\

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

№ 3 (березень)

Київ – 2020

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І.Вернадського. – К., 2020. – №3 (березень) . – 92с.

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

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

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

ЗМІСТ

Стан кібербезпеки в Україні 4
Національна система кібербезпеки 6
Правове забезпечення кібербезпеки в Україні 10
Боротьба з кіберзлочинністю в Україні 10
Коронавірус COVID-19 та питання кібербезпеки 12
Міжнародне співробітництво у галузі кібербезпеки 25
Світові тенденції в галузі кібербезпеки 30
Сполучені Штати Америки 37
Російська Федерація та країни ЄАЕС 38
Інші країни 40
Протидія зовнішній кібернетичній агресії 40
Створення та функціонування кібервійськ 41
Кіберзахист критичної інфраструктури 42
Захист персональних даних 43
Кіберзлочинність та кібертероризм 49
Діяльність хакерів та хакерські угруповування 58
Вірусне та інше шкідливе програмне забезпечення 63
Операції правоохоронних органів та судові справи проти кіберзлочинців 70
Технічні аспекти кібербезпеки 74
Виявлені вразливості технічних засобів та програмного забезпечення 74
Технічні та програмні рішення для протидії кібернетичним загрозам 84
Нові надходження до Національної бібліотеки України імені В.І. Вернадського 92

«У видавництві ASC Academic Publishing (штат Невада) вийшла друком наукова монографія «ISCI'2019: Information Security in Critical Infrastructures», одним зі співавторів якої є завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету, д.т.н., професор Олексій Смірнов - повідомляє ЦНТУ: Центральноукраїнський національний технічний університет.

Як розповів професор Олексій Смірнов, дана монографія містить результати багаторічної роботи колективу українських науковців, які працюють над питаннями кібербезпеки (це відома в багатьох країнах «Харківська школа кібербезпеки», до складу якої входять представники декількох університетів). Редакторами монографії виступили представники даної школи, професори Харківського Національного університету імені В.Н. Каразіна Олександр Кузнєцов та Іван Горбенко. Науковці «Харківської школи кібербезпеки» займалися й займаються розробкою стандартів шифрування, які впроваджено в багатьох національних стандартах України щодо захисту інформації. Колектив наукової школи активно публікується як в Україні, так й за кордоном, маючи у своєму доробку значну кількість монографій, журнальних статей, доповідей на конференціях тощо…

Загалом у монографії акумульовано результати досліджень у різних сферах, пов'язаних із безпечним та ефективним функціонуванням критичних інформаційних інфраструктур. У рамках досліджень представлено результати в галузі захисту криптографічної інформації, оптимізації обчислювальних процесів, безпеки технології блокчейну, синтезу дискретних сигналів та моделювання складних інформаційних систем. Основна мета монографії – провести всебічний аналіз проблем безпеки критичної інфраструктури та запропонувати потенційні методи їх вирішення.

Монографія «ISCI'2019: Information Security in Critical Infrastructures» видана в паперовому (ISBN: 978-0-9989826-8-7) та електронному (ISBN: 978-0-9989826-9-4) вигляді. За номером 2019921084 книгу можна буде знайти в Бібліотеці Конгресу США». ***(Науковець ЦНТУ – співавтор виданої в США монографії // "Кіровоград24.com (http://kirovograd24.com/shortly/2020/03/11/naukovets-tsntu-spivavtor-vidanoi-v-ssha-monografii.htm). 11.03.2020).***

***

«В Україні 12 березня стартує інформаційна кампанія з популяризації методів особистого кіберзахисту.

Про це повідомляє прес-служба Ради національної безпеки і оборони України (РНБО).

"Інформаційна кампанія введена в Україні за підтримки урядів Великої Британії, США та Національного координаційного центру кібербезпеки (робочий орган Ради національної безпеки і оборони України)", – зазначено у повідомленні.

Метою кампанії 2FA є інформування громадян про прості та ефективні методи особистого кіберзахисту. Вона стане продовженням національної інформаційної кампанії з кібербезпеки, проведеної в Україні в березні 2019 року.

Зокрема, у рамках кампанії громадянам роз'яснять важливість використання двофакторної автентифікації та ризики, з якими може зустрітися користувач у мережі». ***(В Україні 12 березня стартує інформаційна кампанія, присвячена особистій кібербезпеці // Рубрика (https://rubryka.com/2020/03/09/v-ukrayini-12-bereznya-startuye-informatsijna-kampaniya-prysvyachena-osobystij-kiberbezpetsi/). 09.03.2020).***

***

«В рамках празднования Международного дня безопасного интернета под девизом «Вместе к лучшему интернету» состоялась конференция «Кибербезопасность в сети Интернет».

Об этом ИА «Контекст-Причерноморье» сообщили в департаменте информации Одесского горсовета.

Организаторами конференции выступили Управление противодействия киберпреступности в Одесской области департамента киберполиции Национальной полиции Украины и департамент образования и науки Одесского горсовета. А провели ее с целью ознакомление руководителей образовательных учреждений с основными принципами обеспечения кибербезопасности Украины, сведениями о рисках в сети Интернет и примерами раскрытия уголовных киберпреступлений.

Участникам встречи рассказали об основных направлениях работы киберполиции, влиянии интернета на развитие и безопасность детей, основных угрозах кибербуллинга (интернет-моббинга) для психики ребенка при пользовании интернетом, ознакомили с видами буллинга и причинами его возникновения.

Во время конференции проходили дискуссии, в ходе которых директора школ имели возможность получить ответы на актуальные вопросы от работников УПК в Одесской области ДКП НП Украины.

По результатам работы конференции готовится проект Меморандума о сотрудничестве между Управлением противодействия киберпреступности в Одесской области департамента киберполиции Национальной полиции Украины и департаментом образования и науки Одесского городского совета». ***(Для директоров одесских школ провели конференцию по кибербезопасности // Информационное агентство «Контекст-Причерноморье» (http://www.prichernomorie.com.ua/odessa/news/education/2020-03-12/205369.php). 12.03.2020).***

***

«ДК "Укроборонпром" ініціював аудит готовності концерну протидіяти кіберзагрозам.

Про це повідомляє пресслужба концерну.

"Незалежна оцінка кіберпезпеки компанії буде проведена у період з 16 по 27 березня силами оновленої команди Державної служби спеціального зв'язку та захисту інформації України – єдиного державного органу, уповноваженого

здійснювати подібний аудит для владних інституцій та державних підприємств", - ідеться у повідомленні.

Аудит кібербезпеки проводиться за рішенням та з ініціативи ДК "Укроборонпром" з метою чітко визначити стан кібербезпеки, а також напрями та підходи до покращення кіберзахищеності концерну відповідно до нових нормативних вимог та найкращих практик.

"Щодня підприємства-учасники концерну та сам Укроборонпром відбивають безліч кібератак, і ми прагнемо застосувати найкращі сучасні підходи, аби забезпечити гнучкість робочих процесів і водночас гарантувати належну кібербезпеку стратегічних для країни підприємств", – зазначила заступник гендиректора Укроборонпрому з цифровізації та інновацій Надія Васильєва». ***(Укроборонпром ініціював аудит своєї кібербезпеки // Укрінформ (https://www.ukrinform.ua/rubric-economy/2898105-ukroboronprom-iniciuvav-audit-svoei-kiberbezpeki.html). 17.03.2020).***

***

«Мобільний додаток для військових “Джура” поповнився безкоштовними онлайн-курсами з кібербезпеки.

…усі військові, які користуються додатком, отримали на свої поштові скриньки посилання на безкоштовний курс із підвищення кваліфікації з кібербезпеки.

Відомо, що після успішного проходження цього курсу користувачі отримають електронний сертифікат…» ***(Марина Конопльова. Військовий додаток “Джура” поповнився онлайн-курсами з кібербезпеки // #ШоТам (https://shotam.info/viys-kovyy-dodatok-dzhura-popovnyvsia-onlayn-kursamy-z-kiberbezpeky/). 19.03.2020).***

***

Національна система кібербезпеки

«Будучи составной частью информационной безопасности, кибербезопасность подразумевает меры, направленные на защиту компьютеров, серверов, сетей и программного обеспечения. В рамках данного комплекса мероприятий обеспечивается шифрование, перенаправление, очистка и фильтрация информации. В действующем законе о кибербезопасности заложено множество коррупционных рисков и неработающих норм.

Например, кибербезопасностью в Украине занимаются шесть субъектов (Госспецсвязь, СБУ, киберполиция, НБУ, Минобороны и координационный совет при СНБО). Каждый из них действует, исходя из собственных интересов и преследуя собственные цели.

Проблема в том, что формально Госспецсвязи должна быть единственным хабом в этой вопросе, но на самом деле это — далеко не так.

Госспецсвязь – это устаревшая структура, пережиток 90-х годов, которая позиционирует себя главным госорганом в сфере кибербезопасности, но по факту

таковым не является (ввиду низкой профессиональной квалификации его сотрудников, а также наличию множества коррупционных составляющих в ее деятельности).

Недавно Госпецсвязью был разработан и вынесен на общественное обсуждение новый законопроект «О безопасности информации и информационно-коммуникационных системах». В основу нового документа были положены законодательные нормы ЕС и НАТО (в частности, Директивы ЕС 2016/1148 от 6 июля 2016, регламента ЕС 2016/679 от 27 апреля 2016, директив НАТО AC / 35-D / 2004 и 2005 годов и других).

Также в проекте закона прописаны новейшие подходы к обеспечению безопасности информации, а именно:

регулирование вопросов обеспечения безопасности информации;

прохождение государственными и частными объектами, обрабатывающих гостайну и служебную информацию, обязательной аккредитации ИКС (информационно-коммуникационная система);

отмена лицензирования «КСЗИ» в области криптографической и технической защиты информации, а также разработка реестра субъектов, осуществляющих деятельность в сфере защиты информации;

введение реестра сертифицированных средств и технических решений защиты информации с целью предоставления к ним публичного доступа;

обеспечение информационной безопасности для сохранения конфиденциальности (confidentiality), целостности (integrity), пригодности (availability — accessibility and useful) и целого ряда других свойств (аутентичности, подотчетности, безотказности и надежности);

имплементация положений NIS-директивы ЕС;

предоставление полномочий отраслевым регуляторам устанавливать требования к информационной безопасности (как к конфиденциальной, так и открытой);

расширение круга обязанностей Госспецсвязи с правом предоставления силам НАТО информации с ограниченным доступом для дальнейшей обработки;

регламентирование подходов к техническому регулированию средств защиты информации в зависимости от категории доступа к ней;

возложение на администрацию Госспецсвязи функций государственного надзора за средствами криптографической защиты информации,

внедрение электронной платформы в сфере информационной безопасности и электронного взаимодействия (оказание соответствующих электронных услуг).

Мы попросили прокомментировать законопроект директора компании Berezha Security Константина Корсуна. Ниже приводится его прямая речь:

«Благодаря заимствованию из иностранных источников в законе иногда встречаются умные вещи. Например, в статье 4 прописаны цели и принципы информационной безопасности и ИКС. Но мы не будем заострять внимание на мелочах и перейдет к более интересным вещам.

Согласно документу, при Кабмине планируют создать киберцентр (на основе, как я понял, существующего CERT-UA) для международного обмена информацией о кибератаках, совершенные на объекты критической инфраструктуры. Но до сих

пор нет ни перечня таких объектов, ни утвержденных критериев принадлежности к ним. Кроме киберцентра Правительство хочет создать еще один госорган — Министерство по кибербезопасности (ст. 5 п.3 ОБИС — специально уполномоченный орган по безопасности информации и информационно коммуникационных систем). То есть они хотят сформировать отдельное государственное ведомство со штатом в 300-500 человек, которому от Госспецсвязи перейдут все киберфункции. Но у меня по этому поводу возникает куча вопросов: этот орган будет при КМУ или будет проходить отдельной строкой в госбюджете? По каким принципам будет формироваться штат? Как будет назначаться руководитель (по конкурсу или как всегда)? Должна, конечно, быть какая-то точка отсчета. То есть должна быть создана авторитетная организация, которая бы консультировала всех игроков в сфере кибербезопасности по ключевым вопросам. Мы, со своей стороны, предлагали создать коллективно-совещательный орган (некий высший совет по кибербезопасности) без каких-либо властных полномочий. Он должен состоять из сугубо профессиональных сотрудников, которым давно доверяют. Они бы, со своей стороны, имели все полномочия для проведения разного рода консультаций (граждан, частных и государственных компаний и высших органов госвласти).

В законе также говорится об аккредитации ИКС, что, в свою очередь, позволит чиновникам законно проворачивать свои коррупционные схемы. Например, ст. 9 объясняет не столько, что такое аккредитация ИКС, сколько кто подписывает и выдает сертификат об аккредитации. На самом деле, в документе не уточняется, по каким именно критериям и какой госорган будет заниматься процедурой подтверждения соответствия продукта требованиям безопасности. При этом выдавать его будет, если закон примут, вышеупомянутый ОБИС и назначенные им «отраслевые органы по аккредитации». У меня сразу возникает вопрос: представляют себе авторы законопроекта хотя бы приблизительное количество ИКС, которые нужно аккредитовать? Это же миллионы систем! В этом случае разумнее было бы перевести аккредитацию на самих владельцев, чтобы они присылали в ОБИС и региональные органы сертификаты аккредитации с печатями и подписями их руководителей. В случае фальсификации сертификата руководителя необходимо привлечь к уголовной или административной ответственности за его подделку.

Также бесперспективной выглядит попытка авторов законопроекта определить все виды работ, касающиеся информационной безопасности (ст. 10-я). Этим, скорее, создаются предпосылки для тотального контроля госорганами бизнеса, а также вмешательства в предпринимательскую деятельность. Там же, в одном из положений, упоминается о рейтинге качества выполненных работ, который будет публиковаться в открытом доступе на специальной электронной платформе. Это написали люди, которые не имеют никакого представления о реалиях современного бизнеса. Которые не в курсе, что никто никаким рейтингам в Украине не верит и не будет верить еще лет сто (это чистая манипуляция и коррупция). Конечно, можно построить процесс формирования рейтингов на абсолютно публичных и основанных на прозрачных и всем понятным принципам. Однако сделать это в нынешних реалиях практически невозможно

Кроме всего прочего, чиновники планируют создать электронную платформу информационной безопасности. Из текста понятно, что они задумали «построить» некий огромный портал, куда будет стекаться вся информация из различных госорганов (обмен информацией об инцидентах, электронная отчетность, публичная информация, реестры исполнителей, а также дискуссионные панели). Они хотят объединить все в одну платформу, на которой бы размещалась публичная информация и происходила внутренняя кооперация между различными субъектами. Но в данном случае лучше создать две отдельные платформы, одна из которых должна быть открытой для общества, а другая — закрытой и предназначенной для сугубо внутреннего пользования. Объединить различные платформы в одну — не совсем правильно. Во-первых, очень трудно с технической точки зрения реализовать ее так, чтобы она работала без каких-либо сбоев. Во-вторых, безопасность самой платформы сводится к нулю, поскольку ее будет очень сложно организовать. Причем чем больше платформа, тем больше на ней хостов, хост-страниц и интерактива. Она будет напоминать, скорее, решето, когда одну дырку залатал, а тем временем появилось еще несколько. Власти на создание платформы потратят огромные деньги, но она работать не будет, т.к. ее нереально обезопасить. Я, вообще, с трудом представляю себе, как такой монстр будет работать со всеми заявленными функциями. При том, что она станет главной целью для киберпреступников, враждебных и дружественных спецслужб, сетевых хулиганов и хакеров.

