанке говорят, что причин для опасения нет.

«Все базы на месте — в данный момент взлом почти невозможен, после атаки в 2014 году были усилены меры безопасности. То же касается и Приват24 — за последнее время мы не фиксировали кибератак на систему», — заверил «Вести» пресс-секретарь ПриватБанка Олег Серга.

Эксперты говорят, что риск того, что какую-то информацию могут украсть, есть всегда. Причем речь идет не только о хакерских атаках (последней массированной DDOS-атаке Приват подвергся еще в 2014 году), но и о том, что данные могут сливать сотрудники финучреждения.

«Сейчас, учитывая ситуацию, многие из уволенных захотят взять с собой фрагменты баз для дальнейшего использования, в т. ч. и для продажи. Не исключено также, что мошенники и воры тоже купят такие базы и начнут обращать внимание на имущество, которым владеют люди, что они покупают. А затем начнут ходить по их домам», — сказал «Вестям» эксперт по безопасности Сергей Шабовта.

База ПриватБанка интересна не сколько платежными данными, а тем, что в ней можно проследить данные связей людей между собой. «В первую очередь она может быть интересна маркетологам — поскольку можно просмотреть, кто, где и как совершались покупки, куда отправлялись в отпуск. Страховщики могут посмотреть, чьими услугами пользовались, а также попытаться переманить клиентов к себе. Интересна информация о вас может быть и фискальным органам, так как ПриватБанк долгое время защищал от них операции клиентов, ссылаясь на банковскую тайну», — говорит «Вестям» начальник лаборатории компьютерной криминалистики CyberLab Сергей Прокопенко.» ***(В Сети начали продавать телефонные номера клиентов «Приватбанка» // Vse.Media (http://vse.media/v-seti-nachali-prodavat-telefonnye-nomera-klientov-privatbanka/). 20.04.2019).***

***

«…Власниця одного із найбільших інтернет-ресурсів з продажу брендового дитячого одягу звернулася до кіберполіції із повідомленням про злам її інтернет-магазину. Відтак, поліцейські розпочали кримінальне провадження за ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України.

Пізніше працівники Київського управління Департаменту кіберполіції встановили причетність до вчинення цього злочину мешканця Черкас. Чоловік, використовуючи вразливості сайту, несанкціоновано отримав доступ до клієнтської бази великого онлайн-магазину та вимагав гроші за не розголошення отриманої конфіденційної інформації. Серед такої – персональні дані клієнтів магазину, їх

логіни та паролі тощо. При цьому, зловмисник використовував надійні методи конспірації. Для прикладу, у якості розрахунку використовувалася криптовалюта, що ускладнює можливість ідентифікації правопорушника…» ***(Кіберполіція викрила чоловіка у зламі бази даних одного з найбільших українських онлайн магазинів дитячого одягу // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-cholovika-u-zlami-bazy-danyx-najbilshogo-ukrayinskogo-onlajn-magazynu-dytyachogo-odyagu-1935/). 19.04.2019).***

***

«Для отримання доступу молодик використовував декілька способів отримання даних, зокрема, і використання власноруч створених фішингових сайтів. Отриману інформацію – продавав замовникам. Наразі за даним фактом розпочато кримінальне провадження. Вирішується питання щодо оголошення підозри.

Працівники Київського управління Департаменту кіберполіції спільно зі слідчими поліції Києва, за процесуального керівництва прокурорів Київської міської прокуратури № 8, викрили у такій протиправній діяльності 24-річного киянина.

Кіберполіція встановила: молодик, на закритих хакерських форумах, пропонував хакерські послуги. Серед таких - організація отримання ідентифікаторів доступу до соціальних сторінок, електронних скриньок тощо. Зловмисник оцінював свої послуги в залежності від складності роботи.

Для цього чоловік створював фішингові сторінки зовні схожі на офіційні сторінки реєстрації у соціальних мережах. Посилання на цей ресурс надсилався жертві за допомогою електронної пошти із проханням підтвердити реєстрацію та ввести пароль. Після переходу за посиланням та введення реєстраційних даних, зловмисник отримував інформацію щодо логінів та паролів користувача. Ці дані він і передавав у подальшому замовникам.

Окрім того, на закритих форумах він продавав шкідливе програмне забезпечення типу «stealer». Основною задачею цього типу вірусів є викрадення інформації щодо логінів, паролів та карткових рахунків, які збережені у браузері…

Кримінальне провадження розпочато за ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) КК України…» ***(Кіберполіція викрила хакера, що «на замовлення» зламував акаунти у соціальних мережах // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-xakera-shho-na-zamovlennya-zlamuvav-akaunty-u-soczialnyx-merezhax-136/). 18.04.2019).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Міністр закордонних справ Канади Христя Фріланд вважає, що співпраця між Україною та Канадою у сфері кібербезпеки дозволяє обом

країнам перейняти провідний досвід протистояння сторонньому втручанню в демократичні процеси. "Високопоставлений американський чиновник нещодавно сказав мені, що Україна - це російська лабораторія для дослідження ворожого втручання, тому взаємодія з Україною дає США можливість зрозуміти, що відбувається, і як захистити власну країну. Канада вважає так само", - сказала Фріланд. Вона підкреслила, що співпраця Канади та України є "дійсно взаємовигідним, коли йдеться про захист наших демократій". "У нас є підстави турбуватися щодо ворожого втручання в нашу демократію. Це точно відбувається, і з наближенням виборів нам слід шукати способи протистояти цьому", - сказала міністр.» ***(У Канаді зробили гучну заяву щодо кібербезпеки України // 7dniv.info (http://7dniv.info/society/112329-u-kanad-zrobili-guchnu-zaiavu-schodo-kberbezpeki-ukraiini.html). 11.04.2019).***

***

«Віце-прем'єр-міністр з питань європейської та євроатлантичної інтеграції України Іванна Климпуш-Цинцадзе та Посол України в США Валерій Чалий провели у Вашингтоні (США) зустріч із заступником Державного секретаря США з питань міжнародної безпеки та контролю над озброєнням Андреа Томпсон…

Американська сторона наголосила на тому, що активно спостерігає за ситуацією з загрозами, які відчуває Україна в кіберпросторі, особливо у період виборів, та підтвердила важливість спільної протидії ним. «Кіберзагрози неможливо обмежити географічними кордонами, наслідки кібератаки відчувають в усьому світі, і ми готові співпрацювати разом, щоб запобігти їм», – заявила Андреа Томпсон…» ***(Американці допомагатимуть Україні у сфері кібербезпеки – заступник Держсекретаря США // Leopolis.news (http://leopolis.news/amerykantsi-dopomagatymut-ukrayini-u-sferi-kiberbezpeky-zastupnyk-derzhsekretarya-ssha/). 05.04.2019).***

***

Світові тенденції в галузі кібербезпеки

«…Международный союз электросвязи при ООН опубликовал предварительный отчет «Глобальный индекс по кибербезопасности» (Global Cybersecurity Index) об уровне кибербезопасности в мире. По данным отчета, Россия заняла 28 позицию в рейтинге стран с самым высоким уровнем кибербезопасности. В пятерку лидеров вошли Великобритания, США, Франция, Литва и Эстония.

В 2018 году число стран, имеющих законодательство, регламентирующее ответственность за киберпреступления, возросло с 79% (в 2017 году) до 91%. Также увеличилось число стран, обладающих Национальной стратегией в области защиты киберпространства (58%).

В сфере законодательства РФ заняла первую строчку среди стран СНГ, опередив Казахстан и Узбекистан. В общем рейтинге лидером по реализации норм

в сфере кибербезопасности, а также мер борьбы с киберпреступлениями и спамом оказалась Европа.

Исследование по определению индекса кибербезопасности проводится ежегодно. При составлении рейтинга принимаются во внимание пять основных критериев: законодательная база, технические и организационные мероприятия, деятельность на международной арене и создание потенциала для развития сферы.» ***(РФ оказалась в числе стран с самым высоким уровнем кибербезопасности // SecurityLab.ru (https://www.securitylab.ru/news/498648.php). 05.04.2019).***

***

«Інвесткомпанія Pamplona Capital Management на вимогу США продає свою частку в компанії Cofense Inc, що надає для великих американських корпорацій послуги в сфері кібербезпеки. Про це повідомляє газета The Wall Street Journal…

За інформацією видання, представників комітету з іноземних інвестицій США (CFIUS), які зажадали продати пакет акцій в Cofense, стурбувала інвестиційна активність російського бізнесмена Михайла Фрідмана - основного акціонера інвесткомпанії LetterOne Holdings - інвестора Pamplona Capital Management.

У той же час представник Фрідмана пояснив виданню, що вимога CFIUS пов`язано з рівнем іноземного капіталу в Pamplona Capital Management, але персональних претензій до Фрідману або LetterOne CFIUS не озвучив…» ***(WSJ: Фрідман на вимогу влади США продає частку в компанії з кібербезпеки // Finbalance (http://finbalance.com.ua/news/WSJ-Fridman-na-vimohu-vladi-SShA-proda-chastku-v-IT-kompani). 11.04.2019).***

***

«Чехія визнана найбільш безпечною з погляду готовності протистояти он-лайн-загрозам. А найуразливішим виявився Південний Судан.

У рейтингу національної кібербезпеки, який складає естонська Академія електронного управління, Чехія зайняла перше місце. Естонія, яка очолювала його минулого року, спустилася на один рядок. На третьому місці — Іспанія.

Рейтинг оцінює країни зв 46 параметрами, зокрема це якість законодавства в галузі кібербезпеки, існування компаній або державних органів, які займаються питаннями кібербезпеки, ефективність взаємодії бізнесу й держави в цій сфері.

Поточного року розглядалося 129 країн. Україна — на 26-му місці, що на 3 позиції гірше, ніж минулого року. Прикметно, що, наприклад, США опинилися лише на 29-му місці, а Росія — на 23-му.» ***(Загрози он-лайн // Закон і Бізнес (https://zib.com.ua/ua/137195-yaki_kraini_gotovi_do_vidvernennya_kiberzagroz__reyting.html). 10.04.2019).***

***

«Большинство блокчейн-компаний слабо заботятся о своей кибербезопасности. Об этом свидетельствуют результаты исследования Всемирного экономического форума (ВЭФ).

Выяснилось, что большинство взломов, происходящих в сфере блокчейна и криптовалют, связаны не с великолепными навыками хакеров, а с недостаточным уровнем компьютерной безопасности.

Также аналитики отметили, что в развитии безопасности блокчейн-компаний важную роль играет лидерство. Если кибербезопасность станет одним из основополагающих принципов создания компаний, то это приведет к значительному снижению количества взломов.

Исследователи подчеркивают, что лишь в 5% компаний есть должность руководителя отдела компьютерной безопасности. Представители ВЭФ рекомендуют основателям блокчейн-стартапов создать такую должность и наделить главу по кибербезопасности необходимыми полномочиями. Кроме того, не менее важно проводить семинары и обучение принципам компьютерной безопасности.» ***(ВЭФ: Блокчейн-компании пренебрегают кибербезопасностью // «LetKnow OÜ» Подробнее: https://letknow.news/ (https://letknow.news/news/vef-blokcheyn-kompanii-prenebregayut-kiberbezopasnostyu-21113.html). 09.04.2019).***

***

«Компания Micro Focus сообщила о приобретении Interset, одного из лидеров в области ПО для аналитики безопасности, обеспечивающего интеллектуальную и точную защиту от киберугроз. Условия сделки не разглашаются.

Как отмечается, добавление этой технологии прогностической аналитики углубит портфель безопасности, рисков и управления Micro Focus и лежит в рамках её стратегии содействия в быстром и точном контроле и оценке рисков цифровой трансформации бизнеса клиентов.

Interset реализует продвинутые возможности аналитики поведения пользователя и его системного окружения (User and Entity Behavioral Analytics, UEBA) и машинного обучения для быстрого и точного анализа обнаружения угроз. Эта технология ускорит появление более надёжного UEBA-предложения от Micro Focus и поможет углубить необходимое для её концепции SecOps Analytics понимание данных безопасности и операций…

По мнению многих аналитиков Interset завоевала прочную репутацию на рынке, а её программное обеспечение было проверено энергетической, аэрокосмической, оборонной отраслях, в госсекторе и в критической инфраструктуре — там, где обнаружение угроз имеет первостепенную важность. Технологии этой компании дополнят ПО для аналитики больших данных Micro Focus Vertica и Micro Focus ArcSight.

Среди ключевых технологий Interset:

Расширяемая аналитика. Благодаря наличию множества готовых к использованию сценариев, в том числе внутренних угроз, целевых атак и мошенничества, эта технология устраняет необходимость в дорогостоящих консультациях и индивидуальной настройке продукта.

Строгий матаппарат. Программное обеспечение использует растущую библиотеку из более чем 350 проверенных моделей машинного обучения и продвинутой аналитики, применяемых как к событиям, так и к объектам, что даёт

высокоточные средства обнаружения, подключения и количественной оценки действий с высокой степенью риска.

Масштабируемые большие данные. Гибкая открытая платформа комбинирует механизм продвинутой аналитики и технологию больших данных с открытым кодом, включая Kafka, Spark, Phoenix, Hadoop, HBase, Elasticsearch, ZooKeeper, d3 и Kibana. Она может быть развёрнута в инфраструктурах Vertica, Hortonworks или Cloudera, а благодаря масштабированию удовлетворит потребностей самых крупных и сложных сред.» ***(Micro Focus усиливает свои позиции в кибербезопасности покупкой Interset // Компьютерное Обозрение (https://ko.com.ua/micro_focus_usilivaet_svoi_pozicii_v_kiberbezopasnosti_pokupkoj_interset_128597). 26.04.2019).***

***

«Компания Fidelis Cybersecurity опубликовала отчет за первый квартал нынешнего года. Из документа следует, что более 557 тысяч срабатываний защитных решений Fidelis пришлись на инциденты, связанные с уязвимостями, эксплойтами и вредоносным ПО, которые известны не менее двух лет. Общая тенденция состоит в том, что ценность уязвимостей для киберпреступников снижается с момента, когда появляются патчи, устраняющие эти уязвимости. Однако данные Fidelis наглядно свидетельствуют, что старые уязвимости и зловреды продолжают представлять весьма серьезную угрозу. Так, в случае с атаками вредоносного ПО 85% всех срабатываний защитных решений были вызваны обнаружением троянцев удаленного доступа H-W0rm и njRAT. Оба они известны как минимум с 2012 года. Более того, 4% зафиксированных атак оказались атаками червя Conficker, впервые обнаруженного еще в 2008 году.

27% всех попыток эксплуатации уязвимостей ПО также были связаны с проблемами, обнаруженными и исправленными в 2017 году и ранее. Исследователи объясняют эту статистику двумя обстоятельствами. Первое состоит в том, что чем старше уязвимость или зловред, тем проще взять их на вооружение – даже хакерам с низкой квалификацией. Как правило, эксплойты для таких уязвимостей и образцы таких зловредов можно обнаружить в открытом доступе в сети. Вторая же причина в том, что даже спустя годы после выпуска обновлений неизбежно находятся пользователи, которые так и не удосужились эти обновления установить.» ***(Старые зловреды по-прежнему в строю // ООО «Технический центр Интернет» (https://tcinet.ru/press-centre/technology-news/6509/). 29.04.2019).***

***

Сполучені Штати Америки

«…ФБР проводит масштабное переобучение своих спецагентов в связи с растущим числом финансируемых противниками кибератак, угрожающих экономическим и политическим интересам США.

По словам главы отдела ФБР по борьбе с киберпреступностью Эми Хесс (Amy Hess), в последний раз бюро проводило переквалификацию сотрудников таких масштабов в 2001 году после террористической атаки 11 сентября…

Эволюция угроз требует изменений в работе ФБР. По данным международной исследовательской организации Third Way, правоохранители предпринимают шаги по отношению лишь к 1% киберинцидентов и расследуют только наиболее значительные из них, такие как кибератаки, финансируемые правительствами зарубежных стран, или сложные транснациональные преступные схемы.

Как отметил исполнительный директор программы по развитию кибербезопасности и технологий Аспенского Института Гарретт Графф (Garrett Graff), с точки зрения киберресурсов бюро находится на порядок или два ниже, чем требуется. Несмотря на очевидный прогресс в последнее время, только четыре или пять региональных управлений ФБР имеют достаточно ресурсов и обладают соответствующими знаниями для противодействия сложным киберпреступлениям…» ***(Сотрудники ФБР проходят переобучение в связи с ростом киберугроз // SecurityLab.ru (https://www.securitylab.ru/news/498569.php). 01.04.2019).***

***

Російська Федерація та країни ЄАЕС

«Держдума Росії 16 квітня ухвалила закон про "забезпечення безпечного і сталого функціонування" інтернету на території Росії. Закон передбачає ізоляцію російського сегмента інтернету.

Згідно з цим законом, російська влада зможе контролювати точки з’єднання інтернету в країні з зовнішнім світом, йдеться на офіційному сайті Держдуми РФ.

Що передбачає закон? Влада Росії вважає, що закон унеможливить небезпеку масштабних кібератак з боку країн Заходу. Відтак рунет буде відключений від світової мережі тільки у надзвичайних ситуаціях. Росіяни не можуть критикувати у мережі дії влади, або ж висловлюватися проти конкретного політика. На думку законодавців, матеріали, які образили владу, автоматично є фейковими.

У законі прописана можливість створення інфраструктури, яка дозволить російському сегменту працювати ізольовано, якщо оператори зв’язку не зможуть під'єднатися до кореневих серверів інтернету за кордоном.

Відповідати за функціонування інтернету в країні буде Роскомнагляд.

Закон набуде чинності 1 листопада 2019 року, однак окремі його положення діятимуть з 1 січня 2021 року. Витрати на виконання закону попередньо оцінюють у 30 мільярдів рублів.