В заключительных и переходных положениях инициаторы проекта закона внесли некоторые изменения в ст. 363 УК. В частности, они увеличили срок за нарушение правил эксплуатации компьютеров или их систем с 3 до 10 лет лишения свободы. Очень большое и не очень адекватное усиление мер наказания, причем данная статья фактически не работает.

В целом, власти не рассматривают вопрос о кибербезопасности в комплексе, а берут и выдергивают отдельные вещи из наших предложений, которые мы ранее озвучили, и частично прописывают их в законах. Таким образом, они хотят всем управлять, всех контролировать и иметь в своих руках все рычаги влияния.

Они создают реестры компаний, предоставляющих услуги по кибербезопасности, которые заведомо не будет работать. С одной стороны, они, вроде бы, отменяют КСЗИ и вводят риско-ориентированную модель и т. д. Но с другой, — они создают новые бюрократические преграды в виде непонятных структур типа министерства кибербезопасности и реестр фирм, которые по своей сути являются коррупционными». ***(Новый законопроект от Госспецсвязи устарел еще до голосования за него в ВР // Goodnews.ua (https://goodnews.ua/technologies/novyj-zakonoproekt-ot-gosspecsvyazi-ustarel-eshhe-do-golosovaniya-za-nego-v-vr/). 27.03.2020).***

***

«У Службі безпеки України розказали про основні новації, які пропонуються у президентському законопроєкті про реформу спецслужби…

Основними новаціями законопроєкту є те, що він розмежовує компетенції СБУ з іншими структурами сектору безпеки. Служба відмовиться від невластивих їй функцій…

Відбудеться демілітаризація СБУ з впровадженням її гнучкої структури. Служба зосередить свою увагу на контррозвідувальній протидії загрозам державній безпеці, кібербезпеці, боротьбі з тероризмом, захисті державної таємниці тощо…». ***(Законопроект: що президент пропонує змінити в СБУ // Рубрика (https://rubryka.com/2020/03/12/zakonoproekt-shho-prezydent-proponuye-zminyty-v-sbu/). 12.03.2020).***

***

Боротьба з кіберзлочинністю в Україні

«…Працівники кіберполіції в Донецькій області спільно зі слідчими поліції Донеччини, під процесуальним керівництвом прокуратури Донецької області, викрили 24-річного місцевого мешканця у несанкціонованому втручанні в роботу електронно-обчислювальної техніки.

Фігурант створив декілька тематичний хакерських форумів. Також самостійно розробив спеціальне шкідливе програмне забезпечення, яке надало доступ до інфікованих комп'ютерів користувачів, для отримання інформації про них.

На власних хакерських форумах чоловік неодноразово створював тематичні записи з посиланням на завантаження вірусу. Він був замаскований під файл для встановлення легальної програми.

Крім цього, кіберполіція встановила, що на початку року фігурант створив інше спеціальне шкідливе програмне забезпечення. Його «робота» полягала в отриманні авторизаційних даних користувачів заражених комп'ютерів. Розповсюдження цього вірусу здійснював за допомогою месенджеру при замовленні певних послуг або консультації. Таким чином фігурант викрадав логіни та паролі від електронних поштових скриньок та інших акаунтів.

Також фігурант здійснював надання послуг з криптування файлів, продажу баз даних, що містили логіни електронних поштових скриньок, які належать мешканцям США та паролів до них…

За даним фактом відкрито кримінальне провадження за ч. 1 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) Кримінального кодексу України. Вирішується питання щодо оголошення чоловіку підозри». ***(Кіберполіція припинила діяльність адміністратора хакерського***

форуму // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-prypynyla-diyalnist-administratora-xakerskogo-forumu-6660/). 12.03.2020).

***

«…Працівники кіберполіції у Запорізькій області спільно зі слідчими поліції, під процесуальним керівництвом місцевої прокуратури, у таких діях викрили місцевого мешканця, 1992 року народження.

Використовуючи розроблене шкідливе програмне забезпечення, фігурант викрадав логіни та паролі від електронних поштових скриньок. Потім за допомогою іншого шкідливого програмного забезпечення перевіряв прив'язку електронної поштової скриньки до електронних гаманців та будь-яких Інтернет-аккаунтів, на яких були гроші. Після отримання необхідної інформації він здійснював вивід грошей на власні підконтрольні рахунки або замовляв товар з-за кордону…

За даним фактом відкрито кримінальне провадження за ч. 1 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) Кримінального кодексу України. Вирішується питання щодо оголошення чоловіку підозри. Йому загрожує до 2 років ув'язнення. (Кіберполіція викрила мешканця Запоріжжя у зламі облікових записів користувачів мережі Інтернет // Кіберполіція України.» ***(https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-meshkanczya-zaporizhzhya-u-zlami-oblikovyx-zapysiv-korystuvachiv-merezhi-internet-2004/). 04.03.2020).***

***

«Служба безопасности Украины, ранее давшая советы по кибербезопасности и медиагигиене, разоблачила хакерскую группировку, члены которой выводили деньги со счетов физических и юридических лиц — речь идет о сумме более 20 миллионов гривен.

В СБУ установили, что группа из пяти человек осуществляла несанкционированное вмешательство в работу компьютерной техники, используя вредоносное программное обеспечение, которое рассылалось по электронной почте для получения несанкционированного доступа к системе «клиент-банк».

Получив доступ, злоумышленники переводили деньги на подставные банковские счета и обналичивали их. Правоохранители провели 34 обыска по месту жительства фигурантов уголовного производства, а также в помещениях, где находились серверы и компьютеры. Обыски провели в Киеве, Одессе и Ивано-Франковской области.

Один из подозреваемых отправлен под арест, еще двое — под круглосуточный домашний арест. Еще по двум фигурантам рассматривается ходатайство об избрании им меры пресечения в виде содержания под стражей…» ***(Хакеры украли со счетов украинцев более 20 млн гривен: раскрыта преступная схема // Факты и комментарии® (https://fakty.ua/338524-hakery-ukrali-so-schetov-ukraincev-bolee-20-mln-griven-raskryta-prestupnaya-shema-foto). 26.03.2020).***

***

Коронавірус COVID-19 та питання кібербезпеки

«Служба безпеки України продовжує припиняти діяльність осіб, які розповсюджують в інтернеті неправдиву інформацію щодо ситуації в Україні через поширення коронавірусу COVID-19.

Фахівці СБУ із кібербезпеки відзначають, що у зв`язку із запровадженням низки обмежувальних заходів для запобігання розповсюдженню хвороби та мінімізації її наслідків активізували діяльність і пропагандисти сепаратизму. Користуючись ситуацією, зловмисники збурюють паніку та протестні настрої серед громадян, намагаються дискредитувати владу, закликають до порушення конституційного ладу та насильницької федералізації.

Підривну діяльність одного із таких інтернет-провокаторів було припинено в Одесі. Він не лише розповсюджував неправдиву інформацію про коронавірус, але й публікував матеріали із закликами до зміни територіальних меж та державного кордону України. А це є кримінальним правопорушенням, передбаченим ст. 110 (посягання на територіальну цілісність і недоторканність України) Кримінального кодексу України.

У межах відкритого кримінального провадження провокатору оголошено про підозру. Вирішується питання щодо застосування обмежувального заходу.

Протягом кількох останніх днів Службою разом із Нацполіцією до адміністративної відповідальності за маніпуляції та спроби дестабілізації суспільної обстановки притягнуто ще 5 осіб у Чернівецькій та Луганській областях.

Крім того СБУ фіксує появу великої кількості деструктивних спільнот на різних інформаційних майданчиках та появу неправдивих публікацій у проросійських ЗМІ. Наразі вживаються заходи щодо блокування їх діяльності та притягнення провокаторів до відповідальності.

У черговий раз закликаємо громадян не вестися на провокації та не довіряти інформації з неперевірених джерел і не поширювати її. Актуальні дані щодо поточної ситуації із розповсюдження коронавірусу є на офіційних сторінках Міністерства охорони здоров'я України та інших державних установ». ***(СБУ притягає до відповідальності осіб, які поширюють фейки про коронавірус // Politica.com.ua (http://politica.com.ua/sbu-prityagaye-do-vidpovidalnosti-osib-yaki-poshiryuyut-fejki-pro-koronavirus/). 18.03.2020).***

***

«Хакеры и мошенники теперь используют веб-сайты или приложения, якобы предназначенные для предоставления информации или сервисов, связанных с распространением коронавируса.

Компания по исследованиям угроз кибербезопасности DomainTools определила, что сайт coronavirusapp.site предлагает своим посетителям установить Android-приложение, которое якобы помогает отслеживать распространение

COVID-19, но на самом деле скрыто устанавливает новый вымогатель под названием CovidLock. Этот сайт также незаконно демонстрирует сертификаты ВОЗ и Центра контроля заболеваемости США (CDCP).

После установки CovidLock вызывает блокировку экрана заражённого устройства и требует оплату в биткоинах на сумму $100 в обмен на пароль, который разблокирует экран и вернёт владельцу контроль над устройством.

Если жертва не заплатит требуемую сумму в течение 48 часов, CovidLock угрожает стереть все файлы, хранящиеся в телефоне, включая контакты, фотографии и видео. Кроме того, CovidLock пытается запугать пользователя тем, что его местоположение отслеживается по GPS.

DomainTools пообещала опубликовать ключи расшифровки для CovidLock, которые ей удалось воссоздать.

Компания по аналитике киберугроз Check Point заявила, что домены, связанные с темой коронавируса, в 50% случаев могут быть связаны со злоумышленниками.

По их оценкам, с января 2020 года в мире зарегистрировано более 4000 доменных имен, связанных с этой тематикой. 3% из них считаются «вредоносными», а 5% – «подозрительными».

11 марта британское Управление финансового надзора (FCA) предупредило о растущем распространении видов мошенничества, связанных с распространением коронавируса, которые также включают «инвестиции в криптовалютные активы».

Британское Национальное бюро по борьбе с мошенничеством (NFIB) говорит, что многие вредоносные сайты предлагают «карты и визуализацию распространения коронавируса».

«Они утверждают, что могут предоставить список людей, инфицированных коронавирусом, в их районе. Чтобы получить доступ к такой информации, жертвы должны пройти по ссылке, которая ведёт на вредоносный веб-сайт, либо должны сделать платёж в биткоинах».

По данным NFIB, мошенники уже получили таким образом около $1 млн. в биткоинах.» ***(Криптовалютные хакеры и мошенники наживаются на коронавирусе // Cryptochain (https://cryptochain.news/kriptovaljutnye-hakery-i-moshenniki-nazhivajutsja-na-koronaviruse.html). 16.03.2020).***

***

«Компания Check Point выявила, что коронавирус стал инструментом хакерских атак на пользователей и бизнес. По данным ее Threat Intelligence, с января в мире зарегистрировано более 4000 доменов, связанных с коронавирусом. Из этих сайтов 3% уже признаны вредоносными, а еще 5% – подозрительными.

По словам экспертов Check Point, такие сайты – часто лишь один элемент атаки. Злоумышленники рассылают спам со ссылкой на вредоносный сайт от лица доверенных организаций, чтобы побудить потенциальную жертву перейти по ней. В случае с коронавирусом это могут быть рекомендации от организаций здравоохранения или данные о распространении вируса, которые могут заинтересовать получателя. В момент перехода по ссылке вредоносное ПО автоматически устанавливается на устройство пользователя.

Check Point обнаружил фишинг-атаку якобы от лица «Всемирной организации здравоохранения», которая распространялась в Италии. Специалисты отметили, что 10% организаций в Италии подверглись этой атаке.

Также крупная спам-кампания была зафиксирована в Японии. Там злоумышленники рассылают спам от лица японской организации помощи инвалидам. В электронных письмах сообщается о распространении коронавируса в нескольких городах Японии, что побуждает получателя открыть документ. Если пользователь заинтересуется и откроет вложение, троян Emotet будет загружен на его компьютер.

Поскольку распространение коронавируса продолжается, злоумышленники будут продолжать использовать тему коронавируса для проведения атак на пользователей и бизнес. Специалисты по кибербезопасности рекомендуют не поддаваться первому импульсу, получая подобные сообщения – не стоит открывать вложения и переходить по ссылкам в подозрительных письмах. Следует остерегаться орфографических ошибок, содержащихся в сообщениях или на сайтах – это один из признаков потенциальной подозрительной активности». ***(Мошенники все активнее используют тему коронавируса в своих вредоносных рассылках // Компьютерное Обозрение (https://ko.com.ua/moshenniki_vse_aktivnee_ispolzuyut_temu_koronavirusa_v_svoih_vredonosnyh_rassylkah_132189). 10.03.2020).***

***

«Из-за пандемии коронавируса в некоторых странах ввели ограничения для заведений общественного питания. Ограничивается количество посетителей и рабочие часы, увеличивается расстояние между столами и т.п. В связи с этим возрос спрос на сервисы доставки еды на дом, чем не преминули воспользоваться кибервымогатели, требующие выкуп за остановку DDoS-атак. По расчетам преступников, их жертвы не захотят терять возросшую прибыль и будут готовы заплатить выкуп.

Одной из жертв кибервымогателей стал немецкий сервис доставки еды на дом Takeaway. Как сообщил в Twitter директор сервиса Йитсе Гроен (Jitse Groen), злоумышленники осуществили DDoS-атаку на сайт Takeaway.com (немецкий раздел Lieferando.de) и потребовали 2 биткойна (около $11 тыс.) за ее прекращение.

Вскоре после публикации твита немецкое подразделение компании Takeaway сообщило об атаке на свои системы. В результате инцидента с целью сохранения целостности данных системы были введены в режим обслуживания.

Некоторые клиенты жаловались на то, что сервис списал деньги за новые заказы, хотя системы были повреждены атакой, и заказы не были приняты. Администрация пообещала вернуть клиентам средства, оплаченные за необработанные заказы. Однако возврат денег не будет осуществляться в автоматическом режиме, и пользователям нужно самим связаться с Takeaway по электронной почте.

По состоянию на 19 марта сервис восстановил работу». ***(Кибервымогатели нашли способ нажиться на карантине // SecurityLab.ru (https://www.securitylab.ru/news/506026.php). 19.03.2020).***

***

«Популярные хакерские соревнования Pwn2Own обычно проходят в рамках конференции CanSecWest в Ванкувере (Канада), и участники должны принимать участие в них лично. Однако в связи с пандемией коронавируса организатор мероприятия Zero Day Initiative (ZDI) принял решение впервые за всю историю Pwn2Own провести соревнования в режиме online.

Первый день Pwn2Own прошел в среду, 18 марта. Команде Georgia Tech Systems Software & Security Lab удалось успешно выполнить код на macOS через уязвимости в браузере Safari и заработать $70 тыс. Разработанная командой атака включала вызов калькулятора в Safari и повышение привилегий до суперпользователя путем эксплуатации шести уязвимостей.

Участник команды RedRocket CTF Манфред Пол (Manfred Paul) получил $30 тыс. за эксплуатацию уязвимости локального повышения привилегий в Ubuntu Desktop, существующую из-за недостаточной проверки входных данных.

Легендарная команда Fluoroacetate в составе Амата Камы (Amat Cama) и Ричарда Чжу (Richard Zhu) заработала $40 тыс. за эксплуатацию уязвимости локального повышения привилегий в Windows 10. За еще одну подобную уязвимость Чжу получил еще $40 тыс». ***(Первый день Pwn2Own прошел в online-режиме из-за коронавируса // SecurityLab.ru (https://www.securitylab.ru/news/506020.php). 19.03.2020).***

***

«Сотрудников компаний и организаций по всей стране отправляют работать из дома в связи с пандемией коронавируса. Но по мере того, как растет количество виртуальных встреч и других интерактивных взаимодействий, увеличивается и количество угроз кибербезопасности.

Национальный Институт стандартов и технологий США (The National Institute of Standards and Technology, NIST) выпустил ряд советов по обеспечению кибербезопасности для организаций, которые должны перейти в режим удаленной работы.

«Неправильная настройка виртуальных встреч может стать причиной прослушки со стороны бывших сотрудников или злоумышленников. Использование некоторых основных мер предосторожности может помочь пользователям обеспечить возможность совместной и эффективной работы на собраниях, не вызывая утечки данных или другие неприятные инциденты, связанные с безопасностью или конфиденциальностью», — отметил директор Национального центра повышения квалификации по кибербезопасности NIST Джефф Грин (Jeff Greene).

Грин представил ряд советов по обеспечению конфиденциальности и безопасности виртуального рабочего общения, большинство из которых просты и, вероятно, уже указаны в существующих политиках организаций.

Ограничение повторного использования кодов доступа для телефонных собраний наряду с одноразовыми PIN-кодами и многофакторной аутентификацией поможет удостовериться, что только авторизованные пользователи будут

участвовать в конфиденциальных разговорах. Комнаты ожидания и информационные панели для виртуальных встреч помогут контролировать посетителей и отслеживать неназванных или общих гостей.

Для более конфиденциальной работы может потребоваться такая практика, как раздача PIN-кодов в последнюю минуту, идентификация всех участников, а затем блокировка собрания и обеспечение подключения всех участников с утвержденных устройств». ***(NIST представил советы по обеспечению безопасности виртуальных встреч // SecurityLab.ru (https://www.securitylab.ru/news/505984.php). 18.03.2020).***

***

«Пока весь мир активно борется с пандемией коронавируса, злоумышленники прибегают к новым способам украсть деньги и данные у пользователей. Киберпреступники распространяют вымогательское ПО под видом Android-приложения для отслеживания заражений коронавирусом.

Специалисты из компании DomainTools зафиксировали активную регистрацию доменных имен в связи коронавирусом. Например, web-сайт coronavirusapp предлагает пользователям установить специальное Android-приложение для отслеживания вспышек заражения.

Как утверждается на сайте, приложение было сертифицировано Всемирной организацией здравоохранения (ВОЗ) и Центрами по контролю и профилактике заболеваний США (Centers for Disease Control and Prevention, CDC). Там же утверждается, что приложение якобы получило более 6 млн отзывов и имеет рейтинг 4,4 звезды.

Однако на самом деле программа является вымогательским ПО под названием CovidLock. После установки приложение запрашивает различные разрешения, включая доступ к экрану блокировки, а затем меняет пароль и требует от жертв выкуп в размере $100 в биткойнах за доступ к устройству». ***(Злоумышленники распространяют фальшивый Android-трекер коронавируса // SecurityLab.ru (https://www.securitylab.ru/news/505916.php). 16.03.2020).***

***

«Журналисты Bleeping Computer обратили внимание на жалобы пользователей, которые сообщали на форумах, что им навязчиво предлагают скачать странное приложение, якобы информирующее о COVID-19 и созданное ВОЗ. Как оказалось, роутеры этих людей были скомпрометированы, а под видом приложения распространялся инфостилер.

Издание рассказывает, что во всех случаях пострадавшие были владельцами роутеров D-Link или Linksys, и неизвестные злоумышленники изменили на устройствах настройки DNS. Пока неясно, как именно атакующие получали доступ к устройствам, но несколько пострадавших признались, что доступ к их роутерам можно было получить удаленно, и они использовали слабые пароли. Так что, вероятно дело идет о брутфорсе и переборе учетных данных по списку известных значений по умолчанию.

Получив доступ к устройству, злоумышленники меняют адреса DNS серверов на 109.234.35.230 и 94.103.82.249…

Исследователи объясняют, что когда компьютер подключается к сети, Microsoft задействует функцию Network Connectivity Status Indicator (NCSI), которая периодически проверяет, активно ли подключение к интернету. Так, в Windows 10 одним из таких тестов будет подключение к http://www.msftconnecttest.com/connecttest.txt и проверка того, содержит ли ответ «Microsoft Connect Test». Если содержит, значит, компьютер подключен к интернету, а если нет, Windows предупредит о том, что интернет недоступен.

Если же пользователь работает со скомпрометированным роутером, то вредоносные DNS-серверы вынуждают Windows, вместо подключения к легитимному IP-адресу Microsoft 13.107.4.52, подключаться к ресурсу злоумышленников, расположенному по адресу 176.113.81.159. В итоге вместо отправки вышеупомянутого текстового файла сайт отображает страницу, предлагающую жертве загрузить и установить поддельное приложение «Emergency - COVID-19 Informator» или «COVID-19 Inform App», якобы созданное ВОЗ.

Если пользователь попадется на удочку атакующих, загрузит и установит это приложение, то вместо информации о коронавирусе он получил трояна Oski. Эта малварь попытается собрать и передать злоумышленникам следующую информацию (список неполный):

cookie-файлы;

историю браузера;

платежную информацию из браузера;

сохраненные учетные данные;

данные криптовалютных кошельков;

текстовые файлы;

данные автозаполнения для форм в браузере;

БД 2ФА идентификаторов Authy;

скриншоты рабочего стола в момент заражения». ***(Мария Нефёдова. Хакеры подменяют настройки DNS для распространения фейковых приложений о коронавирусе // Хакер (https://xakep.ru/2020/03/25/oski-covid19-app/). 25.03.2020).***

***

«Киберпреступники взламывают маршрутизаторы с целью распространения поддельного приложения от Всемирной организации здравоохранения, якобы предоставляющее актуальную информацию о COVID-19. Злоумышленники меняют настройки DNS маршрутизатора таким образом, чтобы в браузере пользователя отображалось уведомление, предлагающее скачать приложение от ВОЗ, на самом деле являющееся инфостилером Vidar.

За последние пять дней в интернете появились сообщения от пользователей о том, что их браузеры вдруг неожиданно сами открывались и отображали уведомления о необходимости скачать COVID-19 Inform App предположительно от ВОЗ.

Как показало исследование, уведомления появлялись в результате кибератаки. Злоумышленники меняли в настройках маршрутизаторов D-Link и

Linksys легитимные DNS-серверы на свои собственные. Поскольку большинство компьютеров используют IP-адреса и информацию DNS, предоставляемую маршрутизатором, подконтрольные злоумышленникам DNS-серверы переадресовывали пользователей на вредоносный контент.

Каким образом злоумышленники получают контроль над маршрутизаторами, пока неизвестно. Однако, по словам некоторых пользователей, у них был включен удаленный доступ к маршрутизатору со слабым паролем.

Пользователям, чьи браузеры внезапно открылись с уведомлением о необходимости скачать приложение от ВОЗ, необходимо авторизоваться на своем маршрутизаторе и проверить в настройках, получает ли он автоматически информацию от DNS-сервера интернет-провайдера. Пользователям, установившим поддельное приложение, рекомендуется провести сканирование системы на наличие вредоносного ПО с помощью надежного антивирусного решения». ***(Хакеры взламывают маршрутизаторы и распространяют поддельное приложение COVID-19 Inform // SecurityLab.ru (https://www.securitylab.ru/news/506128.php). 24.03.2020).***

***

«Медицинская исследовательская компания Hammersmith Medicines Research (HMR), которая должна провести испытания возможной вакцины для COVID-19, стала жертвой атаки операторов вымогательского ПО Maze. Компания отказалась платить выкуп за разблокировку компьютерных систем, и в результате персональные данные тысяч бывших пациентов утекли в Сеть.

Как сообщил ресурс Computer Weekly, операторы Maze опубликовали тайную медицинскую и личную информацию, включающую медицинские опросники, копии паспортов, водительские права и национальные страховые номера более 2300 пациентов организации.

Атака произошла всего через несколько дней после того, как преступная группировка публично сообщила о прекращении атак на медицинские исследовательские организации и компании во время пандемии коронавируса. Свое обещание преступники держали всего три дня. IT-персонал HMR обнаружил кибератаку 14 марта, а к концу того же дня смог остановить ее и возобновить работу компьютерных систем и электронной почты.

HMR не раскрыла, каким образом группа Maze могла получить доступ к ее сети. По словам соучредителя компании Bad Packets Троя Марша (Troy Mursch), Hammersmith Medicines Research использовала VPN-сервер Fortinet, который мог содержать уязвимость, позволившую Maze осуществить взлом». ***(Операторы Maze продолжают атаковать медкомпании, невзирая на обещание // SecurityLab.ru (https://www.securitylab.ru/news/506088.php). 23.03.2020).***

***

«Фахівці з кібербезпеки виявили близько 170 фактів розміщення на інформаційних ресурсах неправдивої чи провокаційної інформації щодо пандемії. Про це повідомив міський голова Києва Віталій Кличко у Facebook.

За його словами, 24-х громадян притягнули до адміністративної відповідальності.

"На жаль, сьогодні багато неправдивої інформації. Її розповсюджують, зокрема, і для маніпуляцій, і для створення паніки. А окремі "діячі" – для отримання сумнівних політичних дивідендів. Ми радимо користуватися інформацією, рекомендаціями, що оприлюднені на офіційних сторінках та сайтах державних установ", – сказав міський голова Києва.

Також Кличко закликав не лікуватися рецептами з інтернету: "А в разі виникнення симптомів хвороби одразу звертатися до лікарів. Тільки медики можуть поставити діагноз, можливо і врятувати здоров'я чи життя людини"…» ***(Коронавірус в Україні: Кіберполіція виявила 170 фейків та провокацій // 5 канал (https://www.5.ua/suspilstvo/koronavirus-v-ukraini-kiberpolitsiia-vyiavyla-170-feikiv-ta-provokatsii-211182.html). 25.03.2020).***

***

«Новий Коронавірус перетворився в глобальну пандемію, яка підриває світову економіку, здоров'я людей, уповільнює бізнес у всьому світі, а також впливає на повсякденне життя мільярдів людей.

Однак це також створило середовище, в якому хакери, шахраї і спамери користуються вразливими користувачами і ситуацією. Оскільки все більше і більше людей працюють з дому з мережами з більш низькою безпекою порівняно з офісними налаштуваннями, ризик піддатися нападу більше.

Атаки з використанням програм-вимагачів, які звичайно ініціюються фішингом, можуть стати причиною неприємностей для лікарень, оскільки зловмисники використовують шифрування для блокування доступу до своїх власних файлів, а потім вимагають платежі в цифровий валюті для розблокування ключів.

минулого тижня університетська лікарня Брно в Чеській Республіці, яка також є великим центром тестування Covid-19, піддалася атаці з застосуванням вимагачів, яка перервала операції і викликала перенесення операцій. Чеський національний центр кібербезпеки і чеські правоохоронні органи досі не повністю відновили дані.

Тепер хакери з угрупування Ransomware заявили, що вони більше не будуть націлюватися на лікарні та медичні організації під час пандемії Коронавіруса (COVID-19).

З іншого боку, хакери з Maze заявили, що вони припинять діяльність проти всіх видів медичних організацій до кінця пандемії. Netwalker Ransomware стверджує, що у них немає мети атакувати лікарню, і подвоює, що “ніхто не буде цілеспрямовано зламувати лікарню”.

Обов'язково підпишись на наш канал в Viber, щоб не пропустити найцікавіше…» ***(Хакери по всьому світу відмовилися від атак на лікарні та будинки престарілих під час пандемії // Znaj.ua (https://techno.znaj.ua/302205-hakeri-po-vsomu-svitu-vidmovilisya-vid-atak-na-likarni-ta-budinki-prestarilih-pid-chas-pandemiji). 25.03.2020).***

***

«Спонсоровані урядом хакерські угрупування та кримінальні хакери з усього світу використовують у своїх інтересах нинішню пандемію коронавірусу, щоб шпигувати за супротивниками. Про це повідомляють численні розвідувальні агентства, які досліджують погрози в області кібербезпеки.

Зокрема, з'ясувалося, що хакерські групи, пов'язані з урядами Китаю і Росії, в останні тижні розсилали шкідливі вкладення електронною поштою. До того ж тематика листів була присвячена коронавірусу.

На рівні уряду

Шкідливий документ Microsoft Word, присвячений тематиці коронавірусу, використовується китайською хакерською групою, відомою як TEMP.Hex.

Вендори в області кібербезпеки — FireEye і Check Point — повідомили, що дві хакерські групи, пов'язані з урядом Китаю, атакували В'єтнам, Філіппіни, Тайвань і Монголію. За словами Бен Ріда (Ben Read), старшого аналітика розвідки в FireEye, хоча хакери відправляють вкладення електронної пошти зі справжньою медичною інформацією про коронавіруси, але там є також шкідливі програми, такі як Sogu і Cobalt Strike.

«Принади складалися з офіційних заяв політичних лідерів, а також правдивих порад для тих, хто турбується про своє здоров'я, ймовірно, взятих з відкритих джерел», — пояснив Рід.

Російська група, відома під назвою TEMP.Armageddon, розіслала цільові фішингові електронні листи українським користувачам. Тактика spear-phishing, яку використали хакери, передбачає розсилку пошти зі спеціально створеними шкідливими посиланнями, які змушують жертву клацнути на посилання і непомітно заразитися.

Аналітики FireEye підозрюють, що нещодавня атака на ціль в Південній Кореї — це робота північнокорейських хакерів. Як і Китай, Південна Корея особливо сильно постраждала від епідеміологічного спалаху. Фішингова електронна пошта розсилалась корейською мовою під назвою «Коронавірусна кореспонденція».

«Ви очікуєте отримати інформацію з урядових джерел, так що, швидше за все, ви відкриєте ці документи, щоб побачити, про що там мова, — зауважив Лотем Фінкельштейн (Lotem Finkelstein), голава розвідки загроз в Check Point. — І це дуже ефективно для запуску атаки. Спалах епідемії коронавірусу дуже добре служить темою приманки, особливо для тих, хто використовує фішингові атаки для їх запуску».