Росіяни не у захваті від такого закону. У трьох містах Росіїі проти ухвалення Держдумою закону про ізоляцію його російського сегмента. У Москві наймасштабніший – участь у ньому взяли щонайменше 15 тисяч людей, не обійшлось без абсурдних затримань.» ***(Держдума РФ остаточно ухвалила закон про ізоляцію інтернету // Телеканал новин «24»***

(https://24tv.ua/techno/derzhduma_rf_ostatochno_uhvalila_zakon_pro_izolyatsiyu_internetu_n1141475). 16.04.2019).

***

«Московский окружной военный суд вынес приговор последнему фигуранту громкого уголовного дела о шпионаже, в котором были замешаны высокопоставленный сотрудник ФСБ, экс-офицер МВД и известный хакер. Сегодня заключивший досудебное соглашение о сотрудничестве экс-оперуполномоченный Центра информационной безопасности (ЦИБ) ФСБ России Дмитрий Докучаев, передававший, по версии следствия, диски с секретной информацией спецслужбам иностранных государств, получил шесть лет колонии строгого режима.

Вызвавшее большой общественный резонанс дело о госизмене (ст. 275 УК РФ) следственное управление ФСБ расследовало около двух лет. Его основными фигурантами стали бывший начальник отдела оперативного управления ЦИБ ФСБ Сергей Михайлов, начальник отдела компьютерных инцидентов «Лаборатории Касперского», ранее служивший в МВД РФ Руслан Стоянов, хакер Георгий Фомченков, получивший известность как Geser, и экс-оперативник ЦИБ майор Дмитрий Докучаев.

…по версии следствия, в 2011 году полковник Сергей Михайлов, возглавлявший в ФСБ борьбу с хакерами, через посредников передал сотрудникам ФБР сведения об оперативно-разыскной деятельности своего ведомства. Все они были связаны с делом основателя и гендиректора процессинговой компании Chronopay Павла Врублевского, которого в США считают одним из главных киберпреступников в мире.

Переданные американцам секретные данные были получены во время оперативной разработки господина Врублевского, который в России обвинялся в организации DDoS-атаки на сайт компании «Аэрофлот».

Записав их на диски, господин Михайлов передал их своему подчиненному майору Дмитрий Докучаеву, а тот — сотруднику «Лаборатории Касперского» Руслану Стоянову. Господин Стоянов, согласно материалам дела, прилетев в Канаду на международную конференцию по кибербезопасности, передал один диск Кимберли Зенц, сотруднице американской компании I-Defence, которая, по данным ФСБ, активно сотрудничает со спецслужбами США. Другим перевозчиком, считает следствие, был Георгий Фомченков. За свою работу фигуранты, по версии следствия, планировали получить $10 млн…

Трое фигурантов дела были осуждены ранее. Господа Михайлов и Стоянов, вины не признавшие, получили соответственно 22 и 14 лет колонии строгого режима соответственно. Георгий Фомченков, заключивший досудебное соглашение о сотрудничестве и давший показания на своих подельников, на днях был приговорен к семи годам колонии. Господин Докучаев также пошел на сотрудничество со следствием. Его дело рассматривалось сегодня в особом порядке — без исследования доказательств и допросов свидетелей. В итоге экс-оперативник ФСБ получил шесть лет колонии и был лишен звания майора. Срок наказания исчисляется с декабря 2016 года, когда майора взяли под стражу.

При этом суд постановил уничтожить ряд вещественных доказательств по делу, в том числе планшет, ноутбук и мобильный телефон подсудимого…» ***(Дмитрия Докучаева, соучастника «слива» секретов агентам ФБР, за госизмену закрыть на 6 лет, его планшет, ноутбук и мобильный — уничтожить // Vse.Media (http://vse.media/dmitriya-dokuchaeva-souchastnika-sliva-sekretov-agentam-fbr-za-gosizmenu-zakryt-na-6-let-ego-planshet-noutbuk-i-mobilnyj-unichtozhit/). 11.04.2019).***

***

Інші країни

«Заступник міністра інформаційних та комунікаційних технологій Еквадору Патрісіо Реал заявив, що сайти держустанов країни постраждали від 40 млн кібератак після рішення позбавити Ассанжа політичного притулку…

За словами заступника міністра, кібератаки почалися у четвер та в основному здійснюються з Бразилії, США, Нідерландів, Румунії, Німеччини, Франції, Австрії, Великої Британії та самого Еквадору.

Раніше президент Еквадору Ленін Морено заявив, що засновник WikiLeaks Джуліан Ассанж намагався використовувати посольство країни у Лондоні як "центр для шпигунства"…» ***(В Еквадорі заявили про 40 млн кібератак після арешту Ассанж // Медіастар (http://mediastar.net.ua.host1361643.serv39.hostland.pro/81807-v-ekvador-zayavili-pro-40-mln-kberatak-pslya-areshtu-assanzh.html). 16.04.2019).***

***

Протидія зовнішній кібернетичній агресії

«Дослідники стверджують, що проти канадців діятимуть тими самими методами, що й проти громадян інших розвинених демократій

Канадцям варто бути готовими до кібернетичного втручання з-за кордону під час парламентських виборів у жовтні цього року.

Про це йдеться у доповіді Канадського центру кібербезпеки.

«Ми вбачаємо дуже вірогідним, що канадські виборці стикнуться з певним іноземним кібернетичним втручанням, пов’язаним із парламентськими виборами 2019 року. Однак наразі малоймовірно, що це іноземне кібервтручання буде співмірним із російськими діями проти президентських виборів у США в 2016-му», – зазначається у доповіді.

Дослідники стверджують, що проти канадців діятимуть тими самими методами, що й проти громадян інших розвинених демократій…» ***(Розвідка попередила канадців про загрозу кібератак під час виборів // “Українські медійні системи” (https://glavcom.ua/news/rozvidka-poperedila-kanadciv-pro-zagrozu-kiberatak-pid-chas-viboriv-584701.html). 10.04.2019).***

***

«…9 квітня в НАТО стартували чотириденні навчання під назвою Locked Shields 2019 з питань кібербезпеки…

В рамках навчань будуть відпрацьовуватися питання відповіді на втручання хакерів у вибори із метою поширення хаосу і паніки.

В вигаданій країні Берулія в процесі проведення волевиявлення народу хакери за легендою навчань своїми діями виводять із ладу критичну інфраструктуру, що викликає перебої із постачанням води, електроенергії. Це викликає протести із боку населення і ставить під питання легітимність виборів.

У навчаннях будуть брати участь шість команд, до яких залучать 1 тисячу спеціалістів. Тренування із кібербезпеки буде координувати спеціалізований центр передового досвіду, який знаходиться в Естонії…» ***(В НАТО почалися навчання із питань кібербезпеки під час виборів // "Українські медійні системи" (https://glavcom.ua/news/v-nato-pochalisya-navchannya-iz-pitan-kiberbezpeki-pid-chas-viboriv-584578.html). 09.04.2019).***

***

«Європейська комісія та Агентство з кібербезпеки ЄС провели навчання, на яких відпрацьовувалися варіанти реагування на можливі інциденти під час виборів до Європарламенту.

Про це повідомляється на сайті Єврокомісії…

У комп'ютерних навчаннях під назвою EU ELEx19, які були проведені сьогодні у Європарламенті, взяли участь більше 80 представників євроінституцій.

Метою навчань була перевірка спроможності європейських служб виявляти та нейтралізувати кібернетичні інциденти, що можуть завдати шкоди демократичному волевиявленню європейців…» ***(До виборів Європарламенту запускають систему кіберзахисту // Західна інформаційна корпорація (https://zik.ua/news/2019/04/05/do_vyboriv_yevroparlamentu_zapuskayut_systemu_kiberzahystu_1545863) 05.04.2019).***

***

«На закриті сайти американського Федерального бюро розслідувань здійснили кібератаку, внаслідок чого викрали персональні дані чотирьох тисяч агентів.

Хакерам стали доступними унікальні облікові записи із іменами членів асоціації, особистими адресами, номерами телефонів, інформацією електронних рахунків, назвами посад. Про це пише видання TechCrunch, яке поспілкувалось у зашифрованому чаті з одним із тих, хто атакував більш ніж тисячу сайтів.

За словами хакера, у них є "понад мільйон даних" про співробітників у декількох федеральних агенціях США та громадських організаціях.

Ті, хто вчинив кібератаку, видалили всі дублікати інформації та завантажили до себе на спеціальний сайт. Нині інформацію структурують, аби її потім продати.

У виданні спитали хакера, чи турбує їх те, що вони ставлять під загрозу безпеку агентів та правоохоронної системи країни, на що почули відповідь "Та

мабуть". А на запитання, що є метою подібних дій, відповів: "Досвід і гроші".»***(Хакери викрали дані про 4 тисяч американських агентів ФБР, – ЗМІ // Телеканал новин «24» (https://24tv.ua/hakeri_vikrali_dani_pro_4_tisyach_amerikanskih_agentiv_fbr__zmi_n1140429?utm_source=rss). 13.04.2019).***

***

«Високий представник ЄС Федеріка Могеріні зробила окрему заяву у зв'язку із посиленням кібернетичних нападів на країни Євросоюзу, які завдають шкоди економіці та несуть загрози основам безпеки та стабільності. Відповідний документ оприлюднений на сайті Служби зовнішніх дій Євросоюзу. «Європейський Союз та його країни-члени занепокоєні зростанням випадків шкідливої поведінки в кібернетичному просторі, яка спрямована на підрив єдності ЄС, його безпеки та економічної конкурентоспроможності, включаючи зростання кількості шахрайських вчинків стосовно інтелектуальної власності. Таке зловживання технологіями інформації та комунікації може призвести до дестабілізуючого каскадного ефекту з високими ризиками конфліктів», – йдеться у заяві. В декларації не йдеться про причини, які спонукали ЄС до такої заяви. Водночас, Високий представник від імені ЄС та країн-членів закликала «залучених акторів припинити здійснювати такі шкідливі вчинки». Могеріні закликала всіх партнерів ЄС посилити міжнародну співпрацю для поширення безпеки та стабільності в кібернетичному просторі, щоб нейтралізувати такі шкідливі дії. Вона висловила готовність до подальшого обговорення цієї теми щодо захисту прав інтелектуальної власності від кібернетичного шахрайства на рівні ООН та в інших міжнародних структурах, таких як «велика двадцятка»…» ***(Могеріні стурбована посиленням кібератак на Євросоюз // ІНФОРМАТОР (https://informator.news/moherini-sturbovana-posylenniam-kiberatak-na-yevrosoiuz/). 13.04.2019).***

***

«Менше ніж за тиждень до парламентських виборів у Фінляндії розслідують кібератаку на онлайн-сервіс, що публікує результати голосування…

Кібератака, спрямована на збій доступу до сайту, відбулася минулого тижня, повідомляє Національне бюро розслідувань 10 квітня. Передбачуваний злочин є серйозним втручанням в телекомунікації країни, з цього приводу триває досудове розслідування.

У Фінляндії немає електронного голосування. Напад не вплинув на процес голосування або фактичний підрахунок бюлетенів, а отже, не може вплинути на результат виборів, повідомили в поліції.

Подібна атака у виборчу ніч може серйозно завадити доступу медіа до результатів виборів і підірвати довіру громадськості до виборів. Наразі немає жодного підозрюваного, повідомили в поліції…» ***(Фінляндія виявила кібератаку на портал, що публікує результати виборів // Європейська правда (https://www.eurointegration.com.ua/news/2019/04/10/7095007/). 10.04.2019).***

***

«…бельгийский центр кибербезопасности не нашел никаких доказательств того, что телекоммуникационное оборудование, поставляемое Huawei Technology, могло бы использоваться для шпионажа.

Агентству, которое отчитывается перед премьер-министром Бельгии, было поручено проанализировать возможную угрозу, создаваемую Huawei, если та будет поставлять оборудование бельгийским операторам мобильной связи Proximus, Orange Belgium и Telenet.

После проведенной проверки, центр кибербезопасности сообщил: «Пока мы не нашли технических признаков, указывающих на угрозу шпионажа, однако, решение не окончательное, мы продолжаем изучать вопрос.»… ***(Бельгия не нашла доказательств того, что телекоммуникационное оборудование Huawei несет угрозу шпионажа // Droidbug.com (https://droidbug.com/belgiya-ne-nashla-dokazatelstv-togo-chto-telekommunikatsionnoe-oborudovanie-huawei-neset-ugrozu-shpionazha/). 17.04.2019).***

***

«…Европейская комиссия и Агентство по кибербезопасности ЕС провели учения по защите компьютерных систем, на которых отрабатывались варианты реагирования на возможные инциденты во время выборов в Европарламент. Об этом сообщает пресс-служба Еврокомиссии.

"Мы должны защитить наши свободные и справедливые выборы. Это краеугольный камень нашей демократии. Для защиты нашего демократического процесса от манипуляций или разрушительных кибернетических действий со стороны частных лиц или отдельных стран, мы решили испытать нашу кибернетическую бдительность и готовность к проведению безопасных выборов в 2019 году", - отметил вице-президент Еврокомиссии по вопросам общего цифрового рынка Андрус Ансип.

В киберучениях под названием EU ELEx19, которые были проведены сегодня в Европарламенте, приняли участие более 80 представителей евроинституций.

Целью учений была проверка способности европейских служб выявлять и нейтрализовать кибернетические угрозы, которые могут нанести ущерб демократическому волеизъявлению европейцев…» ***(В Европарламенте отработали методы киберзащиты выборов // Информационное агентство ЛІГАБізнесІнформ (https://news.liga.net/world/news/v-evroparlamente-otrabotali-metody-kiberzaschity-vyborov). 05.04.2019).***

***

«…Госсекретарь США Майк Помпео призвал союзников по НАТО адаптироваться для противодействия новым угрозам…

Как сообщается, в новой стратегии национальной обороны США Китай и Россия занимают центральное место.

"Мы должны адаптировать наш альянс, чтобы противодействовать возникающим угрозам… будь то российская агрессия, неконтролируемая

миграция, кибератаки, угрозы энергетической безопасности, стратегическая конкуренция со стороны Китая, включая технологии и 5G, и многое другое", - сказал Помпео…

Помпео также отметил, что НАТО следует найти способы противодействия возрастающим киберугрозам, в том числе со стороны Китая…» ***(Помпео призвал союзников по НАТО адаптироваться к новым угрозам РФ и Китая // «РБК-Украина» (https://www.rbc.ua/rus/news/pompeo-prizval-soyuznikov-nato-adaptirovatsya-1554407004.html). 04.04.2019).***

***

Кіберзахист критичної інфраструктури

«Міністерство енергетики США вивчає можливість використання технології блокчейн для запобігання кібератак на об'єкти енергетики. Про це повідомляється на сайті Національної лабораторії енергетичних технологій, яка є підрозділом Міненерго США…

Блокчейн хочуть використовувати для децентралізації енергосистеми, щоб дані, на які зазіхають хакери, не зберігалися в одному місці. Блокчейн показує реальний стан енергосистеми, тоді як раніше під час кібератаки система продовжувала демонструвати штатну ситуацію, при цьому мільйони споживачів залишалися без світла, відзначається в прес-релізі лабораторії.

Технологія дозволить контролювати роботу об'єктів енергетики і дасть можливість виробникам і споживачам енергії виконувати всі транзакції в мережі.

Раніше Міненерго США виділило грант у розмірі 1 млн доларів на фінансування стартапу, він займається розробками блокчейн-технологій для енергетики. Міністерство також виділило майже 5 млн доларів для університетських досліджень в цій області…» ***(Олексій Супрун. У США планують використовувати блокчейн для запобігання кібератак в енергетиці // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1792862-u-ssha-planuyut-vikoristovuvati-blokcheyn-dlya-zapobigannya-kiberatak-v-energetitsi). 12.04.2019).***

***

Захист персональних даних

«Данные пользователей Facebook оказались доступны на других платформах и в облачном хранилище Amazon, сообщила компания UpGuard, занимающаяся кибербезопасностью. В открытый доступ попали более 540 млн записей пользователей соцсети с комментариями, лайками, названиями учетных записей, они были обнаружены на мексиканской цифровой платформе Cultura Colectiva. Bloomberg отмечает, что доступ к базе был закрыт после того, как журналисты предупредили Facebook о проблеме.

Данные еще 22 000 пользователей Facebook, включая имена, пароли, адреса электронной почты, были доступны в уже не существующем приложении At the Pool. UpGuard уточняет, что не знает, как долго они хранились в приложении, поскольку база была закрыта, пока компания изучала ее. Все эти данные находились в облачном хранилище Amazon…» ***(Миллионы записей пользователей Facebook попали в открытый доступ // АО Бизнес Ньюс Медиа (https://www.vedomosti.ru/technology/news/2019/04/03/798227-facebook). 03.04.2019).***

***

«…Як пише The Verge, Microsoft почала сповіщати користувачів Outlook, що хакери могли отримати доступ до їхньої електронної скриньки.

Компанія зазначає, що зловмисники могли переглядали адреси електроні адреси, назви папок і тему листів. В окремих сповіщеннях Microsoft писала, що хакери могли бачити й вміст повідомлень юзерів. Такі попередження отримали майже 6 % користувачів Outlook, підкреслює Vice.

Видання пише, що компанія визнала більший витік даних лише після опублікованих скриншотів, які про нього свідчили. Microsoft сповістила, що неавторизований доступ був можливий з 1 січня до 28 березня 2019 року.