Кримінал

На додаток до поточної діяльності хакерів, спонсорованих урядом, кримінальні кіберзлочинці також хочуть отримати вигоду з хаосу поточних подій. Хоча ця історія не нова — раніше хакери також використовували хаос і страх, викликаний епідеміями Ебола, вірусу Зіка та атипової пневмонії, щоб заробити гроші.

«Чисельність фінансово мотивованих хакерів, що використовують фішингові атаки з використанням коронавірусної тематики в багатьох кампаніях в березні

різко зросла в порівнянні з січнем, — йдеться в повідомленні FireEye. — Ми очікуємо продовження використання приманок на тему коронавірусу різними категоріями кіберзловмисників через глобальну актуальність теми».

Підвищений інтерес людей до новин і розробок, пов'язаних з короновірусом, робить об'єкти атаки потенційно більш сприйнятливими до соціальної інженерії. Своєю чергою, це змушує їх клацати по шкідливих посиланнях, заявляють дослідники з кіберрозвідувальної компанії RiskIQ.

Хоча фішинг — відправка в листі веб-посилання або файлу, призначеного для інфікування системи користувача — це відносно проста технологія, проте, вона є найбільш поширеним і успішним типом атаки вже не перший рік. Хакери, які прагнуть скористатися можливостями, що їм надає епідемія коронавірусу, націлені як на приватних осіб, так і на підприємства. До того ж вони стверджують, що належать довіреним організаціям, таким як Центри контролю захворювань (CDC) і Всесвітня організація охорони здоров'я.

Фішингові електронні листи обіцяють все: від інформації про ліки до медичного обладнання. Насправді вони прагнуть доставити шкідливі програми та вкрасти паролі, щоб заробити на хаосі.

Хакери шукають цілі по всьому світу, але деякі зосередилися на найбільш постраждалих країнах. Італія, яка постраждала більше інших країн в Європі, зазнала потужної фішинг-кампанії проти бізнесу. Підроблені електронні листи, відправлені нібито від Всесвітньої організації охорони здоров'я, обіцяють новітні рекомендації щодо захисту від вірусу. Насправді, замість документів у форматі документу Microsoft Word можна завантажити банківський троян Trickbot, призначений для крадіжки величезних сум грошей.

Хоча відправник електронної пошти стверджує, що він знаходиться в ВООЗ, домен відправника не відповідає веб-сайту ВООЗ — who.int.

В Японії, ще одній країні, яка сильно постраждала від спалаху коронавірусу, також були помічені цільові фішингові розсилки, які нібито надають інформацію про коронавірус від державних органів охорони здоров'я.

«Зловмисники також підривають авторитет внутрішнього бізнесу у своїх атаках. Ми бачили кампанію, в якій була виконана розсилка електронної пошти на тему коронавірусу, яка була замаскована під внутрішню електронну пошту від президента компанії для всіх співробітників… Цей електронний лист був дуже добре продуманий і він містив правильне ім'я президента компанії», заявили дослідники з кіберфірми Proofpoint.

Заходи безпеки

Онлайн-панелі стали стандартом де-факто для відстеження чисельності та географії поширення коронавірусної хвороби. Тому не випадково, що в інтернеті з'явилися фейкові інформаційні панелі, які пропонують вам завантажити додаток для поширення злошкідливого ПЗ AZORult для Windows. Останнє викрадає з інфікованого комп'ютера особисті та фінансові дані, криптовалюту і все інше, що має цінність.

Це не перший і точно не останній випадок, коли хакери використовують заголовки новин, які викликають сильні емоції, намагаючись обдурити свої жертви.

Найкращий захист — підтримувати свої технології інформаційної безпеки в актуальному стані, не переходити за посиланнями від невідомих людей і не завантажувати підозріле програмне забезпечення. Також варто використовувати авторитетні джерела новин для важливих тем». ***(Російські та китайські хакери використовують страх перед коронавірусом для кібершпигунства // Blog Imena.UA (https://www.imena.ua/blog/hackers-use-the-fear-for-cyber-espionage/). 18.03.2020).***

***

«Во время пандемии Covid-19 с риском "подцепить" вирус сталкиваются не только владельцы смартфонов, но и сами гаджеты. Так специалисты по кибербезопасности обнаружили модифицированную версию банковского Android-трояна Ginp, ранее замеченного в подделке текстовых сообщений. Теперь же вредоносное ПО получило новую функцию для кражи денег со счетов пользователей, прикрываясь "заботой" об их здоровье.

Что делает вирус

Троян, который распространяется с помощью сторонних приложений, открывает на зараженном устройстве веб-страницу под названием Coronavirus Finder, которая сообщает, что вблизи якобы есть носители коронавируса.

Чтобы установить их "точное местонахождение", пользователю предлагается заплатить 0,75 евро. В случае согласия на экране появляется форма для ввода платежной информации – при этом деньги со счета не снимал, но реквизиты карты попадают в руки кибермошенников.

Как бороться с вредоносной программой

Чтобы избежать заражения смартфона эксперты рекомендуют скачивать приложения только из официальных источников и не переходить по подозрительным ссылкам, а также не вводить на сомнительных сайтах конфиденциальную информацию, такую как пароли или данные банковской карты.

Специалисты отмечают, что пользователям смартфонов следует быть особенно внимательными в это время, поэтому всплывающие окна, незнакомые веб-страницы и спонтанные сообщения о коронавирусе всегда следует рассматривать скептически». ***(Мошенники используют пандемию коронавируса для заражения Android-смартфонов // Телеканал новостей «24» (https://24tv.ua/techno/ru/moshenniki_ispolzujut_pandemiju_koronavirusa_dlja_zarazhenija_android_smartfonov_n1304243). 25.03.2020).***

***

«Вспышка коронавируса во всем мире сказалась не только на фабриках по производству электроники – многие компании переводят своих сотрудников на удаленный режим работы. Специалисты по кибербезопасности отмечают, что такой шаг негативно скажется на сфере хранения данных и личной безопасности пользователей.

По мнению специалистов из области сохранения данных, источниками слива данных третьим лицам часто становятся сотрудники компании. На фоне эпидемии коронавируса, по сотрудниками, что работают дома, не ведется контроль со

стороны отдела безопасности, а отсутствие коллег рядом может стать дополнительным фактором.

Страшно даже представить, что банки или ИТ-гиганты окажутся неготовыми к новой угрозы – работы по дому. Мы весь прошлый год наблюдали, как недостатки в построении информационной безопасности крупнейших компаний приводили к катастрофическим утечкам данных пользователей и другой информации. А сейчас мы просим сотрудников работать из дома и даем все необходимые доступы,

– заявил руководитель компании в сфере кибербезопасности.

Эксперт отметил, что дома сотрудники различных организаций не защищены от спам-атак и фишинга, а также от взлома рабочих компьютеров злоумышленниками. По его словам, уже сейчас киберпреступники заполнили электронную почту множества пользователей сообщениями, содержащими вредоносные коды.

Как уберечь свои данные и данные компании

Чтобы минимизировать риск потери конфиденциальных данных, специалисты рекомендуют установить на компьютеры сотрудников, работающих удаленно, антивирусные программы и VPN-доступ к учетным записям с двухфакторной аутентификацией, а также обновить софт и IT-оборудованик, обеспечивающие работу организации». ***(Коронавирус вдвое увеличит количество утечек личных данных компаний // Телеканал новостей «24» (https://24tv.ua/techno/ru/koronavirus_vdvoe_uvelichit_kolichestvo_utechek_lichnyh_dannyh_kompanij_n1302394). 23.03.2020).***

***

«Шахраї, кіберзлочинці, організовані злочинні групи і педофіли використовують в своїх інтересах пандемію коронавірусу для активізації своєї діяльності на всій території ЄС. Про це повідомила виконавчий директор Європолу Катерін Де Болле в п'ятницю…

Так, незважаючи на те, що в багатьох країнах зафіксовано скорочення кількості злочинів, таких як крадіжки зі зломом і вуличні бійки, Європол повідомив про зростання онлайн-злочинів, спрямованих на використання підвищеної тривоги і того факту, що так багато людей працюють з дому.

Деякі з кібератак були ретельно скоординовані, націлюючись на критично важливу інфраструктуру.

"Ми не можемо забувати про те, що відбувається в кримінальному світі. Злочинні організації використовують страх людей, використовуючи той факт, що вони шукають інформацію", - заявила в інтерв'ю виданню де Болле.

Із закриттям шкіл по всьому блоку Європол також відзначив зростання дитячої експлуатації, оскільки мільйони дітей проводять більше часу в Інтернеті, що робить їх відкритими для педофілів, які активізували свою діяльність. Національні поліцейські сили, тим часом, зіткнулися з різким зростанням насильства в сім'ї: у Франції за тиждень стався стрибок більш ніж на 30%, зазначає видання.

"У нас є величезна кількість людей, що зловживають дитячими матеріалами в Інтернеті. Ми отримуємо різну інформацію від держав-членів про те, що педофіли шукають матеріали для експлуатації в Інтернеті", - заявила де Болле.

Ще одна сфера для злочинності, за даними Європолу - це контрафакт, оскільки злочинці користуються браком коштів, а схвильовані люди виходять в інтернет, щоб закуповувати медичні товари.

Популярні схеми включають псевдо-тести на коронавірус, підроблені маски і фіктивні фармацевтичні продукти, що рекламуються як лікування від COVID-19.

Серед джерел злочинності, зі слів Де Болле, користуються ситуацією як окремі злочинці, так і організована злочинність.

У звіті Європолу, що має назву "Пандемічна спекуляція" і об'єднує інформацію від поліцейських сил по всьому блоку, особлива увага приділяється зростанню кіберзлочинності.

Замість того, щоб винаходити нові схеми, кіберзлочинці адаптували традиційні фішингові шахрайські розсилки, пов'язуючи їх з коронавірусом, щоб привернути увагу.

Ризик кіберзлочинності посилюється тим фактом, що мільйони людей працюють з дому.

"Вони стають все більш і більш витонченими", - сказала Де Болл про фішинг-шахрайства, більшість з якого було направлено на установку шкідливих програм.

"Ми також бачимо фальшиві сайти, фальшиві новини і фальшиві новини про рішення в зв'язку з коронавірусом", - додала вона.

За даними Європолу, злочинці також стали застосовувати шахрайство, відоме як "бабусин трюк" або "трюк племінника", в якому фальшиві "лікарі" кажуть, що нібито повинні провести тест на коронавірус - тільки щоб проникнути і пограбувати чийсь будинок.

"Багато людей приймають це і дозволяють цим злочинцям входити в свої будинки. У нас є різні країни, де цей трюк використовується, і ми очікуємо, що він буде використовуватися більше в майбутньому", - сказала де Болле…». ***(Саша Картер. Злочинці експлуатують пандемію коронавірусу – Європол // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1860401-zlochintsi-ekspluatuyut-pandemiyu-koronavirusu-yevropol). 27.03.2020).***

***

«По мере того, как все больше людей начинает работать дома в связи с пандемией коронавирусной инфекции, сервис видеоконференций Zoom становится все более популярным. Данной ситуацией решили воспользоваться киберпреступники, регистрируя поддельные домены «Zoom» и создавая одноименные вредоносные исполняемые файлы в попытке заставить людей загрузить вредоносные программы на свои устройства.

Как сообщили специалисты из компании Check Point, с начала пандемии было зарегистрировано более 1700 фейковых доменов Zoom, 25% из которых были зарегистрированы только за последние семь дней.

Эксперты обнаружили вредоносные файлы под названием «zoom-us-zoom_##########.Exe», которые при запуске устанавливают потенциально нежелательные программы, такие как InstallCore — пакетное приложение, устанавливающее другие виды вредоносных программ.

Напомним, ранее стало известно, что iOS-версия Zoom отправляла аналитические данные пользователей компании Facebook, даже если они не были зарегистрированы в соцсети. Обмен данными происходил без ведома пользователей Zoom — приложение уведомляло Facebook о каждом открытии программы, а также сообщало информацию о модели устройства, часовом поясе, городе из которого осуществлялось подключение, название оператора связи и генерируемый мобильным устройством уникальный рекламный идентификатор, используемый компаниями для таргетированной рекламы». ***(Преступники распространяют вредоносное ПО через фейковые домены Zoom // SecurityLab.ru (https://www.securitylab.ru/news/506251.php). 30.03.2020).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Упродовж 2019 року Сполучені Штати Америки та країни Європейського Союзу надали військову техніку для Збройних Сил України на загальну суму близько 143 мільйонів доларів…

Також США та країни Євросоюзу надали обладнання зв'язку, навігаційне обладнання для кораблів ВМС, РЛС контрбатарейної боротьби, засоби кібербезпеки, прилади нічного бачення, намети, мобільні системи освітлення, засоби індивідуального захисту особового складу, обладнання розмінування, медичне обладнання, а також різноманітні запасні частини до технічних засобів, які вже були отримані раніше». ***(США та ЄС надали військову техніку для української армії на 143 мільйони доларів // Інформаційне агентство «1NEWS» (https://1news.com.ua/ukraine/ssha-ta-yes-nadaly-vijskovu-tehniku-dlya-ukrayinskoyi-armiyi-na-143-miljony-dolariv.html). 11.03.2020).***

***

«Експерти громадських організацій України, Чехії, Словаччини і Польщі у 2019 році проводили на Донбасі навчання громадських активістів та поліції щодо безпеки поводження в інтернеті, захисту даних і протистояння вірусним атакам та іншим кіберзагрозам. Зустрічі з громадськими активістами відбувалися у Краматорську, Слов'янську, Щасті, Сєвєродонецьку, Станиці Луганській, Дружківці, Покровську, Авдіївці та Попасній. Вони були частиною проекту «Покращення захисту даних у Луганській області – навички для місцевих, досвід для країн V4 Вишеградської четвірки» (B4), який за підтримки Вишеградського Фонду організувала громадська організація «Team 4 Ukraine» та партнери – «Інформаційний центр Майдан Моніторинг», «Дослідницький центр асоціація словацької зовнішньої політики» і Фонд «Центр досліджень Польща-

Україна»*. Про результати цього проекту Polukr.net розпитав у його керівника – Петера Поймана.

Петре, у рамках проекту ви проїхали майже усю лінію фронту на Донбасі. Які висновки для себе зробили щодо кібербезпеки на цих територіях?

Ми побачили, що ситуація з кібербезпекою на низькому рівні. Наш висновок – такого типу тренінги потрібно проводити системно, з більшим фінансуванням і для більш широкої аудиторії. І робити це потрібно в регіонах, бо, наприклад, в Києві люди є більш обізнані у таких питаннях і в них є більше можливостей відвідувати різноманітні тренінги, зокрема, платні. А в регіонах з цим проблема. Також вважаю, що варто проводити тренінги не лише для звичайних користувачів смартфонів чи комп'ютерів, але й для активістів, які зможуть в подальшому навчати інших. Ми ж не можемо бути постійно на зв'язку і навчити кожного. Тому важливо, щоб з'явилися люди, які готові навчатися і в подальшому вчити інших. За такою схемою, наприклад, працює поліція у Чехії. Вони вибирають пенсіонерів, яких інформують про те як не стати жертвою нападу, а вже ці люди поширюють цю інформацію в маси. Ми хочемо зробити щось схоже, однак не лише з пенсіонерами але й з іншими прошарками населення.

Чому для тренінгів по кібербезпеці вибрали саме територію Луганської та Донецької областей?

У нас була розмова з представниками Вишеградського фонду і вони хотіли, аби ми працювали в першу чергу з областями куди міжнародні організації не завжди доходять. Вони хотіли, аби в першу чергу ми працювали у важкодоступних населених пунктах.

Яка основна мета проекту?

Основна мета – покращення знань у сфері кібербезпеки у Луганській та Донецькій області. Але ми також говорили з людьми про інформаційну безпеку, інформаційну війну. Пояснили що таке сучасна інформаційна війна, які інструменти використовують для її проведення. Зокрема, що це далеко не завжди звичайна брехлива пропаганда, а часто усе набагато складніше. І жертвою може стати навіть людина яка вміє думати, але не завжди має можливість перевірити усі джерела інформації.

Розкажіть, будь ласка, детальніше про сам проект і роботу з людьми на Донбасі.

Цього року наші поїздки були зосереджені на Луганській області. Відбулося декілька зустрічей, лекцій та семінарів. Розпочинали ми у місті Щастя, де було проведено лекцію по кібер та інформаційній безпеці. Після цього переїхали у Сєвєродонецьк. Там у нас дуже хороші стосунки з місцевою поліцією. У них доволі важкі умови роботи. І ми побачили, що у них теж є доволі велика зацікавленість у досвіді роботі нашої чеської поліції, яка займається кібербезпекою. У поліції є доволі багато проблем у роботі. Наприклад, у тому, щоб отримати доступ до інформації чи дозвіл на прослуховування чи моніторинг певних месенджерів злочинців. Зокрема тих, хто торгує наркотиками. Ми розповіли як саме це відбувається у прокуратурі та поліції у нас в Чехії. В результаті відбулася цікава, жива дискусія. Українським поліцейським працюється не завжди просто і не завжди вони отримують належну підтримку від керівництва.

Ми також тренували тренерів. Учасники цих тренінгів не лише дізнавалися як захистити себе і свої девайси, вони також готувалися аби поширювати цю інформацію на ширшу аудиторію. Студенти з Харківського університету, наприклад, поширювали інформацію, яку вони отримали від нас, серед своїх колег.

Важливий момент – ми давали інформацію про кібербезпеку через приклади. Це були не просто лекції – ми давали конкретні поради, які кожен учасник може застосувати на практиці і показували як це працює. Наприклад, ми на екран проектували монітор телефону та комп'ютера і практично показували як налаштувати девайс так, щоб він був більш захищений. І саме в українських реаліях, бо в регіонах не кожен може дозволити собі найновіші моделі телефонів, які мають додаткові можливості безпеки. Тому ми показували як оновлювати систему та як працювати з додатками. Як налаштувати безпеку телефону так, щоб у людей не виникали проблеми.

Які запити найчастіше лунали від учасників тренінгів?

Найчастішим запитанням у нас було "який антивірус використовувати для захисту". Існує така думка, що якщо людина встановила антивірус, то уже все добре. Насправді це не так. І наші кіберспеціалісти попереджають людей, що антивірус далеко не вирішує всі проблеми, а в деяких випадках може навіть зашкодити. Наприклад, у одного з наших спеціалістів взагалі немає жодного антивіруса, бо вони мають і плюси, і мінуси. І один з мінусів – це те, що вони доволі детально вивчають інфраструктуру наших девайсів та інтегруються у нашу систему. Тому деякі антивіруси можуть навпаки бути слабкою ланкою у вашій системі. Особливо, якщо вони російського виробництва. Тому антивіруси слід підбирати дуже ретельно та із спеціалістами.

Які ще поради можуть бути корисні українським пересічним користувачам інтернету?

Є дві найважливіші поради. Перша – в усіх девайсах, які ви плануєте використовувати, має бути оновлена операційна система. Бажано найновіша версія. Пов'язано це з тим, що ті, хто проводить атаки, переважно атакують відомі вже слабкі місця цих систем. Чим свіжіша система тим менше слабких місць. Звичайно, є певні межі, бо є випадки коли ваш комп'ютер чи телефон є старіших моделей і встановлення чогось нового є неможливим. У таких випадках доведеться купувати новий гаджет. А друга порада стосується паролів на пристроях. Річ в тому, що у людей вже так багато різних скриньок, акаунтів, та послуг в інтернеті (електронна пошта, соціальні мережі тощо), що цих паролів потрібно пам'ятати дуже багато. Тут ми радимо людям скачувати програму, яка підбирає паролі за вас (генератор паролей). Є безкоштовні програми для зберігання та генерації паролів. Ми, до речі, хз учасниками тренінгів мали практичні завдання, коли допомагали їм налаштувати їхні пристрої. Виявилося, що ця тема для людей є доволі цікавою.

Яка загалом була реакція людей на ці тренінги і які ваші висновки?

Ми побачили, що потреба у таких тренінгах є. Вважаємо, що потрібно продовжувати це більш системно. Ми побачили, що поінформованість людей покращилася. Ситуації, коли люди вважали, що мати емейл на російських ресурсах є нормально, вже не зустрічаємо. Одночасно ми зрозуміли, що є сенс у забороні соціальних мереж, які створені у певних країнах. Зокрема, тих з якими йде війна.

Бажано, щоб люди не користувалися ними. Особливо ті, хто працює на державу і надає якісь послуги. Бо інколи це виглядає так, якби американські солдати мали акаунти на ресурсах Аль-Каїди. Це ж було б не розу и мно і дивно.

Чи плануєте продовження проекту?

Не готовий наразі дати відповідь на це запитання. Спершу потрібно завершити той проект який розпочали а вже пізніше думати далі. Загалом ми плануємо проекти в Україні, однак дещо з тривогою дивимося на розвиток останніх подій тут. Маємо надію, що все залишиться хоча б так як було раніше і що не буде гіршень з з безпековою ситуацією. Але з того, що я знаю – ситуація з безпекою погіршується навіть на фронті. І це дещо ускладнює реалізацію таких проектів. Тому з цим трохи важко. Люди, які організовують, проводять та фінансують також звертають увагу на такі моменти. Але ми б хотіли продовжувати. Я б навіть збільшив кількість учасників тренінгів, бо бачимо, що можна працювати з групами по двадцять і більше людей. І головне – ми бачимо, що у людей тут є інтерес до набуття таких знань». ***(Петр Пойман: "Тренінги з кібербезпеки в Україні потрібно проводити системно" // Польсько-український Портал polukr.net (http://www.polukr.net/uk/blog/2020/03/%d0%bf%d0%b5%d1%82%d1%80-%d0%bf%d0%be%d0%b9%d0%bc%d0%b0%d0%bd-%d1%82%d1%80%d0%b5%d0%bd%d1%96%d0%bd%d0%b3%d0%b8-%d0%b7-%d0%ba%d1%96%d0%b1%d0%b5%d1%80%d0%b1%d0%b5%d0%b7%d0%bf%d0%b5%d0%ba%d0%b8/). 14.03.2020).***

***

«Сьогодні, 6 березня, у Києві відбулася офіційний старт і презентація додаткового захисту облікового профілю. Участь у заході взяли заступниця посла Великої Британії Хелен Фейзі, перший заступник начальника Департаменту кіберполіції Нацполіції Сергій Кропива, заступник секретаря РНБО Сергій Демедюк і голова Держспецзв'язку Валентин Петров"…

Над створенням цієї інформкампанії працювали спеціалісти Великої Британії, США та України, інформує пресслужба МВС…

За словами Кропиви, кіберполіція тривалий час співпрацювала з урядом Великої Британії над кампанією, яка убезпечить громадян від ключових ризиків у сфері кіберзлочинності, зокрема, йдеться про двофакторну автентифікацію у облікові записи.

«Ці налаштування легкі у використанні - як для молоді, так і для людей похилого віку. Для налаштування потрібно лише кілька хвилин. У результаті наші громадяни та особи, які проживають на території України, зможуть забезпечити безпеку своїх персональних даних та інформації, яка знаходиться на поштових скриньках, телефонах тощо», - зазначив Кропива.

Перший заступник начальника Департаменту кіберполіції Нацполіції додав, що у більшості випадків хакери проводять багатовекторну атаку, яка не спрямована безпосередньо на конкретного громадянина, тож потерпілі, які звертаються до поліції, навіть не розуміють, чому саме вони стали жертвами зловмисників.

У свою чергу Фейзі зазначила, що кіберзагрози стали більш поширеними, адже життя цифровізується.

«Треба зробити необхідні кроки для того, аби захистити себе та свою мережу, тому ця кампанія є такою важливою. Українці не лише повинні розуміти ризики кібератак, а головне - попередити їх», - уточнила Фейзі.

Вона також зауважила, що співпраця Великої Британії з Україною, зокрема з кіберслужбами, добре налагоджена.

«У минулому році ми розпочали кампанію «Пароль грає роль». Це свідчить про те, що сильні паролі можуть захистити онлайн-системи в нашому житті. Сьогодні переходимо до наступного і важливого етапу - двофакторна автентифікація, щоби не дозволити злочинцям підібрати пароль. Це так званий більш міцний рівень безпеки, щоби система залишалася захищеною навіть тоді, коли пароль відомий. Це безкоштовно, просто і дуже ефективно», - наголосила Фейзі.

Кропива підкреслив, що превентивна та просвітницька робота є ключовим завданням для відомства.

«Захід організований для того, щоби повідомити громадянам про різні види кіберзлочинів, а також роз'яснити прості шляхи захисту. Саме двофакторна автентифікація допоможе кожному зробити персональні дані більш захищеними», - зазначив перший заступник начальника Департаменту кіберполіції Нацполіції». ***(В Україні презентували інформкампанію з кібербезпеки // iPress (https://ipress.ua/news/v_ukraini_prezentuvaly_informkampaniyu_z_kiberbezpeky_306936.html). 06.03.2020).***

***

«Держдепартамент оголосив, що США дадуть Україні 8 мільйонів доларів у якості допомоги у сфері кібербезпеки.

Гроші будуть виділені в рамках "кібер-діалогу", проведеного в Києві між чиновниками обох країн.

8 мільйонів доларів підуть на фінансування нового проекту, спонсором якого виступає USAID.

Загалом, проект збирається залучити 38 мільйонів доларів впродовж наступних чотирьох років з метою збільшити можливості України у сфері кібербезпеки.

Зокрема, йдеться про розвиток спеціалістів й проведення регуляторних реформ.

Раніше, в 2017 році США дали Україні 10 мільйонів доларів, які теж пішли на допомогу у сфері кібербезпеки. Кошти так само були виділені після відповідного діалогу представників обох країн, які зустрічалися в 2018 році для перегляду спільних проектів у сфері.

В своїй заяві Держдепартамент наголосив, що останній діалог на цю тему мав на меті повторно підтвердити "нашу спільну рішучість в гарантуванні відкритого, сумісного, надійного й безпечного кіберпростору, в якому всі країни поводяться відповідально".

В зустрічі з українськими чиновниками брали участь чинний заступник голови місії посольства США в Києві Джозеф Пеннінгтон, чиновники з ФБР, а також з міністерств оборони, енергетики, внутрішніх справ й фінансів США.

Сторони обговорили проблеми безпеки, пов'язані зі зміцненням захисту важливої інфраструктури від кібератак, захищеність мереж 5G, а також плани реагування на кібератаки.

Нове фінансування було виділене через два місяці після того, як нова українська влада попросила ФБР про допомогу в розслідуванні атаки російських хакерів проти української газової компанії Burisma.

Остання опинилася в епіцентрі скандалу на тлі процедури імпічменту президента Дональда Трампа, яка була запущена після повідомлення невідомого інформатора про спроби лідера США натиснути на свого українського колегу Володимира Зеленського.

Трамп нібито вимагав від президента України почати розслідування проти колишнього віце-президента Джо Байдена і його сина Гантера, який працював на Burisma у 2014-2019 роках». ***(The Hill: Держдепартамент дасть Україні 8 мільйонів доларів на кібербезпеку // Антикор (https://antikor.com.ua/articles/363107-the_hill_derhdepartament_dastj_ukrajini_8_miljjoniv_dolariv_na_kiberbezpeku). 05.03.2020).***

***

Світові тенденції в галузі кібербезпеки

«Компания Cisco опубликовала шестой ежегодный отчет CISO Benchmark Report, отражающий отношение к вопросам информационной безопасности 2800 профессионалов из 13 стран. Отчет формулирует 20 рекомендаций на 2020 г., отобранных по результатам анализа проведенного исследования и предложенных консультационной комиссией директоров по информационной безопасности.

Директора по ИБ и ИТ продолжают рассматривать цифровую трансформацию как возможность для инноваций и получения конкурентных преимуществ. В то же время трансформация влечет за собой волну инфраструктурных изменений, создающих новые проблемы для ИБ-специалистов, основной заботой которых становится борьба с неизвестными изощренными угрозами.

Сегодня компании используют в среднем более 20 технологий обеспечения информационной безопасности. В тоже время стабильно снижается число вендоров, с которыми работают организации: для 86% организаций их число колеблется от 1 до 20. При этом более 20% (на 7% больше, чем в 2017 г.) отмечают, что управлять мультивендорной средой очень сложно.

Другие примечательные результаты:

42% респондентов страдают от синдрома ИБ-усталости, который определяется как фактическое прекращение активных действий по защите от угроз;

более 96% страдающих синдромом ИБ-усталости заявляют, что управлять мультивендорной средой тяжело, и основной причиной выгорания является сложность.

В процессе борьбы со сложностью ИБ-специалисты наращивают инвестиции в автоматизацию, упрощая свои защитные экосистемы и уменьшая время реакции, прибегают к облачным инструментам ИБ для улучшения обзора своих сетей, а также поддерживают сотрудничество отделов, отвечающих за сеть, оконечные точки и ИБ.

Защита рабочих нагрузок для всех подключенных пользователей и устройств считается исключительно проблематичной. 41% организаций считают защиту дата-центров очень сложной, 39% заявили, что сталкиваются с большими трудностями при защите приложений. Наиболее проблемным местом для защиты данных оказалось публичное облако: 52% считают его исключительно сложным и очень сложным для защиты, в то время как 50% основной проблемой безопасности назвали инфраструктуру частного облака.

ИБ-специалисты сталкиваются с трудностями при защите многочисленных мобильных сотрудников и персональных устройств. 52% респондентов заявили, что сейчас исключительно сложно и очень сложно защищать мобильные устройства. Помочь обезопасить управляемые и неуправляемые устройства без снижения продуктивности сотрудников поможет применение технологий нулевого доверия.