Прес-секретар компанії спростував інформацію про те, що такий доступ хакери мали упродовж півроку…» ***(Microsoft визнала, що хакери могли мати доступ до пошти Outlook // MediaSapiens (https://ms.detector.media/web/cybersecurity/microsoft_viznav_scho_khakeri_mogli_mati_dostup_do_poshti_outlook/). 15.04.2019).***

***

«В Сети в открытом доступе появилась база данных с информацией о вызовах скорой помощи с нескольких подмосковных станций. В базу входят контакты пациентов, а также записи врачей, сделанные по результатам выезда. Эксперты считают, что причиной раскрытия конфиденциальной информации стали неправильные настройки хранилища под управлением MongoDB.

База размером около 18 Гб выложена на одном из облачных сервисов и содержит сведения о пациентах скорой помощи из Долгопрудного, Балашихи, Королева и других подмосковных городов. В частности, в ней указаны даты вызовов, имена, адреса и контактные телефоны пациентов. Кроме того, по каждому выезду имеется заключение врачей с описанием состояния человека, обратившегося за помощью.

Как предполагают эксперты по информационной безопасности, злоумышленники украли данные из незащищенной базы MongoDB, которая отличается слабыми настройками безопасности по умолчанию. Если администратор не позаботится об изменении параметров доступа к хранилищу, оно может остаться открытым для всех желающих. В данном случае сотрудники скорой помощи предположительно забыли защитить свою базу паролем.

Подобная халатность уже стала причиной нескольких утечек…

Следственный комитет Московской области начал проверку по факту обнаружения в Сети базы данных скорой помощи, а представители Министерства

здравоохранения региона уже заявили, что обнаруженные в незащищенном хранилище сведения не имеют отношения к реальным жителям Подмосковья.» ***(Julia Glazova. База данных подмосковной скорой помощи утекла в Сеть // Threatpost (https://threatpost.ru/moscow-region-ambulance-service-database-leaked-due-to-bad-mongodb-settings/32197/). 10.04.2019).***

***

«Согласно результатам глобального исследования InfoWatch, в 2018 г. было зарегистрировано 2263 публичных случаев утечки конфиденциальной информации. В 86% инцидентов были скомпрометированы персональные данные и платежная информация. Всего было похищено около 7,3 млрд записей против 13,3 млрд годом ранее.

Больше всего пользовательских данных утекло из высокотехнологичных компаний, сфер торговли и HoReCa, медицинских и муниципальных учреждений — на них суммарно пришлось 70% годового объема утечек персональной информации в мире. На компании сферы высоких технологий пришлось около 30% от мирового объема утечек. При этом наиболее привлекательными для злоумышленников остаются данные из организаций финансово-кредитной и страховой сферы, где около 65% утечек были совершены умышленно.

Вместе с тем, средняя мощность инцидентов снизилась. В высокотехнологичном секторе она упала более чем в два раза — до 9 млн записей данных на одну утечку, в финансовых и страховых компаниях — в четыре раза до 190 тыс. записей, в промышленных и транспортных предприятиях — в семь раз до менее чем 100 тыс. записей.

«Отраслевую картину утечек определяют два ключевых фактора — это ликвидность и защищенность информации, — отмечает аналитик InfoWatch Сергей Хайрук. — Там, где ценность данных наиболее очевидна и защите информации уделяется большее внимание, например, в банках, страховых компаниях и госсекторе, объем утечек значительно ниже. Такие структуры защищают корпоративные и пользовательские данные с помощью организационных и технических мер: используют DLP-, SIEM- и другие профильные ИБ-системы, заботятся о повышении уровня цифровой гигиены сотрудников. И если раньше бизнес охотнее инвестировал в защиту своей интеллектуальной собственности, коммерческих секретов и ноу-хау, а к безопасности клиентских данных относился с меньшим вниманием, то с введением огромных штрафов за утечки данных эта ситуация меняется»…

Доля утечек по вине внутреннего нарушителя в 2018 г. возросла на 3% до 63% от общего количества утечек. Каждый второй инцидент произошел по вине рядового специалиста, еще около 10% случаев пришлись на «привилегированных» пользователей (руководители и системные администраторы), подрядчиков и бывших сотрудников компаний.

«Результативность хакерских атак упала более чем на треть, в среднем до пяти миллионов записей данных на каждый инцидент, однако говорить о коренном переломе в борьбе с внешними злоумышленниками пока не приходится: общее число таких инцидентов не снизилось, взломы хакерами огромных баз данных по-

прежнему случаются регулярно, — отметил Сергей Хайрук. — «Внутренние» утечки кажутся менее разрушительными из-за меньшего объема скомпрометированных записей данных, но инсайдеры, обладая практически неограниченным доступом к внутренним ресурсам организации, могут завладеть наиболее ценной информацией».

Самая масштабная утечка информации произошла в Индии, где были скомпрометированы 1,2 млрд записей данных пользователей, включая биометрическую информацию, из системы AADHAAR — крупнейшего государственного хранилища идентификационных данных в мире. Также были зафиксированы крупные утечки информации из коммерческих компаний: разработчика ПО Veeam (440 млн записей), гостиничной сети Marriott (383 млн), маркетинговой фирмы Exactis (340 млн), логистической компании SF Express (300 млн), сервисного стартапа Apollo (200 млн), ИТ-компании VNG (около 163 млн) и приложения Under Armour (150 млн).

Наиболее популярным каналом утечки информации остается сетевой (72%). По сравнению с 2017 г. на 5% снизилась доля инцидентов, связанных с использованием электронной почты, также на 0,8% сократилась доля утечек в результате кражи или потери оборудования, на 0,2% — с помощью мобильных устройств.» ***(Объем утечек данных в прошлом году сократился в два раза // «Компьютерное Обозрение» (https://ko.com.ua/obem_utechek_dannyh_v_proshlom_godu_sokratilsya_v_dva_raza_128327). 04.04.2019).***

***

«По данным Национального центра кибербезопасности Великобритании (NCSC), имена звезд, футболистов, музыкантов и вымышленных персонажей стали одними из худших паролей года… Но ничто не сравнится с «123456» как с худшим паролем из всех возможных. В течение многих лет шестизначный пароль считался «наименее удачным», учитывая его широкое использование. За ним следует — «123456789».

По сообщению NCSC, более 30 миллионов жертв используют эти два пароля. Такие выводы сделаны на основании последнего анализа нарушений Pwned Passwords, веб-сайта исследователя безопасности Троя Ханта…» ***(Эксперты назвали худшие пароли года // Goodnews.ua (http://goodnews.ua/technologies/eksperty-nazvali-xudshie-paroli-goda/). 22.04.2019).***

***

«Компания Yahoo, входящая в состав американского телекоммуникационного гиганта Verizon, согласилась выплатить почти 118 млн долларов в качестве компенсации за урегулированию коллективного иска, связанного с масштабными утечками данных. Об этом во вторник, 9 апреля, сообщило информационное агентство "Рейтер" со ссылкой на соглашение, которое Yahoo направила на утверждение в федеральный окружной суд в Сан-Хосе.

Yahoo согласилась заплатить 117,5 млн долларов, в том числе 55 млн долларов в качестве компенсации расходов жертв хакерского взлома. Еще 30 млн долларов пойдут на оплату юридических услуг. Соглашение охватывает до 194 млн пользователей в США и 896 млн в Израиле.

Адвокат Джон Янчунис (John Yanchunis), представляющий интересы стороны обвинения, назвал 117,5 млн долларов "крупнейшей среди публично известных выплат по делу об утечке данных".

В результате серии кибератак хакеры взломали сервисы Yahoo в период с 2013 по 2016 годы, получив доступ к 3 млрд учетных записей. Злоумышленники могли узнать имена пользователей, а также адреса их электронной почты, пароли, телефонные номера.

Договор о досудебном урегулировании должен быть одобрен окружным судьей Люси Кох (Lucy Koh), которая уже отвергала предыдущую попытку досудебной договоренности по причине невыгодности для пострадавших. Так, в конце января 2019 года Люси Кох не утвердила соглашение, по условиям которого Yahoo должна была выплатить пострадавшим 50 млн долларов и бесплатно оказывать услуги кредитного мониторинга (услуги включают контроль за кредитным рейтингом и предотвращение краж персональных данных) в течение двух лет.

По словам Кох, такие условия не являются "принципиально справедливыми, адекватными и разумными", поскольку соглашение не учитывало общую стоимость выплат и не указывало, сколько жертв могут рассчитывать на компенсацию. Кроме того, судья утверждала, что судебные издержки для истцов оказались слишком высокими.

Ранее стало известно о том, что Yahoo придется столкнуться с общенациональным судебным разбирательством, инициированным от имени более одного миллиарда пользователей, которые заявили, что их личная информация была скомпрометирована в результате трех серьезных нарушений данных…» ***(Yahoo заплатит 118 млн долларов за утечку данных 3 млрд пользователей // Goodnews.ua (http://goodnews.ua/technologies/yahoo-zaplatit-118-mln-dollarov-za-utechku-dannyx-3-mlrd-polzovatelej/). 11.04.2019).***

***

«…Генеральный прокурор штата Нью-Йорк Летиция Джеймс (Letitia James) заявила, что занялась расследованием несанкционированного хранения компанием Facebook Inc базы данных электронной почты для контактов около 1,5 миллионов пользователей соцсети. Общее число людей, которые могли пострадать от незаконных действий Facebook, Джеймс оценила в сотни миллионов человек.

Недавно Facebook признал, что с мая 2016 г. мог непреднамеренно получать данные о контактах пользователей в электронной почте без их ведома и хранить эти сведения. В компании уверяют, что не делились полученной информацией с третьими лицами и сейчас удаляют со своих серверов все данные.

По мнению прокуратуры Нью-Йорка, действия Facebook – демонстрация того, что компания не принимает всерьез свою роль в процессе защиты

персональных данных. «Пора призвать Facebook к ответу за то, как соцсеть относится к личной информации пользователей», – заключила Джеймс. Представитель Facebook заявил, что соцсеть сотрудничает со следствием…» ***(В США расследуют незаконное хранение Facebook данных 1,5 млн пользователей // РосКомСвобода (https://roskomsvoboda.org/46845/). 26.04.2019).***

***

«Новая БД под названием Common Identity Repository (CIR) будет доступна для поиска и позволит отслеживать биометрические данные граждан стран Евросоюза и не входящих в союз государств

Парламент ЕС проголосовал за создание большой биометрической базы данных, известной как хранилище общей идентичности (Common Identity Repository, CIR). Данная БД соберет записи о более чем 350 миллионах человек и поможет упростить работу сотрудников пограничных и правоохранительных органов ЕС, будет доступна для поиска и позволит отслеживать биометрические данные граждан стран ЕС и не входящих в него государств.

Предполагается, что CIR будет объединять идентификационные записи (имена, даты рождения, номера паспортов и другую идентифицирующую информацию) и биометрические данные (отпечатки пальцев, сканы лица). Доступ к сведениям смогут получать все пограничные и правоохранительные органы. Основное предназначение БД заключается в упрощении работы пограничников и сотрудников органов правопорядка ЕС, которые смогут быстрее осуществлять поиск в единой системе, а не в разрозненных базах данных.

Согласно опубликованному на сайте Европарламента пресс-релизу, в число охватываемых новыми правилами систем войдут Шенгенская информационная система, Eurodac, Визовая информационная система (VIS) и три новые системы: Европейская система криминальных досье на лиц из третьих стран (ECRIS-TCN), Система въезда/выезда (EES) и автоматическая система авторизации въезда в Шенгенскую зону (ETIAS).

После запуска CIR пополнит число крупнейших отслеживающих БД мира наряду с базой данных китайского правительства и индийской биометрической системой Aadhar. В свою очередь, Европейский парламент и Европейский совет пообещали реализовать надлежащие меры для защиты конфиденциальности граждан и контроля доступа к данным правоохранительных органов.» ***(ЕС создает единую базу биометрических данных // РосКомСвобода (https://roskomsvoboda.org/46738/). 22.04.2019).***

***

«…Аналитический центр InfoWatch составил дайджест утечек из СМИ.

В США жертвой хакерской атаки стало крупное калифорнийское издание Sacramento Bee. Компьютерные злоумышленники проникли на сторонний сервер, на котором хранились две базы данных, поддерживаемые газетой. Первое хранилище включало личную информацию всех избирателей Калифорнии (всего порядка 19,4 млн человек), а во втором были данные 53 тыс. подписчиков

Sacramento Bee. При этом хакеры оставили на сервере записку с требованием о выкупе в биткойнах, но издание не пошло на поводу у преступников.

Филиппинский медиа-конгломерат ABS-CBN благодаря исследователю безопасности Виллему де Гроота раскрыл схему перехвата платежных данных со своего портала заказов. Используя вредоносное ПО, заложенное в файл JavaScript, злоумышленники собирали информацию о банковских картах клиентов и отправляли ее на удаленный сервер в российском Иркутске.

Новостной еженедельник L'Express (Франция) оставил на незащищенном сервере Mongo DB базу данных. В хранилище объемом около 60 ГБ находились данные 693 тыс. читателей (имя, фамилия, e-mail, фото, место работы и т.д.), а также важная информация об операционной деятельности издания. Обнаруживший утечку исследователь почти месяц ждал ответа издания. Все это время добровольному помощнику приходилось периодически восстанавливать базу данных после вмешательства хакеров.

Еще более масштабную утечку потерпела телевизионная компания Sky Brazil. На оставленном без пароля сервере ElasticSearch хранились данные 32 млн подписчиков. Широкому кругу пользователей Сети стала доступна такая информация, как имена, адреса, даты рождения, номера мобильных телефонов, пароли, детали платежей и др. Скомпрометированные данные принадлежали не только домашним подписчикам, но и корпоративным клиентам телекомпании.» ***(Журналисты тоже теряют данные // IKSMEDIA.RU (http://www.iksmedia.ru/news/5584494-Zhurnalisty-tozhe-teryayut-dannye.html). 30.04.2019).***

***

Кіберзлочинність та кібертерроризм

«Чтобы прекратить фишинговые атаки, мы должны быть в состоянии их предвидеть. В то же время это помогает составить представление о том, за какими фишинговыми и вредоносными угрозами мы должны следить…

"В докладе "Шесть фишинговых прогнозов: 2019 год" говорится, что компании и потребители могут ожидать от хакеров и киберпреступности в целом в следующем году", - прокомментировал генеральный директор Networks Unlimited Africa Антон Якобс.

По словам аналитиков Cofense Ника Гуарио и Лукаса Ашбо, надежных сервисов не будет. Согласно их прогнозам, большинство фишинговых атак будут в таких сервисах, как Google Docs, Sharepoint, WeTransfer, Dropbox, Citrix ShareFile и Egnyte.

"Фишинг с учетными данными привлечет внимание хакеров. Как и в прошлом году. Хакерам не нужно взламывать, они входят в систему", - считает консультант Cofense Security Solution Advisor Тони Дадли. – "Этот тип фишинговой кампании останется одной из главных угроз, особенно для организаций, которые не смогли включить многофакторную аутентификацию".

Как заявил директор Cofense Дэвид Маунт, многие люди ждут, что ИИ станет панацеей от фишинговых атак. Тем не менее, 2019 год не улучшит ситуацию. "ИИ может быть настолько же хорош, насколько и тот, кто его создает, и, поскольку фишинг-злоумышленники постоянно развивают свою тактику, ИИ может быть сложно идти в ногу. Пользователи столкнутся с тем, что сам ИИ станет целью. В 2019 году искусственный интеллект начнет играть роль в общей стратегии безопасности многих организаций", - утверждает Маунт.

По мнению менеджера аналитики угроз Cofense Молли МакДугалл и аналитика разведки Даррела Ренделла, стоит ожидать готовых и настраиваемых вредоносных программ. "В фишинговых кампаниях в дальнейшем появятся и другие специализированные вредоносные программы", - прокомментировали эксперты.

"Продолжающееся доминирование недорогих готовых вредоносных программ указывает на то, что они, вероятно, успешны. Настоящая опасность будет в улучшенных банковских троянах и других "похитителях". Ввиду снижения прибыльности операций вирусов-вымогателей и текущего состояния рынка криптовалют, субъекты угроз, скорее всего, будут полагаться на более традиционные вредоносные программы для незаконной монетизации. Более того, благодаря модульным банковским троянам, доступным для покупки, субъекты угроз будут и впредь предлагать более сложные и широкие возможности для своих менее опытных коллег", - сообщается в докладе Cofense.

Джейсон Морер, исследователь Cofense, согласен с тем, что вирусы-вымогатели будут связаны с криптовалютой. "В 2019 году эта тенденция продолжится, даже если она зависит от траектории рынков криптовалют. Если мы увидим возрождение криптовалюты, то и рост популярности вирусов-вымогателей перед скачком цен", - заключил Морер.

Последний прогноз, о котором говорилось в отчете Cofense, сделал Дэвид Маунт - субъекты угроз будут делиться разведданными, чтобы оставаться на шаг впереди. По мере того, как предприятия обновляют свои стратегии кибербезопасности, развиваются и методы атаки.

"Несмотря на очевидные преимущества, отрасль неохотно делится своими знаниями. Из-за этого в 2019 году субъекты угроз будут продолжать оставаться на шаг впереди, и это еще одна причина, по которой предприятия должны действовать быстрее, предпринимая согласованные усилия, чтобы сосредоточиться на самой важной части своей защиты – людях", - заявил Маунт.» ***(Ирина Фоменко. Эксперты определили шесть фишинговых прогнозов на этот год // Internetua (https://internetua.com/eksperty-opredelili-shest-fishingovyh-prognozov-na-etot-god-). 10.04.2019).***

***

«Больницы и индустрия здравоохранения все чаще становятся жертвами хакеров, киберпреступников и шпионов, которые ищут личную и финансовую информацию…

Атаки организованных группировок и даже государственных шпионских агентств вызывают все большую обеспокоенность, поскольку преступники ищут детали, которые можно использовать для вымогательства или даже шпионажа.

Как утверждают в BDO, кража финансируемой государством группы шпионажа личных данных 1,5 миллиона человек из базы данных систем здравоохранения Сингапура, в том числе информации премьер-министра, придала большое значение подобным угрозам.