Для защиты доступа к сети, приложениям, пользователям, устройствам и рабочим нагрузкам необходимо расширить применение технологий нулевого доверия. В настоящий момент лишь 27% организаций используют для защиты сотрудников многофакторную аутентификацию (multi-factor authentication, MFA) как действенную технологию нулевого доверия. Опрос показал наивысший процент внедрения MFA в следующих странах (в порядке убывания): США, Китай, Италия, Индия, Германия, Великобритания. Меньше всего в качестве технологии нулевого доверия для защиты рабочих нагрузок применяется микросегментация (17% респондентов).

Растут потери данных вследствие взломов в результате неисправленных уязвимостей. Главное беспокойство в 2020 г. вызывает тот факт, что 46% организаций заявили об инцидентах безопасности, ставших результатом неисправленных уязвимостей (в прошлом году таких было 30%). В прошлом году 68% взломанных в результате неисправленных уязвимостей организаций потеряли 10 тыс. и более информационных записей. В то же время, среди пострадавших от других причин только 41% потеряли такой же объем данных за тот же период.

Сотрудничество между сетевыми и ИБ-подразделениями поддерживается на высоком уровне. 91% опрошенных заявили, что они очень готовы и исключительно готовы к сотрудничеству.

ИБ-специалисты-практики осознают преимущества автоматизации как способа компенсации нехватки кадров по мере внедрения решений с развитыми средствами машинного обучения и искусственного интеллекта. 77% респондентов планируют наращивать автоматизацию для упрощения своих экосистем ИБ и сокращения времени реакции.

Рост применения облачных инструментов информационной безопасности повышает эффективность и результативность. 86% опрошенных заявили, что

применение облачных средств информационной безопасности улучшило сетевой обзор.

Рекомендации для ИБ-директоров

Использовать многоуровневую защиту, которая должна включать многофакторную аутентификацию, сегментацию сети и защиту оконечных точек.

Добиваться максимального уровня обзора и контроля для повышения управляемости данных, снижения рисков и соблюдения установленных требований.

Уделять внимание кибергигиене: укреплять защиту, обновлять устройства и вносить оперативные исправления, проводить обучение и тренинги.

Внедрить поход нулевого доверия для внедрения зрелой культуры безопасности.

Уменьшить сложность, устранить излишние аварийные сигналы, внедрить интегрированный платформенный подход при управлении множеством решений кибербезопасности». ***(Сложность систем информационной безопасности остается существенной проблемой // Компьютерное Обозрение (https://ko.com.ua/slozhnost_sistem_informacionnoj_bezopasnosti_ostaetsya_sushhestvennoj_problemoj_132202). 11.03.2020).***

***

«Эксперты Positive Technologies проанализировали актуальные киберугрозы 2019 года. Анализ показал, что доля целевых атак существенно превысила долю массовых, а наиболее атакуемыми отраслями оказались госучреждения, промышленность, медицина, сфера образования и финансовая отрасль.

По данным исследования, количество уникальных кибератак выросло на 19%, а доля целенаправленных атак составила 60%, что на 5 п.п. больше, чем в 2018 году. При этом эксперты компании фиксировали поквартальный рост числа атак, и если в I квартале целевыми были менее половины атак (47%), то в конце года их доля составила уже 67%.

«Рост доли целенаправленных атак обусловлен рядом причин, — говорит Алексей Новиков, директор экспертного центра безопасности Positive Technologies (PT Expert Security Center). — Ежегодно появляются новые группы злоумышленников, специализирующиеся на атаках класса APT (advanced persistent threat). В течение года мы отслеживали APT-атаки 27 групп, среди которых есть как широко известные (Cobalt, Silence, APT28), так и относительно новые, малоизученные. Однако более пристальное внимание организаций к кибербезопасности, внедрение и использование специализированных средств защиты, нацеленных на выявление и противодействие сложным атакам (в частности, внедрение решений anti-APT), позволяет более качественно детектировать активность злоумышленников, существенно сокращать время их присутствия в организациях. В итоге в публичном поле оказываются данные об инцидентах, а главное — информация о тактиках и инструментарий APT-группировок, что позволяет повысить эффективность противодействия в целом» [1].

По мнению экспертов, компании сегодня должны сместить фокус внимания с защиты периметра на возможность своевременно выявить развитие атаки внутри сети, регулярно проверять, не были ли они атакованы ранее. Учитывая рост целенаправленных атак, постоянно меняющиеся подходы преступников и усложнение ВПО, ключевыми факторами в обеспечении защиты в ближайшие годы станут непрерывный мониторинг инцидентов ИБ, глубокий анализ сетевого трафика и ретроспективный анализ событий в сети.

Наиболее часто кибератакам подвергались госучреждения, промышленность, медицина, сфера науки и образования, финансовая отрасль. При этом доля атак на промышленные компании выросла до 10% против 4% в 2018 году.

Значительные изменения коснулись мотивации злоумышленников в атаках против частных лиц: как показал анализ киберугроз в 2019 году, более половины атак осуществлялись с целью хищения данных, в то время как в 2018 году аналогичный показатель составлял 30%. В целом кража информации стала главным мотивом атак — и для частных (57%), и для юридических лиц (60%). Наибольший интерес для злоумышленников в 2019 году представляли персональные данные, учетные записи и данные банковских карт.

Как показал анализ, трояны-шифровальщики стали одной из наиболее актуальных киберугроз для юридических лиц по всему миру. В 2019 году на их долю пришлось 31% заражений, а средняя сумма выплат злоумышленникам достигла нескольких сотен тысяч долларов США. В конце года эксперты Positive Technologies отметили новый тренд: операторы шифровальщиков в случаях отказа платить выкуп начали шантажировать жертв публикацией данных, которые они скопировали перед тем, как зашифровать их. По данным исследования, на конец 2019 года такие кампании проводили операторы шифровальщиков Maze и Sodinokibi . Информация о том, что преступникам удалось заработать на выкупах позволяет предположить, что в 2020 году нас ожидает новая волна атак шифровальщиков, а возникшая в конце года тенденция к публикации файлов жертв, отказавшихся платить выкуп, получит развитие…». ***(Positive Technologies: в 2019 году 60% кибератак имели целенаправленный характер // SecurityLab.ru (https://www.securitylab.ru/news/505964.php). 18.03.2020).***

***

«По мере того, как предприятия во всем мире все больше осознают критическую важность программной безопасности для своего дальнейшего развития, суммы, которые платят за специалистов в этой сфере, неуклонно растут.

В ноябре 2018 года Thoma Bravo купила у Broadcom провайдера услуг по проверке безопасности приложений, Veracode, за 950 млн долл. Ведущую калифорнийскую фирму по обеспечению киберзащиты приложений, Shape Security, в декабре прошлого года F5 Networks приобрела уже за миллиард долларов.

Очередной рекорд на прошлой неделе установила частная инвестиционная компания Hellman & Friedman (H&F): израильского вендора безопасности приложений Checkmarx она оценила в 1,15 млрд долл.

Checkmarx была основана в 2006 г., а с июня 2015 г., её владельцем стала Insight Partners, которая тогда инвестировала в неё 84 млн долл. Insight Partners планирует сохранить существенную миноритарную ставку в Checkmarx после её продажи H&F.

Базирующаяся в Тель-Авиве компания имеет штат более 700 человек (их число выросло на 73% за последние два года) и свыше 1400 клиентов в 70 странах, среди которых более 40 входят в список Fortune 1000. Предлагаемый Checkmarx пакет утилит позволяет разработчикам выявлять и устранять уязвимости на ранних стадиях создания своих программных решений.

Широкой публике Checkmarx, наиболее известна тем, что обнаружила ряд ошибок в подключенных устройствах, таких как голосовые помощники Google и Samsung. Её эксперты также нашли проблемы в Amazon Echo и Soundcloud.

«Поскольку все больше корпораций обращаются к разработке ПО в целях масштабирования своего бизнеса, руководители остро осознают возросшие риски, связанные с уязвимостью программ, – отметил Эммануэль Бензакен (Emmanuel Benzaquen), исполнительный директор Checkmarx, в своем заявлении. – Мы очень рады сотрудничать с H&F в путешествии, которое выводит наше видение ”ПО эквивалентно безопасности” на новый уровень».

Со своей стороны, партнёр Hellman & Friedman Тарим Васим (Tarim Wasim) заверил, что его компания рассчитывает развить дальше огромный успех Checkmarx в условиях интенсификации угроз кибербезопасности и обеспечит поддержку быстрого роста этой фирмы в ближайшие годы». ***(Checkmarx куплена инвестором из Сан-Франциско за 1,15 млрд долл. // Компьютерное Обозрение (https://ko.com.ua/checkmarx_kuplena_investorom_iz_san-francisko_za_1_15_mlrd_doll_132347). 23.03.2020).***

***

«Компания-поставщик решений по управлению энергией Eaton продолжает расширять свою программу кибербезопасности. Eaton получил сертификаты кибербезопасности Международной электротехнической комиссии (МЭК) для своих коммуникационных карт Gigabit Network Card и Industrial Gateway Card. Эти устройства также отвечают стандартам кибербезопасности UL, что гарантирует усиленную защиту сети для устройств соединения ИБП. Eaton первой в своей отрасли получила двойные сертификаты IEC и UL, что говорит о соответствии продуктов компании жестким спецификациям и ожиданиям заказчиков в отношении безопасного электропитания.

Эксперты ожидают, что к 2025 году в мире будет 41,6 млрд подключенных устройств, которые будут генерировать 79,4 ЗБ данных, нуждающихся в обслуживании и обработке. (Источник: IDC). Стремительный рост Промышленного Интернета Вещей (IIoT) вызывает необходимость в надежных средствах защиты данных. Без глобальных стандартов кибербезопасности управлять параметрами кибербезопасности IIoT крайне сложно.

«Кибербезопасность — это критически важная тема. Активный и последовательный подход Eaton в этой сфере является уникальным в отрасли», — заявляет Майкл Регельски, старший вице-президент и главный технический

директор электротехнического сектора Eaton. «Но для продвижения IIoT-безопасности в мире, который становится все более электрифицированным и взаимосвязанным, необходимо, чтобы отраслевые организации и организации стандартизации создавали единые глобальные стандарты кибербезопасности. По этим вопросам мы и сотрудничаем с UL и МЭК.

Карта Gigabit Network Card стала первым устройством соединения для ИБП, получившим сертификат UL. Теперь карты Gigabit Network Card и Industrial Gateway Card также имеют сертификаты IEC 62443-4-2. Эти устройства Eaton упрощают подключение однофазных и трехфазных ИБП, одновременно обеспечивая кибербезопасность при включенном питании в коммерческих зданиях, на промышленных объектах и в больших центрах обработки данных». ***(Инфраструктура Eaton для ИБП получила ключевые сертификаты UL и IEC для кибербезопасности // ITUA.info (http://itua.info/press/39093.html). 23.03.2020).***

***

«Аналитики британской исследовательской компании Comparitech составили рейтинг стран мира по уровню кибербезопасности. Они изучили уровень кибербезопасности в 76 странах, оценив такие показатели, как процент мобильных устройств и компьютеров, зараженных вредоносным ПО, количество хакерских атак с целью кражи денег, готовность страны к хакерским атакам и современность ее законодательства в сфере кибербезопасности. Исследователи обнаружили, что законодательство России лучше всего отвечает современным требованиям в сфере кибербезопасности.

Исследователи выявили огромные различия по ряду категорий, от уровня вредоносных программ до законодательства о кибербезопасности. «На самом деле, ни одна страна не была «лучшей в своем классе» по всем направлениям. Все страны, которые мы проанализировали, нуждались в значительных улучшениях», — пояснили в Comparitech.

Исследователи обнаружили, что показатели большинства стран улучшились с прошлого года. Но из-за активизации усилий большинства стран в области кибербезопасности это означает, что некоторые из лучших разработчиков прошлого года опустились в рейтинге. Это касается, например, США, которые опустились с пятого места по кибербезопасности в мире на 17-е.

Согласно исследованию, Алжир по-прежнему является наименее кибербезопасной страной в мире, несмотря на незначительное улучшение показателей. В стране по-прежнему самое плохое законодательство. Алжир также показал плохие результаты по заражению компьютерными вредоносными программами (19,75%) и подготовке к кибератакам (0,262). Во всех других категориях атаки снизились, как это было в большинстве стран.

Другими «отстающими» странами стали Таджикистан, Туркменистан, Сирия и Иран. Самый высокий процент заражений мобильным вредоносным ПО показал Иран — 52,68% пользователей было заражено в 2019 г. Наибольшее количество финансовых вредоносных атак — Белоруссия — 2,9% пользователей. Самый высокий процент компьютерных вредоносных программ — Тунис — 23,26% пользователей. Самый высокий процент атак telnet (по стране происхождения) —

Китай — 13,78%. Наибольший процент атак криптомайнеров — Таджикистан — 7,9% пользователей.

Результаты показали, что Дания является самой кибербезопасной страной в мире, а также Япония, которая опустилась на четыре позиции до пятой по кибербезопасности страны.

Другие страны с самыми высокими показателями: Швеция, Германия, Ирландия и Япония. Франция, Канада и Соединенные Штаты были вытеснены из пятерки самых кибербезопасных стран и заняли соответственно девятое, шестое и 17-е места.

Оценка США значительно снизилась из-за высокого уровня заражения компьютерными вредоносными программами (9,07%) и большого числа атак telnet (4,71%).

Самый низкий процент мобильных вредоносных программ — Финляндия — 0,87% пользователей. Наименьшее количество финансовых вредоносных атак — Дания, Ирландия и Швеция — 0,1% пользователей. Самый низкий процент компьютерных вредоносных программ — Дания — 3,15% пользователей. Самый низкий процент атак telnet (по стране происхождения) — Туркменистан — 0%. Самый низкий процент атак криптомайнеров — Япония — 0,17% пользователей.

По данным исследования, самое современное законодательство по кибербезопасности — во Франции, Китае, России и Германии — все семь категорий охвачены.

Показатели большинства стран улучшились по сравнению с прошлым годом. «Индекс Индонезии значительно улучшился: с 54,89 в прошлом году до 31,33 в этом году. Причем немало европейских стран также отметили значительные улучшения (например, Украина, Германия, Португалия, Болгария и Хорватия). Только США, Бразилия, Япония, Франция, Иран и Сингапур имеют худшие результаты, чем в предыдущем году. Хотя во всех случаях наблюдается лишь небольшая разница, как мы видели в случае с США, этого достаточно, чтобы способствовать значительному снижению рейтинга из-за улучшений во многих других странах», — пишут исследователи в отчете.

Ключевые выводы исследования

Законодательство Алжира хуже всего отвечает современным требованиям в сфере кибербезопасности. В стране только один закон, касающийся приватности. Уровень заражения компьютеров вредоносным ПО составил 19,75%.

Самый высокий процент мобильных устройств, зараженных вредоносным ПО, в Иране – 52,68%.

Самое высокое число хакерских атак, связанных с финансами, в Беларуси. С ними столкнулись 2,9% пользователей.

Самый высокий показатель зараженных вредоносным ПО компьютеров в Тунисе – 23,26%.