"Больницы и клиники намного хуже защищены, нежели банки или государственные учреждения, несмотря на то, что они представляют собой "honeypot" (ресурс-приманка для преступников – ред.) ценной информации", - заявил эксперт по кибербезопасности Грегори Гарретт. – "Индустрия здравоохранения располагает электронными медицинскими записями о физических лицах, личной идентифицируемой информацией, и в большинстве случаев - данными платежных карт".

Национальный центр кибербезопасности Великобритании (National Cyber Security Centre) тесно сотрудничает с сектором здравоохранения и социального обеспечения, "чтобы их платформы были максимально безопасными и устойчивыми".

Предполагаемый ущерб просчитали в ходе атаки WannaCry 2017 года, которая нанесла вред компьютерам NHS. Позднее Министерство здравоохранения обнаружило, что атака обошлась NHS в 92 млн фунтов стерлингов, поскольку треть медицинских учреждений и 8% учетных записей врачей были заблокированы, а за них требовали выкуп.

Кибератака блокировала 200 000 компьютеров, показывая пользователям сообщения об ошибках и требуя криптовалюту Bitcoin. Позже в атаке вымогателей обвинили северокорейских хакеров.

Однако, как считают эксперты BDO, атаки направлены именно на систему здравоохранения, чтобы украсть информацию. В первой половине 2018 года американские организации здравоохранения сообщили о 176 крупных нарушениях данных…

Конфиденциальные медицинские сведения о лидерах бизнеса, политиках или военных деятелях также могут быть полезны шпионам. Когда хакеры взломали базу данных систем здравоохранения Сингапура, они украли имена, адреса и - в некоторых случаях - подробности отпускаемых лекарств. Компания по кибербезопасности в марте 2019 года обвинила "шпионскую группу, спонсируемую государством" Whitefly…» ***(Ирина Фоменко. The Telegraph: зачем хакеры атакуют сайты больниц // Internetua (https://internetua.com/the-telegraph-zacsem-hakery-atakuyut-saity-bolnic). 09.04.2019).***

***

«За последние несколько месяцев исследователи из подразделения Cisco Talos обнаружили в Facebook несколько открытых групп, выступающих в качестве онлайн-рынков и форумов для киберпреступников.

Большая часть сообществ использует названия, явно указывающие на их преступный характер. Тем не менее некоторым из них удалось просуществовать

восемь лет, в общей сложности в них состояло примерно 385 тыс. участников. Подобные сообщества нашлись по ключевым словам, таким как «спам», «кардинг» или «CVV». Более того, если пользователь вступает в одну из них, рекомендательные алгоритмы Facebook предлагают ему аналогичные страницы.

Исследователи составили список из 74 групп, члены которых предлагали спам-инструменты и базы электронных адресов для начинающих мошенников, а также учетные данные с различных сайтов, номера кредитных карт и соответствующие им CVV-коды — иногда даже с документами, удостоверяющими личность, или фотографиями жертв. Помимо прочего, свои услуги продвигали преступники, помогающие в выводе крупных сумм и продающие подставные счета.

В большинстве случаев участники групп принимали оплату в криптовалюте, но некоторые использовали посредников, выступавших гарантами сделки между продавцом и покупателем — они предпочитали счета PayPal.

Исследователи связались со службой безопасности Facebook, и большинство нежелательных групп в скором времени удалили. Однако новые аналогичные сообщества все еще появляются, и некоторые из них были по-прежнему активны на момент публикации Cisco Talos…» ***(Egor Nashilov. В преступных группах на Facebook насчитали 385 тысяч человек // Threatpost (https://threatpost.ru/dozens-of-criminal-communities-found-on-facebook/32158/). 08.04.2019).***

***

«В популярной соцсети набирает активность новая компания с названием «The Nasty List». У мошенников стандартная цель – получить учетные данные пользователей. После этого преступники задействуют пострадавшую запись в фишинговой деятельности. От их имени рассылаются сообщения другим аккаунтам с текстом, которые говорит, что аккаунт якобы был замечен списке «Nasty List».

Вот как примерно выглядит текст такого сообщения:

«Ничего себе, ты действительно здесь — @TheNastyList_34. Твой номер — 15. Это очень плохо».

Такие сообщения, естественно, получают все подписчики взломанной записи. Если же пользователей переходит, по ссылку, то он попадает в профили: «The Nasty», «Nasty List» или «YOUR ON HERE!!». В описание этой записи фишеры добавили сообщение «Люди действительно заносят нас сюда, у меня уже 37 место. Если ты это читаешь, ты тоже должен быть в списке».

Вся суть, конечно же заключена в мошеннической ссылке, где пользователей должен ввести свои данные. После этого он видит страницу, очень похожую на обычную страницу входа в Instagram. После того, как данные были введены на этой страницу – они украдены. В дальнейшем эта страница будет также использоваться для рассылки.» ***(Фишеры атакуют Instagram // SecureNews (https://securenews.ru/instagram-phishing-attack/). 15.04.2019).***

***

«Киберпреступники придумали новый метод, как замаскировать свои незаконные действия. Согласно отчету глобальной платежной системы Swift,

мошенники специально снижают суммы транзакций и выполняют зловредные действия в стандартное рабочее время. Таким образом они пытаются смешаться с регулярными платежными потоками и избежать обнаружения.

Исследование под названием «Three years on from Bangladesh: tackling the adversaries» («Три года спустя после Бангладеша: борьба с противниками») предоставляет новое понимание эволюционирующей природы киберугроз, с которыми сталкивается мировое финансовое общество.

Результаты исследования показывают, что четыре из пяти мошеннических транзакций были переведены на счета бенефициаров в Юго-Восточной Азии. При этом сумма каждой отдельной платежной операции резко снижалась — с более чем $10 млн до $2 млн и даже $250 тыс

Основываясь на расследованиях, проведенных за последние 15 месяцев, в отчете говорится, что злоумышленники переходят на расширенные режимы разведки, работают «молча» в течение нескольких недель или месяцев, тщательно изучая поведение той или иной компании, разрабатывая шаблоны предстоящих атак. Кроме того, изменилось и время совершения афер: ранее преступники предпочитали совершать зловредные действия в нерабочее время, но совсем недавно они полностью трансформировали этот подход и начали действовать в дневное время, чтобы слиться с обычными рабочими процессами.

Уже известная атака на бангладешский банк в 2016 году подтолкнула специалистов Swift к запуску собственной программы обеспечения безопасности клиентов, направленной на общеотраслевое сотрудничество в борьбе с киберугрозами. По словам представителей организации, эта программа предусматривает более тесное партнерство с предприятиями финансовой индустрии. Это поможет быстро идентифицировать те финучреждения, на которые нацелены киберпреступники.

Обмен информацией об угрозах кибератаки позволит Swift выявить изменения в тактике, методах и инструментарии преступников, что позволит участникам отрасли быстро реагировать на все более изощренный характер киберугроз…» ***(Эволюция кибератак: в Swift рассказали о новой тактике действий мошенников // (http://goodnews.ua/technologies/evolyuciya-kiberatak-v-swift-rasskazali-o-novoj-taktike-dejstvij-moshennikov/). 11.04.2019).***

***

«Японский производитель оптического оборудования HOYA был вынужден на три дня приостановить работу своего завода в Таиланде из-за кибератаки… Инцидент произошел в феврале нынешнего года.

…злоумышленники заразили порядка сотни компьютеров вредоносным ПО, предназначенным для хищения учетных данных и внедрения майнера криптовалюты. Атака была обнаружена после того, как специалисты компании заметили существенную нагрузку на сетевой сервер. По словам представителей HOYA, работу криптомайнера удалось заблокировать, однако кибератака привела к снижению производительности завода примерно на 40%.

Инцидент затронул не только серверы в Таиланде, но и подключенные к сети компьютеры в штаб-квартире HOYA в Японии, в результате чего сотрудники

компании не смогли выписывать счета-фактуры. Как отмечается, признаков утечки данных не обнаружено. О том, какую именно криптовалюту пытались майнить злоумышленники, не сообщается…» ***(Кибератака на три дня остановила работу завода в Таиланде // Goodnews.ua (http://goodnews.ua/technologies/kiberataka-na-tri-dnya-ostanovila-rabotu-zavoda-v-tailande/). 10.04.2019).***

***

«Крупнейшая фармацевтическая компания Германии Bayer сообщила об обнаружении и сдерживании кибератаки на свои компьютерные системы. В начале прошлого года специалисты выявили в сетях компании вредоносное ПО из арсенала киберпреступной группировки Winnti и до недавнего времени тайно наблюдали за его активностью, после чего вредонос был удален…

Никаких свидетельств компрометации данных исследователи не обнаружили, однако оценка общего ущерба пока что не окончена…» ***(Киберпреступники атаковали крупную фармацевтическую компанию Bayer // Goodnews.ua (http://goodnews.ua/technologies/kiberprestupniki-atakovali-krupnuyu-farmacevticheskuyu-kompaniyu-bayer/). 04.04.2019).***

***

«Злоумышленники охотно используют протокол шифрования трафика SSL для сокрытия киберугроз. Стандартные корпоративные ИТ-системы с этой проблемой не справляются.

Половину атак не видно

Повсеместный рост использования SSL-шифрования трафика приводит к тому, что корпоративные системы безопасности не видят примерно половины кибератак, направленных на конечных пользователей внутри периметра. Это следует из результатов исследования угроз в сфере облачной безопасности компании Zscaler.

Злоумышленники с большой охотой используют SSL-шифрование, поскольку, как указывается в исследовании, теперь соответствующие сертификаты стало очень просто получить.

«По мере роста озабоченности конфиденциальностью данных возникла мощная тенденция к шифрованию интернет-трафика по умолчанию, — заявил старший технический директор и вице-президент Zscaler Амит Синха (Amit Sinha). — Для конфиденциальности это действительно великолепное решение, но для ИТ-безопасности это новая проблема. Расшифровка, исследование и перешифровка трафика — задача нетривиальная, у традиционных устройств защиты сетей она вызывает резкий спад производительности, и большинство организацией не имеют технической оснастки для инспектирования зашифрованного трафика в должных объемах».

По его словам, сегодня значительная часть киберугроз «доставляется» посредством шифрованного трафика, и системы безопасности организаций не видят более половины вредоносного ПО, которое направляется работникам этих организаций.

Способ борьбы? «Промежуточная инспекция»

Облачная платформа Zscaler позволяет производить широкомасштабную промежуточную инспекцию SSL-трафика без ущерба производительности; половину прошлого года (июль-декабрь 2018 г.) разработки Zscaler позволили заблокировать 1,7 млрд. угроз, скрытых в SSL-трафике.

По общему итогу Zscaler удалось ежемесячно блокировать 2,7 млн фишинговых атак, производившихся через зашифрованные каналы (+400% по сравнению с 2017 г.), 32 млн соединений с ботнетам, порядка 240 тыс. попыток атаковать пользователей через браузер.

Примерно треть новых вредоносных доменов, которые блокировались системами Zscaler, использовали SSL-соединения.

Фишеры также охотно использовали HTTPS-трафик для атак на пользователей ряда крупнейших мировых сервисов. Например, на пользователей Microsoft Office 365 и OneDrive были направлены 58% атак; 12% атак — на пользователей Facebook, по 10% — на Amazon и Apple, по 4% — на пользователей Adobe и Dropbox, 2% — DocuSign.

Одна из самых неприятных тенденций, отмеченных Zscaler в 2018 г., — это рост количества атак с использованием программных скиммеров на JavaScript. Они начинаются с компрометации площадок электронной коммерции и внедрением тщательно замаскированного скрипта, который пытается перехватывать платежные данные. С использованием SSL эти атаки становятся особенно опасными, поскольку своевременное их обнаружение оказывается чрезвычайно затруднено.

Не все эксперты, однако, согласны с тем, что предлагаемый Zscaler подход адекватен проблеме. «Любая технология может быть использована в преступных целях, и технологии шифрования тут не исключение, — отмечает Тарас Татаринов, эксперт по информационной безопасности компании SEC Consult Services. — Это, однако, не повод отказываться от шифрования: наоборот, фактически подтверждается эффективность протокола SSL в защите передаваемых данных. Что же касается внедрения решений, обеспечивающих расшифровку анализ и повторное шифрование данных, то здесь следует проявлять большую осторожность: по сути речь идет об атаке “человек посередине”. Такой подход компрометирует основы концепции сквозного шифрования, и потенциально представляют значительную угрозу конфиденциальности как таковой».» ***(Самое распространенное шифрование интернет-трафика делает пользователей беззащитными перед хакерами // Goodnews.ua (http://goodnews.ua/technologies/samoe-rasprostranennoe-shifrovanie-internet-trafika-delaet-polzovatelej-bezzashhitnymi-pered-xakerami/). 04.04.2019).***

***

«В четверг, 4 апреля, в мире празднуют День интернета. Уже тяжело представить, как раньше люди жили без доступа к всемирной сети. Существование интернета упрощает нам жизнь, расширяет кругозор и дает возможность активно развиваться не только человеку, но и целым компаниям. Однако иногда случаются хакерские атаки, которые способны повлечь за собой массу убытков и потерь. О самых массовых кибератаках пишет kaspersky.ru.

WannaCry…

NotPetya/ExPetr: самая дорогая атака за всю историю…

Dark Hotel: шпионы в нумерах…

Mirai: падение интернета…» ***(Наталия Клюева. День интернета: топ-5 кибератак десятилетия // ООО "Национальные информационные системы" (https://podrobnosti.ua/2291662-den-interneta-top-5-kiberatak-desjatiletija.html). 04.04.2019).***

***

«Эксперты обнаружили новый сервис для аренды вымогательского ПО. В отличие от RaaS-платформ, портал позволяет скачать исходный код зловреда, чтобы доработать его функциональность и затруднить обнаружение.

За $500 злоумышленники получают доступ к вредоносному ПО и панели управления текущими кампаниями. Сам вымогатель написан на C++ и может поражать весь набор ОС от Windows XP до Windows 10. Пользовательские данные блокируются с применением комбинированного шифрования на основе алгоритма AES и публичных RSA-ключей.

Создатели сайта рассказали журналистам, что предоставляют своим клиентам обучение по работе с исходным кодом вымогателя. В пакет ПО также входит утилита-декриптор, которая возвращает файлы в изначальный вид.

С появлением первых жертв злоумышленники получают возможность в реальном времени контролировать ключевые параметры кампании через онлайн-панель. На этой странице отображается процесс шифрования, географическое распределение зараженных хостов, их ОС, статус оплаты. Здесь же преступник может установить своим жертвам индивидуальные суммы выкупа или связаться с ними через чат.

По словам экспертов, создатели портала сделали ставку на удобство и скорость работы. На странице с описанием разработчики сервиса отмечают его низкую требовательность к ресурсам и современный плоский дизайн. При этом, поскольку сайт не предлагает RaaS, услуги хостинга не предоставляются.

Эксперты ожидают, что многие кибервымогатели воспользуются возможностью создать собственный зловред. Это может привести к появлению множества уникальных шифровальщиков, которые объединят в себе функции сразу нескольких представителей семейства. Такой подход затруднит автоматическое обнаружение вымогательского ПО в системе — сделать это смогут только системы с продвинутой поведенческой аналитикой…» ***(Dmitry Nazarov. В Сети появился конструктор вымогательского ПО // Threatpost (https://threatpost.ru/hackers-sell-new-ransomware-service/32435/). 22.04.2019).***

***

«Эксперты Confiant обнаружили вредоносную рекламную кампанию, ориентированную на iOS-устройства. Злоумышленники встраивали нежелательный код в легитимные баннеры, что позволило им за пять дней направить на опасные сайты миллионы пользователей.

Организаторы атак воспользовались уязвимостью в iOS-версии Chrome, которая позволяет совершить побег из песочницы. В результате преступники

смогли показывать пользователям всплывающие рекламные баннеры со ссылками на мошеннические страницы и площадки с вредоносным ПО. Все эти сайты были размещены в доменной зоне .world.

Эксперты подчеркнули, что атаки коснулись только Chrome для iOS-устройств. Нативный браузер Apple, с которым Chrome делит движок WebKit, также не попал под удар. Это позволило исследователям предположить, что угроза связана с особенностями работы WebKit именно в iOS-приложении от Google.

Особое беспокойство у экспертов вызвал тот факт, что организаторы атак смогли обойти правило ограничения домена (same origin policy). Эта политика запрещает скриптам одного сайта обращаться к сценариям другого ресурса, однако в ходе нынешних атак вредоносные iframe-объекты загружались со сторонних площадок. Исследователи опасаются, что в дальнейшем преступники смогут применить эту же технику для взлома рекламных систем Google AdX и EBDA.

Аналитики обнаружили восемь отдельных кампаний, организованных через 30 поддельных фирм. Вину за произошедшее исследователи возложили на группировку eGobbler, которая уже несколько раз отметилась подобными атаками. Все они приурочены к крупным праздникам США и направлены исключительно на американских пользователей…» ***(Dmitry Nazarov. Американские пользователи iOS пострадали от опасной рекламы // Threatpost (https://threatpost.ru/american-ios-users-suffered-from-malicious-ads/32400/). 18.04.2019).***

***

«ESET предупреждает о новой фишинговой рассылке, направленной на пользователей популярного видеосервиса.

Мошенники отправляют от имени Netflix сообщение, где просят подтвердить учетную запись пользователя. В письме утверждается, что это позволит избежать блокировки аккаунта из-за зафиксированной подозрительной активности.

После нажатия кнопки «Обновить» пользователь перенаправляется на фальшивую страницу, которая имитирует дизайн официального сайта Netflix.