Самый большой процент атак с применением криптомайнеров в Таджикистане – 7,9%.

Страной, наименее подготовленной к кибератакам, эксперты признали Туркменистан.

В список стран с самым современным законодательством, которое охватывает все семь категорий в сфере кибербезопасности, попали Россия, Франция, Китай и Германия.

Напомним, страной с самым несвободным интернетом из 65 проанализированных был признан Китай с 10 баллами свободы. Лидером же рейтинга стала Исландия, набравшая 95 баллов». ***(Comparitech: рейтинг стран мира по уровню кибербезопасности возглавила Дания // mResearcher (https://mresearcher.com/2020/03/comparitech-rejting-stran-mira-po-urovnyu-kiberbezopasnosti-vozglavila-daniya.html). 17.03.2020).***

***

Сполучені Штати Америки

«…Соединенным Штатам необходимо назначить координатора по вопросам кибербезопасности и выработать более эффективную стратегию сдерживания хакеров и иных киберугроз, заявила в среду учрежденная Конгрессом комиссия по вопросам киберпространства.

Согласно докладу комиссии, для эффективной обороны в киберпространстве нужно провести серию реформ и принять политические инициативы, направленные на противодействие атакам.

Двухпартийная комиссия, в которую вошли законодатели и эксперты из частного сектора, подготовила более 80 рекомендаций – от реформ в исполнительной и законодательной власти до развития сотрудничества с союзниками.

«Реальность такова, что мы опасно незащищены», – отметили сопредседатели комиссии сенатор Ангус Кинг и член Палаты представителей Майк Галлахер.

«Вся ваша жизнь – ваша зарплата, медицинское обслуживание, электричество – все больше зависит от сетей и цифровых устройств, которые хранят, обрабатывают и анализируют данные. Эти сети уязвимы, если уже не скомпрометированы».

Члены комиссии заявили, что необходимы усилия, сопоставимые по масштабу с предотвращением терактов, подобных атакам 11 сентября.

Комиссия рекомендовала создать в Белом доме позицию «национального кибердиректора», который будет координировать усилия правительства и частного сектора.

Комиссия также отметила необходимость более эффективной стратегии сдерживания, чтобы показать, что атаки в киберпространстве повлекут за собой последствия.

«Сдерживание в киберпространстве возможно», – считают авторы доклада.

«Сегодня большинство кибердеятелей не боятся атаковать наши личные данные и общественную инфрастуктуру… Своей неспособностью или нежеланием выявлять и наказывать наших киберпротивников мы демонстрируем, что

вмешательство в американские выборы и хищение интеллектуальной собственности на миллиарды долларов являются приемлемым поведением».

Комиссия подчеркивает, что и правительство, и частный сектор «должны защищаться и давать отпор быстро и маневренно».

Комиссия призывает выработать «многослойную» стратегию, которая будет предусматривать ответные меры.

«Ключевой, хотя не единственный элемент реагирования – военный инструмент власти», – отмечают авторы доклада.

«Соединенные Штаты должны сохранять способность, решимость и готовность задействовать возможности киберсферы и иные меры разного рода», – подчеркивают они». ***(Комиссия Конгресса призвала учредить должность координатора по кибербезопасности // Голос Америки (https://www.golos-ameriki.ru/a/afp-us-cyber-coordinator/5324658.html). 11.03.2020).***

***

Російська Федерація та країни ЄАЕС

«Хакерская группа Digital Revolution рассказала о закупке ФСБ программы «Фронтон» для кибератак с помощью цифровых ассистентов и «умных домов». Атакуя серверы через «умные» устройства интернета вещей, она позволит обвалить сайты соцсетей и блокировать интернет в небольших странах…

Digital Revolution опубликовала документы, схемы и фрагменты кода, которые создали в 2017-2018 годах. Как утверждают хакеры, у программы есть разные версии…

Согласно документам, «макет опытно-конструкторской работы» изготовила «ИнформИнвестГрупп» по заказу войсковой части №64829, известной как Центр информационной безопасности ФСБ.

Отмечается, что «ИнформИнвестГрупп» ранее выполняла заказы МВД.

По прогнозам агентства Gartner, в 2020 году к «умным» программам подключат более 20 млрд гаджетов. Часто пользователи используют «умные» устройства, не меняя заводские пароли — это делает их доступными для хакеров.

«Фронтон» сможет использовать IP-камеры и цифровые видеорекордеры как ботов для массового отправления запросов на сервера и выводить их таким образом из строя, утверждается в документах. Взламывать «умные» устройства планируют с помощью словаря типичных паролей.

«Мощная атака нескольких сотен тысяч машин способна сделать сайты социальных сетей, файлообменников недоступными в течение нескольких часов. Атака на национальные DNS-серверы может сделать недоступным интернет в течение нескольких часов в небольшой стране», — говорится в документах. Также хакеры отмечают, что зараженные устройства могут использоваться для «шпионажа за всем миром». ***(Digital Revolution: ФСБ закупила программу для кибератак на умные устройства // РосКомСвобода (https://roskomsvoboda.org/56503/). 19.03.2020).***

***

«Председатель Следственного комитета РФ Александр Бастрыкин на расширенной коллегии ведомства заявил о создании нового подразделения:

«Образован отдел по расследованию киберпреступлений и преступлений в сфере высоких технологий».

Ранее СК неоднократно поднимал тему необходимости борьбы с вовлечением несовершеннолетних в «группы смерти» в соцсетях.

Глава СКР сделал особый акцент на создании специализированных подразделений в СК по различным видам преступлений, а также развитие криминалистических возможностей. В качестве примера он привел применение данных со спутников при расследовании уголовных дел. «Полученные данные дистанционного зондирования Земли из космоса легли в основу целого ряда обвинительных приговоров», — пояснил Бастрыкин.

СК также нацелен на цифровое развитие — глава ведомства потребовал от подчиненных эффективно использовать возможности для обращения граждан через электронные сервисы. В ведомстве создан и информационно-технический совет по вопросу информационной деятельности. Кроме того, сообщил Бастрыкин, «введены должности специалистов для социологических исследований». ***(Следком создал отдел по борьбе с киберпреступлениями // РосКомСвобода (https://roskomsvoboda.org/56010/). 04.03.2020).***

***

«Следственный комитет Республики Беларусь возбудил уголовные дела по фактам несанкционированного доступа к компьютерным системам учреждений здравоохранения Беларуси.

12 февраля нынешнего года руководитель РНПЦ пульмонологии и фтизиатрии Минздрава Беларуси сообщил в милицию о том, что некие киберпреступники взломали электронную почту центра. Вскоре от имени центра злоумышленники разослали сообщения с несколькими ссылками на загрузку вредоносного ПО. Позже с аналогичным сообщением в милицию обратился один из руководителей Минского зонального центра гигиены и эпидемиологии.

«В обоих случаях скомпрометированные электронные почтовые ящики были зарегистрированы на хостинге tut.by. Сообщения были подготовлены с применением приемов социальной инженерии — в них содержалась не соответствующая действительности информация, касающаяся распространения коронавируса в Беларуси», — сообщили в СК.

После открытия вредоносных ссылок на компьютер пользователя под видом pdf-файла скачивался скрипт, запускающий исполняемый вредоносный файл.

Уголовные дела возбуждены по ст. 349 («Несанкционированный доступ к компьютерной информации») УК Центральным (г. Минска) районным отделом и Минским районным отделом. Следователи в настоящее время работают над установлением личностей подозреваемых». ***(Преступники рассылали вредоносы со взломанной почты медучреждений Беларуси // SecurityLab.ru (https://www.securitylab.ru/news/505607.php). 05.03.2020).***

***

«…Поліція Японії минулого року щодня виявляла рекордну кількість кібератак.

Про це пише Xinhua із посиланням на Національне поліційне агентство Японії…

“Кіберцентр щодня виявляв у середньому 4192 кібернетичні атаки, що майже на 50% більше, ніж минулого року”, - йдеться у матеріалі.

Зазначається, що вірогідною причиною зростання кількості атак є збільшення числа можливих цілей, таких як під’єднана до Інтернету домашня техніка.

“Кількість виявлених поліцією кіберзлочинів у порівнянні із минулим роком зросла на 479 випадки й досягла у 2019-му році 9519-ти, встановивши рекорд четвертий рік поспіль”, - зазначає Xinhua.

Найчастіше поліція виявляла дитячу проституцію та порнографію, що разом склали 2281 випадок. Ще 785 - злочини, пов’язані із викраденням паролів чи ідентифікаційних документів. “Сума грошей, отриманих в незаконних операціях за допомогою інтернет банків, досягла 2,52 мільярда йен ($23,5 мільйона), що уп’ятеро більше, ніж минулого року”, - підсумовує Xinhua.» ***(У Японії суттєво зросла кількість кібератак // iPress (https://ipress.ua/news/u_yaponii_suttievo_zrosla_kilkist_kiberatak_306892.html). 06.03.2020).***

***

Протидія зовнішній кібернетичній агресії

«Компания Qihoo 360, которая занимается исследованиями цифровой и интернет-безопасности, обвинила ЦРУ в том, что эта организация на протяжении 11 лет — с сентября 2008 по июнь 2019 годов, вела шпионскую и хакерскую деятельность против Китая.

Согласно заявлению, ЦРУ (упомянута хакерская группа APT-C-39) проводила серию хакерских атак против многочисленных компаний в различных отраслях: научные исследования, авиация, нефтяная сфера, цифровые коммуникации, а также правительственных агентств, преимущественно расположенных в Пекине, Чжэцзяне и Гуандуне.

Qihoo 360 заявляет, что хакерские инструменты, такие как Fluxwire и Grasshopper, использовались американцами не только против Китая, но и против других стран.

Некоторая информация была известна китайским исследователям и ранее, но сейчас стало известно, что США в последнее время усиленно интересовались авиационной отраслью, включая информацию о пассажирских и грузовых перелетах, а также об инфраструктуре. Исследователи полагают, что собранной

информации ЦРУ должно хватить, чтобы в реальном времени отслеживать любой грузовой или пассажирский самолет.

Многие издания, поддерживающие Китай, стали призывать к введению санкций против американского кибершпионажа. Впрочем, обвинение не стало сюрпризом после того, как власти США обвинили нескольких китайских военных в хакерских атаках на американские компании, в том числе Equifax». ***(Китай обвиняет США в 11-летней хакерской деятельности // SecureNews (https://securenews.ru/china-accuses-us-of-11-years-of-hacking/). 05.03.2020).***

***

Створення та функціонування кібервійськ

«Уряд Великої Британії створив особливий відділ боротьби з дезінформацією через підозри, що Росія навмисне поширює у мережі фейки про коронавірус…

Уряд прем'єрміністра Великої Британії Бориса Джонсона створив особливий відділ боротьби із дезінформацією на тлі підозр, що Росія навмисно розповсюджує фейкові новини щодо коронавірусу, сіючи паніку серед населення Сполученого Королівства.

У британському керівництві висловлюють дедалі більше занепокоєння спробами Кремля та асоційованих із ним угруповань використати пандемію, наповнюючи медіапростір та соціальні мережі плітками, щоб загострити ситуацію. Зокрема, у дезінформаційній кампанії використовують чутки про нестачу продуктів харчування і ліків.

Британський оглядач із питань безпеки Тім Гарлі зазначає, що однією з головних цілей Росії з-поміж країн західного альянсу є саме британці.

Щоб протидіяти цьому, до новоутвореного відділу британського уряду увійшли фахівці з різних міністерств, які мають досвід роботи із засобами масової інформації, соціальними мережами і кібербезпекою…». ***(Росія тероризує британців фейками про коронавірус // Espreso.tv (https://espreso.tv/news/2020/03/15/rosiya_teroryzuye_brytanciv_feykamy_pro_koronavirus). 15.03.2020).***

***

«…Створено Кібернетичні сили Євросоюзу швидкого реагування, до складу яких увійшли представники шести європейських держав. Ініціатором їхнього створення стала Литва.

Про це повідомляє Міністерство оборони Литви…

«Шість європейських країн - Литва, Естонія, Хорватія, Польща, Нідерланди та Румунія - об'єднали зусилля щодо боротьби з кіберзагрозами у створенні спільних міжнародних можливостей швидкого реагування. Відтепер міжнародна команда швидкого реагування (Cyber Rapid Response Team, CRRT - ред.) перебуватиме у режимі очікування на декількох фізичних сайтах і готова негайно відреагувати на кібератаку в разі її виникнення», - йдеться в повідомленні.

Це було остаточно погоджено 4 березня в Загребі (Хорватія) у Меморандумі про взаєморозуміння. Документ юридично дозволяє роботу таких груп у юрисдикціях різних країн, визначає механізм роботи CRRT, правовий статус, ролі і процедури. Створені цивільними і військовими експертами, CRRT приєднаються до нейтралізації і розслідування небезпечних кіберінцидентів практично або, за необхідності, фізично.

«Досягнувши прориву в зміцненні національних кібернетичних сил, Литва також зміцнює міжнародне співробітництво, це сприятиме відсічі кіберзагрозам, обміну знаннями, проведенню спільних навчань. Це конкретний приклад того, як країни ЄС невійськовими засобами можуть сприяти підвищенню безпеки Європи, підтримувати зусилля в справі оборони і стримування», - сказав по телефону із Загреба міністр оборони Раймундас Каробліс.

З ініціативою створення таких сил Литва виступила в 2017 році, минулого року відбулися перші навчання, а з початку цього року вже несе чергування міжнародна команда з литовців, голландців, поляків і румунів. За словами Каробліса, кіберсили можуть реагувати на інциденти в країнах, які підписали угоду, а також у країнах-спостерігачах, а в майбутньому - і в структурах ЄС. Міністр уточнив, що статус спостерігача отримали Бельгія, Греція, Іспанія, Італія, Франція, Словенія і Фінляндія.

На церемонії підписання був присутній і Верховний представник ЄС із закордонних справ і політики безпеки Жозеп Боррель…». ***(У ЄС з'явиться спецпідрозділ, що відповідатиме за кібербезпеку // ipress (https://ipress.ua/news/u_yes_zyavytsya_spetspidrozdil_shcho_vidpovidatyme_za_kiberbezpeku_306881.html). 05.03.2020).***

***

Кіберзахист критичної інфраструктури

«Рабочая группа центра компетенций «Энерджинет» подготовила отчет, в котором сравнила ключевые документы в области кибербезопасности энергетических отраслей США и России. Компания InfoWatch, чьи эксперты вошли в рабочую группу, предоставила доклад «Известиям» во вторник, 10 марта.

В США основные решения по управлению рисками возложены на собственников и операторов критической инфраструктуры. Госорганы обеспечивают указанных лиц информацией об угрозах, стандартах управления рисками, лучших практиках и возможных решениях.

В России при организации государственной системы обеспечения кибербезопасности также присутствует этап по управлению рисками. Однако он заключается лишь в процедуре категорирования объектов критической информационной инфраструктуры (КИИ).

После определения категории значимости объекта его собственники и операторы в обязательном порядке должны исполнить требования регуляторов по информационной безопасности.