При этом URL портала не только не соответствует реальному адресу видеосервиса, но даже не содержит название Netflix. Экспертам ESET удалось установить, что домен привязан к бесплатному хостингу, расположенному в ОАЭ.

После открытия интернет-ресурса пользователь должен ввести логин и пароль. Независимо от того, какие данные будут введены, пользователь все равно будет переброшен на форму ввода данных кредитной карты.

Эксперты ESET полагают, что целью атаки является кража личных и банковских данных с последующей перепродажей на черном рынке (такие сведения стоят не менее 45$ или 2800 рублей), а также для совершения целевых атак в будущем…» ***(Обнаружена атака на пользователей Netflix // IKSMEDIA.RU (http://www.iksmedia.ru/news/5583046-Obnaruzhena-ataka-na-polzovatelej.html). 22.04.2019).***

***

«Крупнейший американский регистратор доменов и хостинг-провайдер GoDaddy аннулировал более 15 тыс. поддоменов, перенаправляющих

посетителей на сайты торговцев БАДами, стимуляторами работы мозга и другими сомнительными препаратами.

Мошеннические редиректы выявил эксперт Palo Alto Networks Джефф Уайт (Jeff White), который два года изучал партнерские программы по продвижению шарлатанских снадобий через спам. За это время ему удалось обнаружить свыше 21,6 тыс. сайтов-редиректоров и 689 связанных с ними страниц с целевой рекламой.

Примечательно, что все URL спамеров представляли собой короткие ссылки; многие из них были сгенерированы на специализированном сервисе GoDaddy. В названиях соответствующих сайтов прослеживался некий шаблон — как будто кто-то открыл англоязычный словарь и выбирал по одному слову на каждую букву. По мнению Уайта, имена в данном случае создавались автоматизированными средствами.

Исследователь насчитал более 4 тыс. поддоменов, отвечавших этому шаблону, и 3 тыс. уникальных доменов второго уровня. Большинство из них вызывалось по сокращенным ссылкам GoDaddy.

Расследование показало, что все поддомены, используемые в рамках рекламных кампаний, были созданы через взлом учетных записей клиентов хостинга, и этот процесс тоже мог быть автоматизирован. Таким образом была создана целая сеть редиректоров для привлечения пользователей потенциальных покупателей на опекаемые спамерами площадки. Чтобы повысить эффект от таких визитов, пользователя вначале «подогревали» рекламой: лендинг-страницы пестрели восторженными отзывами звезд телеэкрана и кинематографа о «чудодейственных» свойствах пилюль для снижения веса и обретения стройной фигуры.

Все ссылки на такой странице, по словам Уайта, вели непосредственно на сайт, торгующий хваленым товаром. Здесь визитеру предлагали самому опробовать «панацею», оплатив только доставку. В то же время мелким шрифтом в подвале указывалось, что в пакет входит подписка (с абонентской платой), которая будет автоматически возобновляться до тех пор, пока клиент ее не отменит.

Исследователь поделился с GoDaddy своими находками и даже написал несколько скриптов, чтобы облегчить идентификацию и блокировку мошеннических сайтов. Провайдер также сбросил пароли к затронутым аккаунтам, уведомив владельцев об инциденте.» ***(Maxim Zaitsev. GoDaddy вычистил редиректоры мошенников // Threatpost (https://threatpost.ru/godaddy-takes-down-subdomains-used-in-scam-campaigns/32501/). 29.04.2019).***

***

«Эксперты Check Point обнаружили серию атак, направленных на государственных служащих сразу нескольких стран. Злоумышленники использовали вредоносные документы Excel и скомпрометированную версию TeamViewer, чтобы обеспечить себе полный доступ к компьютерам жертв.

Под удар попали сотрудники финансовых ведомств и посольств Бермудских островов, Гайаны, Кении, Италии, Либерии, Ливана и Непала. Специалисты затрудняются определить цели организаторов кампании. Пока в качестве основной

версии эксперты называют хищение денежных средств. В ее пользу говорит тот факт, что все жертвы были тщательно отобраны и так или иначе имели отношение к финансовым операциям своих организаций.

Заражение происходило через вредоносный XLSM-документ, замаскированный под секретные материалы Государственного департамента США. Если при открытии файла пользователь разрешал работу макросов, из таблицы выгружался зашифрованный код для скачивания остальных компонентов — легитимной программы AutoHotkeyU32 и рабочего скрипта к ней.

Этот сценарий обращался к удаленному серверу за дополнительными модулями, которые исполнялись через ту же программу. Их функции позволяли операторам получать с зараженных машин скриншоты и системную информацию, загружать и устанавливать на компьютер TeamViewer вместе с вредоносной DLL-библиотекой. Эксперты обнаружили в ее коде изменения, которые скрывают программу от жертвы и позволяют исполнять полученные извне файлы EXE и DLL.

По неизвестным причинам на момент обнаружения атак хранилище скриншотов было доступно для просмотра. Это позволило аналитикам определить часть жертв кампании и предположить, что злоумышленники атаковали сотрудников финансовых отделов. Позже злоумышленники закрыли эту директорию.

Специалисты отследили развитие данной кампании до 2018 года, отметив при этом, что атаки могли начаться и раньше. За прошедшее время злоумышленники несколько раз меняли свою технику — например, в первых инцидентах вместо документов MS Office они использовали самораспаковывающиеся архивы. Сама вредоносная DLL-библиотека также прошла заметную эволюцию: актуальный вариант с поддержкой скриптов AutoHotKey появился только в 2019 году, а до этого преступники отправляли команды программе вручную.

Аналитики также нашли следы одного из организаторов кампании на подпольных хакерских сайтах. На этих ресурсах он обсуждал технологии, которые позже нашли применение в нынешних атаках. Некоторые куски кода из этих постов полностью совпадают с описанными выше скриптами. Эксперты также обнаружили учетную запись этого пользователя на форуме похитителей платежных данных. Это также свидетельствует о том, что целью нынешней кампании была именно кража денежных средств…» ***(Dmitry Nazarov. Киберпреступники превратили TeamViewer в продвинутого шпиона // Threatpost (https://threatpost.ru/cybercrimanls-used-teamviewer-as-spyware/32449/).*** 23.04.2019).

***

«Швейцарская компания Aebi Schmidt, производитель тяжелой строительной и дорожной спецтехники, в частности – снегоуборочных машин для аэропортов и автомагистралей, стала очередной жертвой атак с использованием зловредов-шифровальщиков.

…в минувший вторник производственные процессы оказались парализованы из-за масштабного компьютерного сбоя, вызванного заражением вредоносным ПО.

Инцидент затронул также систему внутренней электронной почты компании. В результате рабочие были отправлены по домам, а части из них пришлось даже уйти в неоплачиваемые отпуска.

На следующий день представитель Aebi Schmidt Томас Шисс подтвердил факт инцидента. Он уточнил, что производственные процессы уже восстановлены, но констатировал, что системы компании, использующие ОС Windows, «затронуты вирусом». Шисс также добавил, что часть незатронутых атакой систем была отключена, чтобы избежать распространения инфекции. В компании не уточняют, о каком именно вредоносном ПО идет речь, но источники TechCrunch уверяют, что Aebi Schmidt столкнулась с атакой зловреда-шифровальщика. Это далеко не первый случай подобного рода за последнее время. Так, в марте текущего года похожая атака временно прервала производственный цикл норвежской компании Norsk Hydro – одного из крупнейших в мире производителей алюминия, а буквально несколько дней назад зловредом-шифровальщиком были инфицированы системы телеканала Weather Channel, что привело к срыву эфира утреннего телешоу. Аналитики отмечают, что, помимо получения выкупа за разблокировку зашифрованных данных, организаторы таких атак могут преследовать и другие цели. В частности, инциденты с крупными производственным компаниями подрывают их авторитет и влекут за собой снижение биржевой стоимости их ценных бумаг.» ***(Вредоносное ПО парализовало производство компании Aebi Schmidt // IKSMEDIA.RU (http://www.iksmedia.ru/news/5584268-Vredonosnoe-PO-paralizovalo-proizvo.html). 29.04.2019).***

***

Діяльність хакерів та хакерські угруповування

«Пресловутые северокорейские хакеры используют в своих атаках новый троян, предупредили в среду Министерство внутренней безопасности США и Федеральное бюро расследований (ФБР)…

Считается, что Lazarus, BlueNoroff и Hidden Cobra поддерживаются правительством Северной Кореи. Группа организовала ряд громких атак, в том числе ограбление центрального банка Бангладеш и нападения на многочисленные финансовые организации.

За последние несколько лет США связали множество инструментов с деятельностью Hidden Cobra, включая Typeframe, Sharpknot, Hardrain, Badcall, Bankshot, Fallchil, Volgmer, Delta Charlie, Joanap и Brambul.

В отчете по анализу вредоносных программ (MAR), представленном на этой неделе, Министерство и ФБР подробно описывают HOPLIGHT, новый троян, используемый Hidden Cobra. Бэкдор может собирать информацию с зараженных систем и выполнять различные действия в соответствии с инструкциями командно-контрольного сервера (C&C).

Троян состоит из девяти файлов, 7 из них – прокси-приложения, предназначенные для маскировки трафика между вредоносным ПО и удаленными операторами. Прокси-серверы могут генерировать фейковые подтверждения

установления связи TLS, используя действующие общедоступные сертификаты SSL, чтобы скрыть сетевые соединения с вредоносными серверами…

Троян HOPLIGHT может считывать и записывать файлы, подсчитывать системные диски, создавать и завершать процессы, внедрять код в запущенные процессы, изменять параметры реестра, подключаться к удаленному хосту для загрузки и скачивания файлов, а также создавать, запускать и останавливать службы.

Hidden Cobra известна своей нацеленностью на финансовую выгоду, которая отделяет ее от других спонсируемых государством хакерских групп, и считается самой серьезной угрозой для банков. В прошлом году исследователям безопасности удалось связать большинство северокорейских вредоносных программ с этой организацией через повторное использование кода. Некоторые из кампаний Hidden Cobra - Operation Blockbuster, Dark Seoul и Operation Troy, хакеров также обвиняют в атаке WannaCry.» ***(Ирина Фоменко. Северокорейские хакеры используют в своих атаках новый троян // Internetua (http://internetua.com/severokoreiskie-hakery-ispolzuuat-v-svoih-atakah-novyi-troyan). 12.04.2019).***

***

«Группа кибербезопасности Talos компании Cisco вчера информировала о широкомасштабной кампании шпионажа, проводившейся хакерами из команды под названием Sea Turtle против четырёх десятков различных организаций. Особняком эти атаки ставит использовавшийся метод взлома DNS — «адресной книги» Интернета.

Об этой фундаментальной уязвимости Всемирной Сети эксперты кибербезопасности предупреждают уже многие годы, и вот, их худшие опасения оправдались. Хакерам удалось взломать домены верхнего уровня, закреплённые за целыми странами, из-за чего в зоне риска оказался весь трафик по адресам, которые заканчиваются такими суффиксами, как .co.uk или .ru.

Жертвами Sea Turtle стали телекоммуникационные компании, провайдеры Интернет-сервисов и регистры доменных имён, отвечающие за функционирование системы DNS. Но приоритетные цели хакеров, по данным Cisco, это правительственные учреждения, включая министерства внутренних дел, разведывательные, военные и энергетические организации, расположенные в регионах Ближнего Востока и Северной Африки.

Проникнув в систему каталогов Интернета, злоумышленники могли скрытно организовывать атаки через посредника (man in the middle) для перехвата всех данных почтового и веб-трафика своих жертв. Крейг Уильямс (Craig Williams) из Cisco Talos считает, что особую обеспокоенность должна внушать не дерзость этой серии киберпреступлений, а то, что они подрывают фундамент, на котором зиждется доверие к Интернету…

Специалисты Cisco Talos сталкивались со взломом DNS неоднократно: инциденты варьировались от грубой подстановки фальшивых веб-страниц до прошлогодней кампании кибершпионажа, DNSpionage, связываемой с Ираном. Но действия Sea Turtle повышают градус серьёзности таких инцидентов, считают они.

Cisco Talos не смогла определить национальную принадлежность Sea Turtle. Также она отказалась назвать конкретные цели хакеров, перечислив только страны, где те находятся: Албания, Армения, Кипр, Египет, Ирак, Иордания, Ливан, Ливия, Сирия, Турция и ОАЭ. Из доменов верхнего уровня группа официально подтвердила взлом только домена Армении — .am, а из фирм, связанных с управлением DND — шведскую NetNod и калифорнийскую Packet Clearinghouse, которые в феврале сами сообщили о взломе.

Одним и способов остановить распространение взломов инфраструктуры DNS может быть блокировка регистра (registry lock) — серия дополнительных мер аутентификации и оповещения владельцев при попытке смены настроек домена. Однако, по словам Уильямса, многие регистры до сих пор не обеспечивают такой функции, оставляя своих клиентов в состоянии неопределённости.

Всё это значит, что взлом DNS продолжает оставаться растущим фактором угрозы компьютерной безопасности. Даже если Sea Turtle будет остановлена, другие уже увидели действенность их методики и не замедлят скопировать её, предупреждает эксперт Cisco Talos.» ***(Хакеры замахнулись на инфраструктуру Интернета // «Компьютерное Обозрение» (https://ko.com.ua/hakery_zamahnulis_na_infrastrukturu_interneta_128502). 18.04.2019).***

***

«Гонконгский офис правозащитной организации Amnesty International в течение нескольких лет находился под атакой хакеров, предположительно работающих на правительство Китая.

Впервые признаки взлома были обнаружены 15 марта текущего года в процессе миграции IT-инфраструктуры в более защищенные сети в рамках планового обновления. Заподозрив неладное, организация обратилась за помощью к ИБ-экспертам, пишет Agence France-Press.

В ходе расследования специалисты выявили связь между инфраструктурой, использовавшейся для атак на Amnesty International, и предыдущими операциями APT-группы, связываемой исследователями с китайским правительством. Как отметили ИБ-эксперты, за атаками стоит «известная APT-группа», чьи «тактики, техники и процедуры указывают на хорошо подготовленного противника». Поскольку расследование все еще продолжается, название группировки не раскрывается, однако Amnesty International пообещала опубликовать подробный отчет через некоторое время.

Организация связалась с лицами, чьи данные могли оказаться под угрозой из-за кибератак. Amnesty International не сообщила, сколько человек могли пострадать. Финансовые данные затронуты не были, уверены правозащитники.

Руководитель регионального представительства Amnesty International в Восточной Азии Джошуа Розенцвейг (Joshua Rosenzweig) не сомневается, что атаки на организацию финансировались государством. «Мы рассматриваем их как атаки на гражданское общество и некоммерческие организации в целом. Мы не намерены это скрывать. Надеюсь, уже само сообщение о факте кибератаки поможет нам защитить себя», — заявил Розенцвейг.» ***(Правозащитная организация Amnesty***

International в течение нескольких лет находилась под кибератакой // Goodnews.ua (http://goodnews.ua/technologies/pravozashhitnaya-organizaciya-amnesty-international-v-techenie-neskolkix-let-naxodilas-pod-kiberatakoj/). 26.04.2019).

***

«Хакерские атаки, связанные с компрометацией электронной почты (Business Email Compromise – BEC) приобретают все большую популярность и несут все большую угрозу. По данным ФБР США, в прошлом году суммарный ущерб, причиненный ими гражданам и организациям США, превысил 1,2 миллиарда долларов. Классические BEC-атаки удобны хакерам тем, что не требуют серьезной технологической подготовки, ее с успехом заменяют навыки социальной инженерии. Жертва получает сообщение электронной почты с указанием перевести некую сумму на указанный счет – а дальше все зависит от того, насколько убедительным окажется такое сообщение. Изначально киберпреступники атаковали подобным образом финансовые департаменты компаний, выдавая свои письма за распоряжения руководства. Но в последнее время сценарии атак стали намного более разнообразными.

Это подтверждает печальный инцидент в городе Брансуик, штат Огайо, США. Крупнейшая в городе католическая церковь Святого Амвросия ведет масштабные ремонтные работы, средства на которые пожертвовали прихожане. На минувшей неделе компания-подрядчик Marous Brothers, ведущая работы, потребовала срочно внести оплату за последние два месяца. По словам пастора Боба Стека, это сообщение повергло представителей прихода в шок, поскольку церковь исправно осуществляла ежемесячные платежи. Начавшие расследование агенты ФБР быстро установили истину. Два месяца назад неизвестным киберпреступникам удалось в переписке убедить нескольких сотрудников прихода, что компания Marous Brothers сменила банк, и платежи следует осуществлять по новым реквизитам. Таким образом, деньги переводились на счета хакеров, которые при этом даже присылали подтверждения о получении средств от имени строительной компании. В результате у церкви похищены 1,75 миллиона долларов. В настоящий момент приход обратился в страховую компанию в надежде покрыть убытки и расплатиться со строителями.» ***(Хакеры украли 1,75 миллиона долларов, собранных на реставрацию церкви // ООО «Технический центр Интернет» (https://tcinet.ru/press-centre/technology-news/6512/). 30.04.2019).***

***

Вірусне та інше шкідливе програмне забезпечення

«В то время как вирусы и вредоносные программы оставались в топ-10 "вещей на совести CISO", общая угроза неуклонно снижается в течение десяти лет. К сожалению, WannaCry, NotPetya и другие вирусы-вымогатели выдвинули на первый план риски, которые несут современные межсетевые бизнес-системы и взрывной рост неуправляемых устройств…

Эксперты в течение следующих двух-трех лет видят шесть экономически жизнеспособных и самых очевидных применений зараженных ИИ вредоносных программ - все они направлены на оптимизацию эффективности сбора ценных данных, нацеливание на конкретных пользователей и обход технологий обнаружения.

Устранение зависимости от частых коммуникаций C&C. Интеллектуальная автоматизация и базовая логическая обработка могут использоваться для автоматической навигации по скомпрометированной сети, осуществления неповторяющейся и выборочной эксплуатации желаемых типов целей и, после идентификации и сбора данных, передавать информацию на удаленный сервис, контролируемый владельцем вредоносного ПО.

Использование возможностей маркировки и классификации данных для динамического выявления и сбора наиболее интересных или ценных данных. Организации используют эти типы классификаторов данных и машинное обучение для маркировки и защиты ценных активов информации. Но злоумышленники могут использовать ту же эффективность поиска, чтобы найти наиболее важные бизнес-данные реальных пользователей и систем, и уменьшить размер файлов для скрытой эксфильтрации.

Использование когнитивного ИИ для отслеживания трафика электронной почты и чата локального хоста, а также для динамического подражания пользователю. ИИ вредоносного ПО может вставлять новый разговорный контент в электронную почту и чаты с целью социальной инженерии других сотрудников для раскрытия секретов и получения доступа ими к вредоносному контенту.

Использование ИИ для преобразования речи в текст с целью получить секреты пользователя. Через физический микрофон ИИ может преобразовывать все обсуждения в пределах диапазона скомпрометированного устройства в текст. Такой подход позволяет хакерам более избирательно выбирать секреты, что еще больше минимизирует объем данных.

Использование встроенного когнитивного ИИ в приложениях для выборочного запуска вредоносных полезных нагрузок. Поскольку системы когнитивного ИИ могут не только распознавать определенное лицо или голос, но и определять расу, пол и возраст, авторы вредоносных программ знают точно, на кого рассчитаны такие атаки.

Захват поведенческих характеристик пользователей систем. Системы обучения ИИ могу собирать информацию о частоте, характеристике набора текста пользователями, движения мыши, словарный запас, орфографические ошибки и создавать "биопрофайл" человека. Такие "биопрофили" используются для обхода современного поколения систем мониторинга поведения.

Поскольку глубокие нейронные сети, когнитивный ИИ и обученные классификаторы машинного языка невероятно сложны для расшифровки, механизм запуска для злонамеренного поведения невозможно раскрыть с помощью методов обратного инжиниринга. Основой для защиты от этих атак будет обеспечение прозрачности частей организации и постоянного контроля.» ***(Ирина Фоменко. ИИ несет угрозу мировой интернет-аудитории // Internetua (https://internetua.com/ii-neset-ugrozu-mirovoi-internet-auditorii). 10.04.2019).***

***

«Исследователи кибербезопасности создали компьютерный вирус, который может добавлять поддельные опухоли к медицинским изображениям…

В ходе лабораторных испытаний вредоносная программа изменила 70 изображений и сумела обмануть трех радиологов, заставив их поверить, что у пациентов был рак. Измененные изображения также сумели обмануть автоматизированные системы скрининга.

Команда из Израиля разработала это вредоносное ПО, чтобы показать, как легко обойти средства защиты для диагностического оборудования. Программа смогла убедительно добавить ложные злокачественные новообразования к изображениям легких, сделанным на машинах МРТ и КТ.

Исследователи из центра кибербезопасности Университета им. Бен-Гуриона заявили, что вредоносное ПО может также удалять фактические злокачественные образования из файлов изображений, создавать другие поддельные заболевания, в том числе опухоль головного мозга, тромбы, переломы или проблемы с позвоночником.

Эксперты утверждают, что изображения и сканы были уязвимы, поскольку файлы, как правило, не имели цифровой подписи и не шифровались. Это означает, что любые изменения будет трудно заметить. По словам специалистов, уязвимости в безопасности могут быть использованы для сеяния сомнений в отношении здоровья правительственных деятелей, саботажа исследований и участия в террористических атаках.

Кроме того, недостатки в способе защиты больницами и медицинскими центрами сетей могут обеспечить злоумышленникам легкий доступ. Как заявил один из экспертов, медучреждения уделяют слишком мало внимания внутренней обработке данных…». ***(Ирина Фоменко. BBC: интернет-вирус смог дорисовать к скану пациента раковую опухоль // Internetua (https://internetua.com/bbc-internet-virus-smog-dorisovat-k-skanu-pacienta-rakovuua-opuhol). 05.04.2019).***

***

«Создатели IoT-бота Bashlite расширили его возможности: теперь он умеет проводить несколько вариантов DDoS-атак, обладает функциями бэкдора, а также способен удалять клиенты конкурентов.

Очередной вариант Bashlite нацелен на линейку оборудования WeMo компании Belkin и доставляется на устройство посредством эксплуатации уязвимости в прошивке приборов, закрытой в 2015 году Производитель отметил, что угроза актуальна лишь для тех пользователей, которые до сих пор не обновили системное ПО.

Необычный штамм зловреда, также известного как Gafgyt и Qbot, обнаружили специалисты Trend Micro. Они выяснили, что ботоводы используют доступный на сайте Metasploit RCE-эксплойт для проведения атак на умные устройства с API-интерфейсом UPnP.

Оказавшись на гаджете, некоторые образцы Bashlite запускают Telnet-сканер для поиска новых целей и атакуют их, используя подбор паролей. Если взлом удается, на скомпрометированное IoT-устройство загружается дроппер бота Hakai, заимствующего код у Bashlite. На момент исследования попытки экспертов установить клиент еще одной вредоносной сети заканчивались неудачей, поскольку сервер, где хранился дистрибутив, был недоступен.

Как выяснили аналитики, по команде из центра управления обновленный Bashlite может выполнять несколько типов DDoS-атак:

HOLD — удерживает подключение к IP-адресу и порту в течение определенного времени.

JUNK — дополнительно к подключению по целевому IP-адресу отправляет на него случайную последовательность символов.

UDP — массовая отправка UDP-пакетов на сервер жертвы.

STD — то же самое, что UDP.

TCP — массовая передача TCP-запросов.

VSE — атака с усилением DDoS-трафика, нацеленная на исчерпание ресурсов жертвы.

OVH — DDoS-атака с целью обхода средств защиты.

ACK — передача ACK-подтверждений для нарушения канала передачи данных.

GRENADE — осуществление всех типов атак одновременно.

Другая особенность новой итерации — бэкдор, через который злоумышленники могут устанавливать на устройство криптомайнеры и другое ПО, а также удалять активные процессы конкурирующих зловредов…» ***(Egor Nashilov. Ботнет Bashlite нацелился на умные устройства Belkin WeMo // Threatpost (https://threatpost.ru/bashlite-botnet-evolves-targets-belkin-wemo-devices/32115/). 04.04.2019).***

***

«APT-группировка Lazarus взяла на вооружение ранее неизвестный троян HOPLIGHT, способный доставлять на целевое устройство вредоносные модули, изменять реестр и делать инъекции в уже запущенные процессы.

К такому выводу пришли эксперты Департамента внутренней безопасности США и специалисты ФБР, опубликовавшие детальный отчет о зловреде. Они утверждают, что программа использует многоуровневую обфускацию канала передачи данных, чтобы скрыть командные серверы и затруднить обнаружение атаки антивирусными сканерами.

HOPLIGHT состоит из девяти исполняемых файлов, из них семь — прокси-приложения для маскировки трафика между инфицированным компьютером и центром управления. ИБ-специалисты выяснили, что троян использует легитимный SSL-сертификат южнокорейского поисковика Naver для генерации фальшивых TSL-рукопожатий и сокрытия канала передачи данных с жестко заданными IP-адресами хостов.

Вредоносные компоненты могут:

– Подключаться к удаленному серверу.

– Скачивать файлы с целевой машины и доставлять на нее полезную нагрузку.
– Вести подсчет системных дисков.
– Создавать и завершать процессы.
– Вносить изменения в системный реестр.
– Перемещать, читать и изменять файлы.
– Внедрять код в активные процессы.
– Запускать и останавливать службы в рамках ОС.

Исследователи обнаружили, что один из компонентов HOPLIGHT загружает в скомпрометированную систему несколько программных интерфейсов, связанных с тулкитами, для атак Pass-The-Hash. Такие вредоносные инструменты предназначены для авторизации на удаленном сервере, а также кражи пользовательских паролей и другой учетной информации. Помимо этого, зловред собирает и передает операторам данные о версии ОС, метках дисков и системном времени…» ***(Egor Nashilov. Злоумышленники из Lazarus вооружились трояном HOPLIGHT // Threatpost (https://threatpost.ru/lazurus-group-brings-into-play-hoplight-trojan/32253/). 12.04.2019).***

***

«Специалисты Palo Alto Networks/Unit 42 обнаружили масштабную кампанию по распространению трояна удаленного доступа RevengeRAT. Для обхода защитных решений при передаче вредоносных файлов злоумышленники использовали сайты Blogspot, Pastebin и сервис Bit.ly. Намерения преступников пока неизвестны, их целями являются организации из стран Ближнего Востока, Азии, Европы и Северной Америки.

Эксперты изучили сообщение, присланное якобы от крупного финансового учреждения. В теме письма злоумышленники сообщали о блокировке учетной записи. Во вложении находился файл в формате .doc, в котором помещалось изображение с просьбой разрешить запуск макросов.

Когда жертва выдавала это разрешение, на компьютер методом внедрения шаблона скачивался OLE-файл с внешнего сервера. Встроенные в него макросы загружали Excel-документ с обфусцированным кодом, который расшифровывал и открывал URL злоумышленников.

Ссылка вела на страницу сайта Blogspot и была сокращена с помощью Bit.ly. Оттуда с помощью встроенного приложения mshta в систему жертвы проникал вредоносный JavaScript. Скрипт пытался удалить список сигнатур Защитника Windows и приостановить его работу, а также отключить безопасный режим в Word, PowerPoint и Excel. После этого происходила загрузка исполняемых файлов с сайта Pastebin.

В качестве полезной нагрузки выступала одна из версий трояна RevengeRAT под названием Nuclear Explosion. В результате злоумышленники получали удаленный доступ к зараженным системам и могли управлять файлами, процессами, службами и реестром Windows, а также отслеживать IP-адрес жертвы, регистрировать нажатия клавиш, сбрасывать пароли и даже использовать веб-камеру устройства…» ***(Dmitry Nazarov. RAT-зловред распространяется через***

сайты Blogspot и Pastebin // Threatpost (https://threatpost.ru/rat-spreads-through-blogpost-and-pastebin/32426/). 20.04.2019).

***

«Эксперты Trend Micro обнаружили криптоджекинговую кампанию, которая объединила в себе несколько вредоносных PowerShell-скриптов и эксплойт EternalBlue. Атаки злоумышленников направлены на пользователей в странах Азиатско-Тихоокеанского региона.

Для доставки майнера XMrig на компьютеры жертв организаторы кампании используют специфический загрузчик с целым набором вредоносных функций. Первым делом он отправляет организаторам кампании MAC-адрес зараженной машины и данные об установленном защитном ПО. Далее программа скачивает PowerShell-скрипт, который догружает дополнительные модули. Эксперты отмечают, что в основном это новые копии зловреда.

Загрузчик уточняет, какие компоненты отсутствуют на компьютере жертвы, и устанавливает их актуальные версии. После этого зловред отправляет операторам расширенные данные об устройстве, включая имя машины, версию ОС и информацию о видеопамяти.

«Хотя эти данные могут показаться не слишком ценными, они позволяют четко идентифицировать конкретный компьютер, — подчеркивают исследователи. — В дальнейшем с их помощью преступники смогут отслеживать активность пользователей».

Криптомайнер XMrig также разворачивается на компьютере с помощью PowerShell. Примечательно, что код на загрузку и запуск зловреда встроен внутрь opensource-скрипта — это позволило преступникам не использовать дополнительный файл. Эксперты также нашли в коде дроппера отсылку еще к одному исполняемому компоненту, но изучить его не удалось, поскольку на момент обнаружения соответствующий URL был неактивен.

Программа эффективно распространяется по корпоративной сети, пытаясь авторизоваться с помощью вшитых паролей. На пораженных компьютерах она меняет настройки брандмауэров таким образом, чтобы те сами скачивали и запускали дистрибутив зловреда. Отдельный блок паролей обеспечивает возможность взлома SQL-баз.

В дополнение к слабым учетным данным обнаруженный загрузчик применяет технику pass the hash, авторизуясь на удаленных серверах с помощью хешированных паролей, хранящихся на зараженных компьютерах. За эту функцию отвечает бинарный Python-файл, который скачивает и запускает PowerShell-версию легитимной утилиты Mimikatz. В случае успеха этот компонент запускает передачу файлов через SMB-протокол, используя доступный в Сети скрипт Invoke-SMBClient.

Если же первые два способа не дают ожидаемый результат, программа выполняет эксплойт EternalBlue. Эта брешь SMB-протокола ранее спровоцировала эпидемии WannaCry и Petya, после чего ее взяли на вооружение операторы самых разных зловредов…» ***(Dmitry Nazarov. XMrig атакует через PowerShell-скрипты***

и EternalBlue // Threatpost (https://threatpost.ru/xmrig-attacks-through-powershell-and-eteranlblue-exploit/32275/). 15.04.2019).

***

«Специалисты компании Bitdefender обнаружили новый многофункциональный руткит Scranos. Зловред распространяется под видом пиратских программ для работы с видеофайлами и электронными книгами, маскируется под антивирусные продукты и драйверы. Исследователи отмечают, что многие компоненты пока что находятся в разработке. Однако его возможности уже позволяют преступникам похищать платежные данные пользователей онлайн-сервисов и подписывать жертв на YouTube-каналы.

Первая информация о Scranos появилась в этом году. Восьмого января ИБ-исследователи из Tencent Threat Intelligence Center сообщили о результатах проверки некоторых компонентов руткита. Самые ранние из обнаруженных образцов были созданы в ноябре 2018 года.

Чтобы проникнуть на устройство жертвы, Scranos маскируется под легитимные и взломанные версии приложений. Более чем в половине случаев зловред оказывается на компьютерах пользователей Windows 10, но работать может и в других версиях ОС вплоть до XP.

Под видом искомой программы на устройство жертвы попадает дроппер и похититель паролей. После запуска он отправляет сведения о компьютере на внешний сервер и извлекает файлы cookie и учетные данные жертвы из браузеров Google Chrome, Firefox, Edge, Opera, Baidu Browser и Яндекс.Браузер. Помимо этого, к злоумышленникам попадают платежные сведения и другая информация из учетных записей Facebook, Amazon и Airbnb.

Затем дроппер устанавливает руткит и прочие модули. Scranos способен рассылать с захваченных аккаунтов APK-файлы контактам пользователя и запросы на добавление в друзья в Facebook. Отдельный модуль зловреда подписывает жертву на различные YouTube-каналы.

Кроме того, Scranos похищает данные из аккаунтов Steam, устанавливает рекламное ПО, а также проигрывает рекламу или видео с YouTube через браузер на устройстве жертвы. Иногда преступники используют зараженные компьютеры для тестирования новых компонентов.

Эксперты отмечают, что зловред недавно вышел за пределы Китая и пока не получил в других странах широкого распространения. Кроме жителей Поднебесной жертвами Scranos чаще всего становятся пользователи из Индии, Румынии, Бразилии, Франции, Италии и Индонезии, — пока пострадавших менее пяти тысяч.

Некоторым экспертам Scranos напоминает вредоносную программу Zacinlo, которая активно распространялась летом прошлого года. Зловред открывал рекламные окна и перехватывал интернет-трафик на зараженных устройствах. Чтобы скрыть следы его присутствия в системе, злоумышленники также внедряли на устройство жертвы руткит.» ***(Dmitry Nazarov. Руткит Scranos крадет пароли и платежные данные жертв // Threatpost (https://threatpost.ru/scranos-rootkit-steals-passwords-and-financial-data/32380/). 18.04.2019).***

***

«Операторы трояна Emotet стали рассылать свой зловред в электронных сообщениях пользователей, украденных с его помощью. Новый способ распространения позволяет преступникам обходить спам-фильтры и усыплять бдительность жертв.

Многофункциональный троян Emotet входит в пятерку самых распространенных зловредов по итогам 2018 года. Его функции включают кражу данных с зараженных компьютеров и загрузку стороннего ПО. Эксперты оценивают охват этого трояна в сотни тысяч пользователей — точное число остается неизвестным, поскольку зловред может скрытно перемещаться по IT-инфраструктуре.

О новой тактике распространителей Emotet сообщили эксперты сразу нескольких ИБ-компаний. По их словам, злоумышленники начали подготовку к кампании еще в ноябре 2018 года, когда их троян научился красть электронные письма. Специалисты сразу предположили, что преступники намерены применить эти данные для шпионажа или направленных атак.

Как выяснилось в последние недели, письма используются для доставки Emotet участникам переписки. Расчет построен на том, что адресаты вредоносных рассылок скорее откроют сообщение от знакомого отправителя, особенно если оно продолжает начатую ранее тему.

Злоумышленники оставляют текст старых писем без изменений, добавляя лишь пару слов с призывом открыть приложенную ссылку или Word-документ с вредоносным макросом.

Исследователи сообщают о двух волнах кампании, в которых используются письма на английском и немецком языках. Под первый удар попали пользователи в Германии, Канаде, США и Японии, второй пришелся на Мексику и страны Южной Америки. По мнению экспертов, в настоящий момент на этих атаках сосредоточены основные усилия операторов Emotet. Об этом говорит тот факт, что преступники задействовали мощности обоих своих серверных кластеров — в обычных условиях они работают поочередно.

Хотя основной целью злоумышленников остается расширение охвата Emotet, специалисты призывают не забывать об угрозе пользовательской конфиденциальности. Данные из украденных сообщений по-прежнему можно использовать для шпионажа и подготовки направленных атак…

Исследователи призывают пользователей с осторожностью относиться даже к сообщениям знакомых отправителей.

…операторы Emotet внесли несколько новшеств в технологию компрометации переписки. Так, северокорейским преступникам приходилось взламывать каждый аккаунт отдельно, а операторы Ursnif сами сочиняли текст писем. В отличие от них, организаторы нынешних атак автоматизировали свою кампанию как на этапе хищения писем, так и при рассылке вредоносных сообщений и использовали подлинные электронные сообщения.» ***(Dmitry Nazarov. Троян Emotet использует старые письма пользователей // Threatpost (https://threatpost.ru/emotet-uses-previous-email-conversations/32272/). 15.04.2019).***

***

«Шон Диллон (Sean Dillon), исследователь кибербезопасности из фирмы RiskSence, сообщил о создании вредоносного ПО SMBdoor, относящегося к категории бэкдоров – программ, открывающих несанкционированный доступ в заражённую ими систему.

SMBdoor замаскирован под драйвер ядра Windows, после установки использует недокументированные возможности API в процессе srvnet.sys и регистрирует себя обработчиком соединений SMB (Server Message Block).

Это концептуальное ПО не привязывается к каким-либо локальным сокетам и открытым портам, не подключается к имеющимся функциям, оставаясь практически необнаружимым для многих антивирусных систем.

Примером для автора SMBdoor служили вредоносные импланты DoublePulsar и DarkPulsar, созданные в АНБ и обнародованные печально знаменитой группой хакеров Shadow Brokers в начале 2017 г.

В отличие от этих программ, экспериментальный бэкдор Диллона имеет ряд ограничений, препятствующих использованию его в преступных целях. Обойти их в принципе можно, сообщает исследователь, но цель не будет оправдывать затраченных усилий.

Автор рассчитывает, что его «невидимая» программа вызовет интерес в академической среде и у производителей средств обнаружения вторжений, позволив улучшить безопасность пользователей Windows благодаря более эффективному детектированию угроз SMBdoor, DoublePulsar и DarkPulsar.» ***(Экспериментальный «невидимый» бэкдор создан по образу шпионского ПО АНБ // Компьютерное Обозрение (https://ko.com.ua/jeksperimentalnyj_nevidimyj_bjekdor_sozdan_po_obrazu_shpionskogo_po_anb_128577). 226.04.2019).***

***

«Эксперты кибербезопасности, расследующие деятельность FIN7, одной из самых опасных и успешных хакерских групп, давно пытались заполучить исходный код, созданного группой банковского трояна Carbanak, но им приходилось довольствоваться неудобной для анализа скомпилированной версией этого вредоносного ПО.

Однако в апреле 2017 г., Ник Карр (Nick Carr) из фирмы FireEye, обнаружил на бесплатном сервисе антивирусного анализа VirusTotal два архива с исходниками Carbanak, загруженные туда с российского IP-адреса.

Теперь, спустя два года, сотрудники FireEye Майкл Бейли (Michael Bailey) и Джеймс Беннетт (James T. Bennett), начали публикацию серии блогов, Carbanak Week, в которых знакомят общественность с результатами анализа кода этого ПО.

Долгая задержка объясняется большим объёмом работы. Обычно, исходники вирусов содержат не более нескольких десятков файлов, но архивы Carbanak общим размером 20 МБ включали 755 файлов с 39 двоичными модулями и 100 тысячами строк кода.

Группировка FIN7 прекратила существование после того как, в апреле 2018 года, в Испании был арестован её главарь, а в августе, украинской полицией

задержаны ещё трое подозреваемых. Тем не менее, атаки Carbanak на банковский сектор, общий ущерб от которых оценивают в миллиард евро, не прекратились. По сведениям из многих источников, FIN7 просто распалась на несколько команд меньших размеров.» ***(Опубликованы результаты анализа кода опасного банковского трояна Carbanak // Компьютерное Обозрение (Опубликованы результаты анализа кода опасного банковского трояна Carbanak). 24.04.2019).***

***

«По свидетельству Trend Micro, обновленный Linux-зловред AESDDoS способен не только проводить DDoS-атаки, но также загружать майнер криптовалюты на зараженное устройство. Более того, его доставка на устройства ныне осуществляется с помощью эксплойта для Confluence Server.

Критическая уязвимость в приложении для совместной работы, получившая идентификатор CVE-2019-3396, возникла из-за ошибки в коде модуля Widget Connector. Использование бреши не требует аутентификации и позволяет удаленно выполнить произвольный код в системе. Соответствующий патч был выпущен 20 марта, а через три недели в открытом доступе появился PoC-эксплойт, который злоумышленники почти сразу взяли на вооружение.

Вредоносная программа AESDDoS, известная также как Dofloo, MrBlack и Spike, появилась на интернет-арене в 2014 году. Злоумышленники неоднократно создавали на ее основе ботнеты для проведения DDoS-атак, заражая в основном маршрутизаторы.

Как выяснили исследователи, распространяемый посредством эксплойта новый вариант DDoS-бота попадает на устройство не сразу. Вначале удаленно выполняется шелл-команда на загрузку и запуск вредоносного сценария командной оболочки. Тот, в свою очередь, загружает другой шелл-скрипт, который уже устанавливает AESDDoS.

Анализ показал, что обновленный зловред владеет несколькими техниками DDoS, в том числе SYN flood, UDP flood и TCP flood. Проникнув в систему, он модифицирует файл rc.local, чтобы обеспечить свой автозапуск при перезагрузке системы. После запуска AESDDoS собирает информацию о зараженном устройстве (модель, процессор, сетевые интерфейсы, запущенные процессы), шифрует ее AES-ключом и отправляет на командный сервер. Оттуда же он получает шифрованные команды на проведение DDoS-атаки или загрузку криптомайнера…» ***(Maxim Zaitsev. Боты AESDDoS раздаются через уязвимость в Confluence Server // Threatpost (https://threatpost.ru/confluence-server-exploited-to-amass-aesddos-botnet/32516/). 30.04.2019).***

***

«Лондонский суд приговорил киберпреступника, причастного к вымогательской кампании, к шести годам и пяти месяцам лишения свободы. Как установило следствие, начиная с 2012 года Зейн Кайзер (Zain Qaiser) получил свыше 700 тыс. фунтов стерлингов выкупа от граждан более чем 20 стран мира.

Подсудимый скупал рекламный трафик на порносайтах и размещал на них вредоносные баннеры. Для коммуникации с агентствами, которые распоряжаются этими ресурсами, Кайзер использовал поддельные документы и фирмы-однодневки. По словам правоохранителей, знание рекламного рынка и владение приемами социальной инженерии позволило преступнику выглядеть убедительно в глазах контрагентов.

Нажав на баннер Кайзера, пользователи попадали на сайт, где был размещен эксплойт-пак Angler. Набор вредоносных программ проверял систему на наличие определенных уязвимостей и в случае успеха загружал на компьютер зловреда, в частности блокировщик Reveton.

Первые атаки этого зловреда исследователи заметили еще в 2012 году. Тогда зловред занимался исключительно вымогательством. Позже в процессе эволюции Reveton приобрел шпионские функции и научился скрытой добыче криптовалюты. Принцип работы блокировщика при этом не поменялся — программа закрывала доступ к зараженной системе и показывала уведомление якобы от лица правоохранительных органов о том, что на устройстве обнаружены следы преступной деятельности. Чтобы избежать проблем с законом, пользователю предлагали оперативно заплатить «штраф».

По информации следственных органов, Кайзер требовал у своих жертв выкуп в размере $300–1000, а общее количество заражений насчитывает миллионы машин. Полученные средства преступник выводил через цепочку платежных систем с привлечением сообщников-мулов, которые обналичивали и переводили выручку в криптовалюту. Впоследствии официально безработный мошенник тратил прибыль на азартные игры, проституток и предметы роскоши.

Несколько рекламных агентств заподозрили Кайзера в нелегальной деятельности и попытались его остановить, однако он стал шантажировать и запугивать своих контрагентов. Как минимум две компании пострадали от организованных им DDoS-атак, а в одном случае преступник угрожал руководителю агентства доносами о распространении детской порнографии.

Впервые правоохранительные органы задержали Кайзера в середине 2014 года, но тогда предъявить обвинение не получилось из-за отсутствия доказательств. Только к декабрю 2018-го следователи накопили достаточную базу материалов, чтобы арестовать молодого человека за отмывание денег. Всего Кайзеру вменяются 11 типов преступлений, включая мошенничество, махинации с компьютерной техникой и шантаж. Свою вину вымогатель признал…» ***(Julia Glazova. Вымогатель, распространявший Reveton, получил 6 лет тюрьмы // Threatpost (https://threatpost.ru/reveton-malware-distributer-arrested/32201/). 10.04.2019).***

***

«Британский эксперт в области кибербезопасности Маркус Хатчинс (Marcus Hutchins), в заслугу которому ставят нейтрализацию глобальной атаки вымогательского ПО WannaCry в 2017 году, признал себя виновным в создании вредоносных программ.

Он был обвинен в Соединенных Штатах и признал себя виновным в двух пунктах обвинения из десяти, после чего правительство США согласилось отменить оставшиеся пункты во время вынесения приговора.

«Я признал себя виновным в двух обвинениях, связанных с написанием вредоносных программ за несколько лет до моей карьеры в области безопасности», — сказано в заявлении Хатчинса, также известного как MalwareTech.

Хатчинсу грозит лишение свободы на срок до пяти лет по каждому из обвинений и крупный штраф…» ***(Эксперт в области кибербезопасности, застопоривший атаку WannaCry, сознался в создании вредоносных программ // Украина сегодня (http://ukr-today.com/high-tech/389198-jekspert-v-oblasti-kiberbezopasnosti-ostanovivshij-ataku-wannacry-priznalsja-v-sozdanii-vredonosnyh-programm.html). 21.04.2019).***

***

«**Екс-студент на суді зізнався у знищенні даних на 66 компьютерах, які належали коледжу Сент-Роуз в Олбані, штат Нью-Йорк.** Відомо, що хлопець використовував для такої кібератаки пристрій USB Killer ("USB-вбивця")…

За інформацією журналістів, на суді 27-річний громадянин Індії Вішванат Акутота, що проживає в США по студентській візі, зізнався, що 14 лютого 2019 року особисто знищив 59 комп'ютерів з Windows і сім комп'ютерів Apple Mac, а також кілька цифрових моніторів з USB-портами.

При підключенні до комп'ютера або будь-якого пристрою "смертельна флешка" починає накопичувати заряд від джерела в своїх конденсаторах, поки не досягне критичного напруги, а потім різко розряджає його назад в хост-пристрій. Цей стрибок напруги перевантажує і руйнує USB-порт комп'ютера, а також всі його електричні системи, що фізично виводить з ладу комп'ютер…» ***(Студент однією флешкою ліквідував весь університет: подробиці кібератаки століття // znaj.ua (https://znaj.ua/world/227729-student-odniyeyu-fleshkoyu-likviduvav-ves-universitet-podrobici-kiberataki-stolittya). 21.02.2019).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Серьезная уязвимость в WordPress-плагине для отображения рекомендованных постов эксплуатируется злоумышленниками, перенаправляющими посетителей взломанных сайтов на страницу ложной техподдержки. Об этом сообщили специалисты компании Wordfence и эксперты Sucuri. Баг в Yuzo Related Posts позволяет неавторизованному киберпреступнику провести XXS-атаку и разместить вредоносный скрипт на целевом веб-ресурсе. Проблемное расширение уже удалено из репозитория, однако остается установленным на более чем 60 тыс. площадках.

Как выяснили специалисты, создатели плагина допустили ошибку при использовании оператора is_admin() для запуска одной из подсистем программы с административными привилегиями. В результате некорректного применения команды нападающий имеет возможность отправить POST-запрос на целевой сайт и сохранить вредоносный скрипт в параметрах настройки плагина. Модифицированный код будет внедрен на всех страницах веб-ресурса, где отображаются списки рекомендованных публикаций.

Баг был отловлен ИБ-специалистами 30 марта, после чего администрация официального репозитория WordPress заблокировала доступ к загрузке плагина. Тем не менее тысячи сайтов по-прежнему используют разработку и остаются уязвимыми для атаки. Этим не преминули воспользоваться злоумышленники, нападающие на веб-ресурсы с установленным расширением.

По данным экспертов, атаки начались 10 апреля этого года, после того как PoC-эксплойт утек в Сеть. В рамках текущей кампании киберпреступники внедряют на сервер скрипт, переадресующий посетителя на мошеннический сайт, однако ИБ-специалисты отмечают, что при помощи той же техники можно произвести дефейс или скомпрометировать учетные записи администратора.

Домен и IP-адрес сервера, на котором размещен вредоносный скрипт, совпадает с данными площадки, задействованной в атаках на пользователей плагинов Social Warfare и Easy WP SMTP. Кампания, эксплуатирующая бреши в этих расширениях, была зафиксирована в начале марта, после того как информация о багах утекла в Интернет. Разработчики выпустили обновления для своих продуктов, однако злоумышленники продолжили сканировать Сеть в поисках непропатченных сайтов.» ***(Maxim Zaitsev. Киберпреступники используют 0-day плагина Yuzo Related Posts // Threatpost (https://threatpost.ru/yuzo-related-posts-zero-day-vuln-used-to-mass-hack-wordpress-sites/32255/). 12.04.2019).***

***

«Упродовж п'яти останніх років в Android існувала небезпечна уразливість, яка ставила під загрозу особисте життя користувачів мільйонів смартфонів по всьому світу.

Експерт в області кібербезпеки компанії Positive Technology знайшов ваду в Андроїді, відкриває зловмисникам доступ до конфіденційної інформації. Втім, нічого дивного, так як Google просто не здатна протистояти вірусам.

Уразливість в Android зачепила всі мобільні пристрої під управлінням від Android 4.4 KitKat і до Android 9.0 Pie. Вона ховалася в компоненті WebView і могла використовуватися для установки шкідливих програм, а також виїмки особистих даних користувача. Це означає, що хакери могли непомітно отримувати доступ до особистої інформації користувачів, і робити це протягом декількох років. Звичайно ж, кількість Android-пристроїв вже давно перевищила 1 млрд, і всі вони могли бути зламані хакерами.

Лякає своєю простотою спосіб отримання всієї особистої інформації зловмисниками – достатньо просто відкрити посилання на миттєве додаток з шкідливою функціональністю і спровокувати її перехід. Зробити це дуже просто - достатньо всього лише відправити фішингове повідомлення на електронну пошту, і вірус зробить все сам…» ***(У роботі Android виявили масову вразливість: всі смартфони під загрозою // znaj.ua (https://znaj.ua/techno/223225-u-roboti-android-viyavili-masovu-vrazlivist-vsi-smartfoni-pid-zagrozoyu). 02.04.2019).***

***

«В 2018 году Microsoft заплатила за найденные в своих продуктах уязвимости в общей сложности более 2 млн долларов. Речь идет о программах баг-баунти (Bug Bounty, дословно с английского — премия за ошибку, программа поощрения за найденные проблемы в сфере кибербезопасности).

Чтобы еще сильнее стимулировать пользователей искать ошибки в программном обеспечении Microsoft, компания ускорила выплаты. Теперь участники баг-баунти могут получать вознаграждения через платежную систему PayPal и перечислять их на свои банковские счета более чем в 30 странах мира.

Кроме того, за свою работу хакеры могут получить премию в виде криптовалюты. Microsoft не уточняет, какой именно цифровой валютой корпорация будет оплачивать найденные уязвимости.

Microsoft также увеличивает вознаграждения для хакеров. Например, максимальные выплаты в программе Windows Insider Preview повышены с 15 до 50 тысяч долларов. В программе Microsoft Cloud (участники ищут ошибки в Azure, Office 365 и т. п.) предел бонусов возрос с 15 до 20 тысяч долларов…» ***(Microsoft заплатила 2 млн долларов за найденные уязвимости в своем ПО // Goodnews.ua (http://goodnews.ua/technologies/microsoft-zaplatila-2-mln-dollarov-za-najdennye-uyazvimosti-v-svoem-po/). 12.04.2019).***

***

«Компания, занимающаяся кибербезопасностью, Check Point Software Technologies из Тель-Авива сообщила о найденной уязвимости защиты телефонов Xiaomi.

Изучив приложение безопасности «Guard Provider» в телефонах марки Xiaomi, Check Point Software нашли недостаток, который мог пропускать злоумышленников данным владельцев смартфонов.

Слабое место ПО китайских смартфонов позволяло хакерам подключаться к тому же Wi-Fi-соединению, что и пользователь телефона данной марки, и перехватывать его данные с целью их кражи или повреждения.

Израильская компания уведомила производителей Xiaomi о найденной прорехе в ПО и те выпустили обновление, исправляющее этот баг…» ***(Израильская кибер-компания выявила брешь в безопасности Xiaomi // Jewishnews (https://jewishnews.com.ua/economics-and-business/izrailskaya-kiber-kompaniya-vyiyavila-bresh-v-bezopasnosti-xiaomi). 05.04.2019).***

***

«В сервере приложений Oracle WebLogic обнаружена брешь, позволяющая злоумышленнику перехватить управление целевой системой. Производитель пока не выпустил заплатку для этого бага, а киберпреступники уже сканируют Интернет в поисках уязвимых машин. ИБ-специалисты, ссылаясь на данные поисковика ZoomEye, заявляют, что под угрозой взлома находятся более 36 тыс. систем.

Аналитики китайской компании KnownSec 404 зафиксировали всплеск обращений к двум компонентам серверов WebLogic. Удаленные злоумышленники искали системы с установленными модулями wls9_async и wls-wsat, один из которых отвечает за выполнение асинхронных операций, а другой входит в контур безопасности. Как выяснили эксперты, недостатки в этих компонентах позволяют атакующему вызвать ошибку десериализации и захватить контроль над системой.

Баг затрагивает все версии WebLogic. Исследователи выяснили, что большинство уязвимых серверов находятся на территории США и Китая. Компания Oracle выпускает обновления безопасности для своих разработок раз в три месяца, поэтому заплатка для этой бреши появится не раньше июля 2019 года. В качестве кременной меры защиты специалисты рекомендуют отключить проблемные компоненты или настроить блокировку внешних обращений к содержимому директорий /_async/ и /wls-wsat/.

Сообщение экспертов KnownSec 404 подтвердили аналитики других ИБ-компаний. Как отмечают специалисты, пока киберпреступники лишь ищут уязвимые системы, но не устанавливают на них вредоносное ПО, хотя в ближайшее время ситуация может перемениться…» ***(Egor Nashilov. Серверы WebLogic содержат незакрытую уязвимость // Threatpost (https://threatpost.ru/oracle-weblogic-zero-day-under-attack/32483/). 26.04.2019).***

***

«Независимый ИБ-исследователь Пол Маррапезе (Paul Marrapese) обнаружил уязвимости в IoT-оборудовании десятков китайских производителей, которые можно использовать для MitM-атак и вмешательства в работу устройств. По подсчетам эксперта, угрозе подвержены более 2 млн IP-камер, умных дверных звонков, радионянь и прочих IoT-устройств.

Проблема содержится в P2P-утилите iLnkP2P, которая позволяет удаленно управлять техникой через мобильное приложение, минуя ограничения брандмауэров. Для подключения пользователи сканируют штрихкод на своем

устройстве или вводят указанный на нем шестизначный код. Для дальнейшей работы авторизация уже не требуется.

Именно это и стало слабым местом данной технологии. По словам Маррапезе, злоумышленникам не составит труда найти уязвимые устройства и перехватить информацию, которую те отправляют на управляющие серверы. Поскольку разработчики не побеспокоились о шифровании этих данных, взломщики могут узнать пользовательский пароль и установить контроль над гаджетом. Это позволит им не только подглядывать за владельцем взломанной камеры, но и создавать обширные IoT-ботнеты наподобие Mirai и его наследников.

Исследователь также напоминает, что подобные устройства могут подолгу работать с заводскими учетными данными и множеством незакрытых уязвимостей в коде. Это избавит злоумышленников от необходимости перехватывать пароль.

По данным Маррапезе, в мире насчитывается более 2 млн гаджетов с этими уязвимостями. Эксперт подчеркнул, что проблема касается только устройств с iLnkP2P — аналогичные программы других разработчиков угрозе не подвержены. Основная часть небезопасных устройств сосредоточена в Китае (39%), на втором месте оказались страны Европы (19%), за ними следуют США (7%)…

В сложившихся условиях владельцам уязвимых устройств стоит прекратить их использование. Другой способ защититься от возможных атак —заблокировать обмен данными по UDP-порту 32100.» ***(Egor Nashilov. В двух миллионах IoT-устройств обнаружена уязвимость // Threatpost (https://threatpost.ru/ilnkp2p-vuln-paves-way-for-new-botnet/32506/). 29.04.2019).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«…Компания Microsoft опубликовала проект нового «фреймворка настроек безопасности», призванного помочь пользователям усилить защиту устройств на базе Windows 10. В руководстве под названием SECCON описаны пять уровней конфигураций безопасности по аналогии с DEFCON - шкалой готовности вооруженных сил США

…новый фреймворк упрощает настройку безопасности, в то же время «предоставляя достаточно гибкости для баланса защиты, производительности и пользовательского взаимодействия.

Компания предлагает следующие уровни настройки безопасности:

Уровень 5. Enterprise security (Корпоративная безопасность) – минимальный уровень настройки безопасности корпоративных устройств.

Уровень 4. Enterprise high security (Высокий уровень корпоративной безопасности) – рекомендуется для устройств, хранящих конфиденциальную информацию.

Уровень 3. Enterprise VIP security (Корпоративная безопасность уровня VIP) – рекомендуется для устройств организаций с большими командами безопасности либо для пользователей, находящихся в группе высокого риска.

Уровень 2. DevOps workstation (Рабочая станция DevOps) – рекомендуется для разработчиков и тестировщиков, находящихся в зоне риска атак, преследующих цель доступа к серверам и системам, содержащим ценные данные или связанные с важными бизнес-операциями. Рекомендации еще дополняются.

Уровень 1. Administrator workstation (Рабочая станция администратора) – в настоящее время рекомендации находятся на стадии разработки.» ***(Microsoft опубликовала руководство по усилению защиты Windows 10 // SecurityLab.ru (https://www.securitylab.ru/news/498769.php). 12.04.2019).***

***

«Некогда надежные компании все чаще подвергаются целевым атакам и теряют доверие партнеров и клиентов из-за утечек данных. Прошлый год стал показательным в этом плане, и многие организации стали пересматривать подход к информационной безопасности.

«В 2018 году общемировые расходы на кибербезопасность составили 114 млрд долл. Это говорит о том, что все произошедшие инциденты и утечки данных — результат не бездействия или игнорирования проблемы, а недостаточной эффективности применяемых механизмов защиты, — заявил Стью Брэдли, вице-президент по безопасности SAS. — На сегодняшний день обычная компания использует более 30 различных продуктов безопасности для защиты своей инфраструктуры и обрабатываемых данных. Ирония в том, что такое лоскутное одеяло из разнообразных систем защиты как раз и способствует росту уязвимости».

Применение разрозненных, изолированных решений в области кибербезопасности может обеспечить лишь фрагментированную картину текущего риска. Отсутствие централизованных средств корреляции и анализа событий безопасности из различных источников может привести к тому, что сложная атака, задействующая различные способы и каналы реализации угроз, останется незамеченной. Обновленное решение SAS Cybersecurity сводит в общую картину данные от разрозненных систем защиты и компонентов корпоративной инфраструктуры и использует возможности машинного обучения и искусственного интеллекта для глубокого анализа происходящих событий и выявления потенциальных инцидентов безопасности.

Как подчеркивается, решение имеет прозрачную архитектуру «белого ящика» и предлагает проверенные и доказавшие свою эффективность аналитические алгоритмы и инструменты, настроенные на решение типовых задач информационной безопасности. Решение «из коробки» включает более 70 аналитических моделей и комплексных правил, направленных на выявление потенциальных угроз, а также обеспечивает возможность разработки новых моделей. Такие модели могут быть разработаны на различных языках программирования, в том числе с использованием открытого ПО, например, с помощью Jupyter Notebook и языка Python. Результатом является точная аналитика, которая выявляет риски безопасности на самом раннем этапе, помогает определить

эффективные способы реагирования на возникающие угрозы, а также варианты оптимизации и приоритеты доработок в текущей системе защиты.

«Организациям нужно больше, чем просто алгоритмы обнаружения угроз. Им нужна комплексная архитектура и единый набор аналитических возможностей для обеспечения безопасности и управляемые процессы защиты сетей», — считает Джон Олцик, главный аналитик Enterprise Strategy Group.

SAS Cybersecurity встраивается в существующую корпоративную инфраструктуру кибербезопасности, помогая организациям применять искусственный интеллект и машинное обучение для обнаружения и расследования событий и инцидентов безопасности. Непрерывный контроль сетевой активности, а также анализ событий, регистрируемых на различных устройствах корпоративной сети, помогает сотрудникам подразделений безопасности обнаруживать и предотвращать несанкционированный доступ к данным и сложные вредоносные атаки.

Решение SAS содержит средства интеграции и готовые описания данных для типовых источников (например, сетевого оборудования, поддерживающего протокол Netflow, систем аутентификации, прокси-серверов, DNS-серверов, DHCP-серверов, конечных точек и др.), а также допускает возможность интеграции с иными корпоративными системами, в т.ч. использующими нестандартные или редкие форматы представления данных…» ***(SAS обновила решения в области кибербезопасности // «Компьютерное Обозрение» (https://ko.com.ua/sas_obnovila_resheniya_v_oblasti_kiberbezopasnosti_128496). 18.04.2019).***

***

«Компания Eset сообщает о выходе новой версии Safetica – решения для предотвращения утечек конфиденциальных данных. Продукт позволяет осуществить комплексный анализ кибербезопасности корпоративной среды и выявить проблемы в защите конфиденциальных данных.

Этот анализ включает оценку:

– количества защищенных корпоративных устройств;
– определение конфиденциальных данных компании;
– безопасных направлений для конфиденциальных файлов;
– разрешенных и запрещенных каналов связи для передачи конфиденциальных данных;
– наличие аномальных или проблемных ситуаций в потоке данных;
– использование опасных программ и веб-сайтов;
– использование ИТ-ресурсов компании.

На основе анализа можно перейти к применению эффективных действий для повышения защиты конфиденциальных данных. Благодаря новой функции в WebSafetica 9.0 администраторы могут быстро и всесторонне определить приоритеты инцидентов безопасности, а также быстро фильтровать данные. Одним кликом мыши можно открыть нужные графики и сделать соответствующие выводы.

Интерактивные диаграммы в продукте позволят сосредоточиться на отклонениях и выходных данных, которые представляют интерес, и интуитивно фильтровать графики для поиска необходимого. Таким образом, Safetica 9.0 поможет точно определить, какие конфиденциальные данные нуждаются в особой защите.» ***(Safetica 9.0 помогает сфокусироваться на важных проблемах безопасности // «Компьютерное Обозрение» (https://ko.com.ua/safetica_9_0_pomogaet_sfokusirovatsya_na_vazhnyh_problemah_bezopasnosti_128531). 22.04.2019).***

***

«Латвийский IT-интегратор Tet (ранее – Lattelecom) разработал тест, который поможет украинским предприятиям определить уровень уязвимости IT-инфраструктуры

В зависимости от результатов тестирования Tet предложит оптимальные варианты защиты информации. Компания предоставляет широкий спектр IT-услуг для бизнеса, в том числе предлагая инновационные IT-решения для повышения кибербезопасности.

Глобальная компьютеризация бизнеса привела к появлению новых способов незаконного получения данных компаний. Эти способы часто используют конкуренты для доступа к конфиденциальной информации, шантажа и нанесения урона репутации предприятия. Из-за повышения уровня IT-угрозы компаниям необходимо уделять больше внимания защите от IT-рисков. Они могут быть результатом как намеренной атаки извне, так и небрежности руководства и сотрудников.

Распространённой угрозой кибербезопасности являются DDoS-атаки - поток ложных запросов от разных хостов, который блокирует сервер нужного ресурса. Также серьезный ущерб наносят компьютерные вирусы. В последнее время повысилась активность вирусов-шифровальщиков, таких как WannaCry, Petya и Trojan. Они представляют особенную опасность, так как с их помощью злоумышленники сперва проникают в инфраструктуру предприятия, а не атакуют ее напрямую.

Информационную угрозу могут представлять и сами сотрудники. По причине халатности или неосведомлённости они могут открыть письмо с вирусом с рабочего компьютера или переслать важное рабочее письмо по ложному адресу. Также владельцы бизнесов иногда пытаются сэкономить на покупке лицензионного ПО, лишаясь технической поддержки компаний-разработчиков.

Для обеспечения и защиты информационной безопасности предприятиям следует в первую очередь сосредоточиться на предотвращении возможных рисков, а не на ликвидации их последствий. Тест от Tet предлагает украинским компаниям дать ответы на 10 вопросов, которые касаются проблем кибербезопасности, и таким образом определить уровень IT-угрозы. Тест можно пройти по ссылке…

После прохождения теста Tet предлагает в течение месяца проверить уязвимость IT-инфраструктуры с помощью системы Nexpose производства Rapid7 - всемирно известного и надежного поставщика услуг, оцененного такими гигантами, как Gartner. Эта система дает возможность провести идентификацию

уязвимости всех IT-устройств компании, определяет уровень критичности рисков и предоставляет рекомендации по их устранению. Кроме того, Tet предлагает защиту от DDoS-атак, а также работает над решениями SIEM (IBM QRadar), а до конца года планирует создать SOC (Security Operations Center)…» ***(Tet разработал тест на определение уровня IT-безопасности бизнеса (ПРЕСС-РЕЛИЗ) // DsNews (http://www.dsnews.ua/society/tet-razrabotal-test-na-opredelenie-urovnya-it-bezopasnosti-05042019180200). 05.04.2019).***

***

«…Национальный институт стандартов и технологий США (The National Institute of Standards and Technology, NIST) выпустил обновление исследовательского набора инструментов (Automated Combinatorial Testing for Software, ACTS), призванное помочь разработчикам сложных критически важных с точки зрения безопасности приложений выявлять потенциально опасные ошибки в своем ПО.

Решение ACTS позволяет разработчикам удостовериться, что их продукты не содержат «одновременные комбинации входных значений», которые могут вызвать серьезную ошибку. В случае критически важных с точки зрения безопасности приложений, реализованных в автомобилях, самолетах, на ядерных объектах и т.д., подобные ошибки могут привести к серьезным последствиям.

Исследователи из NIST в сотрудничестве с Техасским университетом, Adobe и австрийской исследовательской лабораторией SBA Research разработали инструмент под названием Combinatorial Coverage Measurement (CCM), позволяющий тестировать программное обеспечение с тысячами входных переменных. Как отметили в NIST, новое решение позволит не только улучшить безопасность, но и снизить расходы на разработку ПО.

Инструмент CCM уже добавлен в состав набора ACTS. Разработанный SBA Research алгоритм пока официально не включен в состав ACTS, однако разработчики могут запросить его у NIST.» ***(NIST обновил инструмент для поиска ошибок в критически важном ПО // SecurityLab (https://www.securitylab.ru/news/498931.php). 26.04.2019).***

***

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

Балакін С. В. Методи та засоби підвищення достовірності ідентифікації несанкціонованих дій та атак в комп'ютерній мережі : автореф. дис. ... канд. техн. наук : 05.13.05 / Балакін Сергій В'ячеславович ; Нац. авіац. ун-т. - Київ, 2018. - 20 с.

Визначено методи виявлення несанкціонованих дій і атак в комп’ютерній мережі за рахунок використання засобів штучних імунних систем та діагностування на основі теорії Демпстера-Шафера, котрі дають можливості

ефективно протидіяти вторгненням. Досліджено можливості використання операторів імунних систем для моделювання роботи запропонованих методів. На основі цих властивостей запропоновано процедури ідентифікації несанкціонованих дій і атак в комп'ютерній мережі.

Шифр зберігання НБУВ: РА439082

***

Зацеркляний Г. А. Виявлення слідів комп'ютерних інцидентів : [навч. посіб.] / Зацеркляний Г. А. - Харків, 2017. - 360 с.

Звернуто увагу на виявлення і дослідження злочинів, пов'язаних із комп'ютерною інформацією, на методи одержання доказів, які мають форму комп'ютерної інформації, на застосуванні для цього технічних та програмних засобів.

Шифр зберігання НБУВ: ВА829480

***

Освіта і формування конкурентоспроможності фахівців в умовах євроінтеграції : зб. тез доп. за матеріалами II Міжнар. наук.-практ. конф., 25-26 жовт. 2018 р. - Мукачево, 2018. - 489 с.

Зі змісту:

- Бистрова Б. Нормативно-правові засади професійної підготовки фахівців з кібербезпеки у США.

Шифр зберігання НБУВ: ВА829996

***

Піцик Ю. М. Кіберзлочини проти власності: кримінально-правова та кримінологічна характеристика : автореф. дис. ... канд. юрид. наук : 12.00.08 / Піцик Юрій Миколайович ; ПрАТ "ВНЗ "Міжрегіон. акад. упр. персоналом". - Київ, 2019. - 20 с.

Розкрито сутність та надано кримінально-правову характеристику кіберзлочинів. Здійснено класифікацію злочинів проти власності, що можуть вчинятися у кіберпросторі. Узагальнено причини та умови, що сприяють вчиненню кіберзлочинів проти власності. Запропоновано заходи запобігання кіберзлочинам проти власності з урахуванням посилення координаційної діяльності правоохоронних органів.

Шифр зберігання НБУВ: РА438664

***

Суспільство, право, психологія та педагогіка: поступ у майбутнє : зб. матеріалів міжнар. курсант.-студент. форуму "STUDIO ВЕСНА 2017" (Київ, 21 квіт. 2017 р.). - Київ, 2017. - 382 с.

Зі змісту:

- Закорчевна Ганна-Марія В., Мостова А.А. Актуальні питання стратегії кібербезпеки України;
- Мажула Р.О. Соціальні мережі та особиста кібербезпека.

Шифр зберігання НБУВ: ВА830240

***

Технології комплексного захисту інформації в кіберпросторі : навч. посіб. - Чернівці : ЧНУ ім Ю. Федьковича, 2018. - 203 с.

Викладено методологічні основи комплексної інформаційної безпеки підприємств, установ та організацій.

Шифр зберігання НБУВ: ВА830137

***

Тринадцяті юридичні читання. Українська державність: крізь призму часу (до 100 річчя Української національно-демократичної революції 1917-1921 рр.) : матеріали міжнар. наук. конф., 24-25 трав. 2018 р., м. Київ, Україна. - Київ : Вид-во НПУ ім. М. П. Драгоманова, 2018. - 335 с.

Зі змісту:

- Бучма О.В., Гнинюк Р.Ю. Особливості сучасного стану кібербезпеки України;
- Доронін І.М. Парламентський контроль у сфері кібербезпеки.

Шифр зберігання НБУВ: ВА830004

***

Яцишин М.Ю. «Інтернет речей» в системі міжнародно-правової протидії кіберзлочинності / М.Ю. Яцишин // Держава і право. Юридичні науки. - 2018. - Вип. 82. - С. 287-298.

Досліджено проблему міжнародно-правового співробітництва держав у боротьбі з кіберзлочинністю в контексті впровадження новітніх технологій. Аналіз здійснено на прикладі Інтернету речей. Заропоновано включення до міжнародних угод положень про «емерджентні технології».

Шифр зберігання НБУВ: Ж69395/юрид.

***