Получается, что российские предприятия реализуют только техническую часть процесса, а управление рисками конкретных предприятий остается в ведении государства, отмечается в докладе.

Согласно результатам отчета, кибератаки на инфраструктуру относятся к числу наиболее значимых глобальных рисков, их значимость составляет 76,1%.

При этом в международном рейтинге стран по индексу информационной безопасности за 2018 год Россия заняла 26-е место с показателем 0,836 балла.

Составители рейтинга за 2018 год особо отметили улучшение в России мер против мошенничества в сфере использования электронных платежных систем.

Соединенные Штаты заняли второе место с показателем 0,926 балла. Всего в рейтинг входят 194 страны – участницы ООН». ***(Эксперты сравнили кибербезопасность критической инфраструктуры США и РФ // Известия (https://iz.ru/985225/2020-03-10/eksperty-sravnili-kiberbezopasnost-kriticheskoi-infrastruktury-ssha-i-rf). 10.03.2020).***

***

Захист персональних даних

«Возглавляемая советником спикера Госдумы и экс-главой комитета по конституционному законодательству Владимиром Плигиным АЮР подготовила предложения по изменению закона «О персональных данных»… Они направлены руководителю Роскомнадзора Александру Жарову и председателю комитета Госдумы по информполитике Александру Хинштейну. Юристы хотят обязать операторов персональных данных (то есть все госорганы, компании и физические лица, обрабатывающие такие данные) по требованию граждан выплачивать им по решению суда в случае утечки компенсацию в размере от 500 тыс. до 5 млн руб. Если утечка данных произошла по вине пользователя, оператор освобождается от ответственности.

Возможность взыскать компенсацию с компании в случае утечки теоретически есть и сейчас, но, по мнению АЮР, она сильно затруднена.

«Чтобы взыскать убытки от утечки персональных данных через суд, гражданину необходимо доказать не только факт нарушения, но и размер убытков, а также причинно-следственную связь между допущенным оператором нарушением и такими убытками»,— поясняет председатель комиссии по правовому обеспечению цифровой экономики московского отделения АЮР Александр Журавлев. При этом обычно гражданин не знает, кем, в каком объеме и зачем обрабатывались его персональные данные, после того как первоначальный оператор передал их дальше, полагает господин Журавлев.

Существующие штрафы Роскомнадзора за нарушение прав субъектов персональных данных до 75 тыс. руб. «не создают достаточных финансовых стимулов для операторов», суды же присуждают «крайне невысокие суммы» в качестве компенсации морального ущерба, добавляет он.

Гендиректор платформы для управления данными HFLabs Дмитрий Журавлев предупреждает, что ужесточение регулирования может, наоборот, повысить риски. Чтобы получить выплаты в случае утечки, гражданину придется идентифицироваться, то есть, например, заполняя обычную анкету на дисконтную карту, указать еще и паспортные данные, поясняет он. Базы данных с паспортами клиентов представляют намного более высокую ценность, и вероятность утечки таких данных серьезно повышается, уверен господин Журавлев. Кроме того, если штрафы будут существенными, это создаст условия для недобросовестной конкурентной борьбы, «фактически, украв данные, можно будет и клиентов переманить, и утопить бизнес конкурента через штрафы», опасается он. В долгосрочной же перспективе ужесточение скорее плюс, признает господин Журавлев.

Доцент факультета права НИУ ВШЭ, зампред комиссии по правовому обеспечению цифровой экономики московского отделения АЮР Александр Савельев отмечает:

«Ни для кого не секрет, что законодательство о персданных в настоящее время практически не работает и за это его не критикует только ленивый. Необходима «перезагрузка» законодательства о персданных. Для этого требуется наделение самих граждан эффективным инструментов защиты своих прав на персданные».

Существующие ныне инструменты, считает он, не эффективны:

убытки нельзя взыскать по причине крайне тяжелого бремени доказывания (размер убытков, причинно-следственная связь между нарушением и убытками), моральный вред если и взыскивается в этой сфере, то в крайне мизерных размерах.

административные штрафы низкие и идут при этом в бюджет, а не потерпевшему субъекту.

Ситуацию могло бы кардинальным образом исправить введение, по аналогии с законодательством об авторских правах, компенсации за нарушение прав субъектов персональных данных. При доказанности факта нарушения права (например, факта утечки данных или факта неисполнения оператором каких-либо своих обязанностей перед субъектом, например, по уточнению или удалению данных), гражданин вправе будет получить компенсацию от 10 000 до 1 млн. рублей (размеры обсуждаемы), размер которой устанавливается судом с учетом всех обстоятельств дела. При массовых нарушениях прав граждан можно будет объединяться и подавать коллективные иски.

«Гражданин будет обращаться за компенсацией через суд, это гражданское судопроизводство, в рамках которого действительно придется себя идентифицировать, — также отмечает он. — Но, по идее, здесь уже работают другие нормы. Здесь ситуация не станет хуже по сравнению с той, которая уже есть. Вполне предсказуемо, что крупные операторы восприняли такую инициативу несколько в штыки. Однако некоторые из них все-таки признают, что законодательство надо реформировать».

Эти меры, считает Савельев, будут стимулировать операторов обеспечивать комплаенс не на бумаге, а на деле; разгрузит Роскомнадзор и переместит акцент споров с операторами по поводу персональных данных из административной в

частноправовую плоскость. Кроме того, это будет стимулировать и иностранных операторов, ведущих бизнес в рунете, соблюдать законодательство РФ в области персональных данных, поскольку решение о взыскании компенсации в пользу частного лица может быть исполнено за рубежом, в отличие от взыскания административных штрафов. Эксперт уверен, что:

«…любая либерализация процессов обработки персональных данных, о которой так много говорится в контексте цифровой экономики, должна быть адекватно компенсирована соответствующими защитными механизмами для граждан, а не должна быть «игрой в одни ворота» со стороны операторов.

В конечном итоге, как только граждане поймут, что их данные имеют ценность, это станет отправной точкой для формирования ответственного отношения к распоряжению ими — трансформации, без которой цифровую экономику вряд ли возможно построить».

В Европе штрафы за утечку персональных данных более высокие — до 4% оборота компании. Это заставляет организации серьезнее подходить к защите данных пользователей. Предложенные меры сильно ситуацию в России не изменят, считает эксперт по информационной безопасности компании Cisco Systems Алексей Лукацкий.

«Это не совсем задача Роскомнадзора — заниматься именно расследованиями правонарушений, была ли утечка, по чьей вине произошла утечка, — говорит он. — Этим должны заниматься правоохранительные органы. А правоохранительные органы этим заниматься сейчас не могут, потому что в Уголовном кодексе отсутствуют соответствующие статьи. А вот вводить ли уголовную статью за утечки персональных данных — это очень непростой вопрос, это может привести к поиску ведьм и наказанию непричастных за возможные утечки. У нас нет штрафов за утечку, у нас есть наказание только за несоблюдение требований самого закона, то есть за отсутствие каких-то согласий, за отсутствие или нарушение правил обработки персональных данных. Ее пытались много лет назад внести, но тогда регуляторы сказали, что у них нет ни ресурсов, ни возможности реагировать на каждое заявление потенциальной жертвы. Здесь надо бороться с причиной, почему эти данные появляются, увеличивать активность именно правоохранительных органов в части проведения контрольных закупок, в части выявления тех, кто эти данные сливает, в части наказания тех, кто эти данные заказывает, приобретает, а потом ими торгует. И когда число дел возрастет и преступники увидят, что за торговлю персональными данными можно получить вполне реальные сроки, тогда ситуация сдвинется с мертвой точки». ***(Юристы предлагают штрафовать на 5 млн рублей за утечки данных // РосКомСвобода (https://roskomsvoboda.org/56159/). 10.03.2020).***

***

«Значительная часть оборудования для медицинской визуализации в США допускают утечку данных пациентов и делают больницы уязвимыми к кибератакам, которые могут нарушить их работу. По данным команды Unit 42 компании Palo Alto Networks, доля такой аппаратуры (от маммографов до

компьютерных томографов) составляет 83%, что на 56% выше по сравнению с 2018 годом.

Специалисты объясняют такой рост прекращением Microsoft поддержки операционной системы Windows 7. Медицинское оборудование имеет длительных срок эксплуатации, но если оно работает на уязвимых версиях ПО или устаревших операционных системах, хакеры могут получить доступ к данным, внедриться в сеть медучреждения и вызвать сбои в его работе.

В качестве примера исследователи привели случай, когда преступники инфицировали червем Conficker системы одной из больниц через уязвимый маммограф. Зараженными оказались еще один маммограф, рентгеновский аппарат, прибор для цифровой визуализации и прочее оборудование.

Перезагрузка систем не дала желаемого результата, и больнице пришлось потратить неделю на то, чтобы отключить устройства от интернета, установить нужные обновления безопасности и восстанавить устройства по одному.

О вредоносной программе Conficker стало известно в 2008 году. Тогда червь заражал устройства, работающие на Windows XP и более ранних версиях Windows, объединяя их в ботнет. К 2009 году вредонос заразил порядка 15 млн компьютеров в больницах правительственных учреждениях и компаниях. По оценкам Palo Alto, в 2020 году число зараженных устройств может достигнуть полумиллиона.

Для предотвращения кибератак специалисты рекомендуют организациям проводить регулярное сканирование сетей на наличие подключенных IoT-устройств и отключать ненужные; постоянно обновлять ПО устройств; отделить медицинское IoT-оборудование от обычной сети». ***(Преступники проникли в сеть больницы через уязвимый маммограф // SecurityLab.ru (https://www.securitylab.ru/news/505899.php). 15.03.2020).***

***

«На прошлых выходных иранский исследователь Нариман Гариб сообщил в своем Твиттере, что, согласно его исследованию, иранское приложение для тестирования на коронавирус собирало конфиденциальную информацию пользователей, в том числе и ту, которая не требовалась ему для работы. В числе прочих, приложение собирало сведения о местоположении в реальном времени.

Нариман использовал apklab.io, мобильную платформу для анализа угроз от компании Avast, чтобы определить происхождение приложения и проанализировать информацию, которую приложение собирало и отправляло на серверы разработчика. По словам Гариба, приложение было выпущено министерством здравоохранения Ирана. Информация о нем распространялась посредством SMS среди граждан Ирана. Власти поощряли пользователей устанавливать приложение и проводить тестирование, чтобы определить наличие у них симптомов коронавируса. Надо отметить, что корпорация Google уже удалила приложение из своего магазина Play Store, поскольку оно нарушает их условия.

10 марта Нариман написал в Твиттере, что сотрудник Министерства здравоохранения Ирана заявил, что использование приложения не было санкционировано его министерством. Тем не менее, тот же сотрудник признал, что

приложение было разработано министерством ИКТ Ирана. Далее Гариб пишет о том, что в тот же день министерство здравоохранения Ирана опубликовало разъяснение, в котором говорится, что «никто не имеет права получать личную информацию пользователей».

Николаос Хрисаидос, глава отдела исследования угроз и защиты для мобильных устройств Avast, проанализировал приложение и может подтвердить выводы Гариба: приложение собирает информацию, которая не нужна ему для функционирования.

Сначала приложение требует, чтобы пользователи регистрировались по номеру телефона. Приложение запрашивает разрешение на доступ к точному местоположению пользователя: это имеет смысл, поскольку местоположение пользователя можно использовать для рекомендации ближайшей больницы в случае, если есть подозрение на заражение вирусом. Но потом приложение запрашивает разрешение на доступ к ACTIVITY_RECOGNITION — этот параметр может использоваться для определения того, сидит ли пользователь устройства, гуляет или бегает. Как правило, это разрешение обычно запрашивают фитнес-приложения для отслеживания занятий спортом.

Подсказки, обнаруженные в коде, показывают, что приложение было разработано той же группой, которая разработала мессенджеры Talagram и Hotgram. Они были запрещены в Google Play Store в прошлом году. Как сообщается, и Talagram, и Hotgram были разработаны для иранского правительства: планировалось, что эти мессенджеры заменят Telegram, который известен своим надежным шифрованием и который запрещен правительством Ирана.

Помимо точного местоположения, приложение также отправляет на сервер разработчика информацию, которую ввел пользователь: его номер мобильного телефона, пол, имя, рост и вес». ***(Иранское приложение Coronavirus собирало личную информацию пользователей // IKSMEDIA.RU (http://www.iksmedia.ru/news/5650603-Iranskoe-prilozhenie-Coronavirus.html). 13.03.2020).***

***

«Пользователи браузера Blisk стали жертвами утечки информации, которая произошла по вине его создателей. Браузер создан, чтобы упростить работу веб-разработчикам, содержит продвинутые инструменты для них, позволяет работать над проектами совместно. Но исследователи информационной безопасности наткнулись на оставленный без защиты сервер Elasticsearch с данными о пользователях Blisk.

Сервер содержал 2,9 миллиона записей, похожих на логи действий, совершенных пользователями в браузере, в том числе приглашения друзей и регистрации. Также были видны email-адреса. Разработчики заявили, что закрыли доступ к базе, как только узнали о ситуации.

Платежные данные, идентификационная информация и пароли пользователей в доступ не попали. Однако информации, которая была доступна, может хватить для создания фишинговых рассылок и таргетированных атак, в том числе с применением приемов социальной инженерии». ***(Данные пользователей браузера***

Blisk оказались в свободном доступе // SecureNews (https://securenews.ru/blisk-browser-users-data-available/). 16.03.2020).

***

«Исследовательская команда ресурса CyberNews обнаружила в Google Cloud незащищенную базу данных объемом в 800 ГБ, в которой содержалось более 200 млн записей с подробной персональной информацией жителей США.

База данных включала в том числе полные имена, электронные адреса, даты рождения, сведения о кредитном статусе, домашние адреса и адреса недвижимого имущества, находящегося в залоге, данные о количестве детей и их поле, профили с информацией о персональных интересах, вкладах и пожертвованиях. Судя по всему, источником большинства записей являлось Бюро переписи населения США.

Кроме того, в базе хранились еще две папки, в одной из которых содержались записи об экстренных вызовах (даты, время вызова, местоположение и пр.) в одну из американских пожарных частей, во второй папке находился список 74 станций велопроката, принадлежащих компании Lyft.

Журналистам не удалось выяснить, кому принадлежала вышеупомянутая база данных, или определить, сколько времени она находилась в открытом доступе. 3 марта нынешнего года вся информация в базе данных была удалена, хотя сама БД по-прежнему доступна в Сети». ***(Открытая БД хранила подробные данные более чем 200 млн американцев // SecurityLab.ru (https://www.securitylab.ru/news/506072.php). 22.03.2020).***

***

«Пользователь одного из подпольных форумов опубликовал информацию о более чем 4,9 млн избирателей Грузии. Персональные данные, включая полные имена, информацию о дате рождения и домашних адресах, идентификационные номера и номера мобильных телефонов, были размещены в Сети в виде MDB-файла объемом 1,04 ГБ.

…утечку обнаружили специалисты из сервиса мониторинга и предотвращения утечек данных Under the Breach. База данных содержала 4 934 863 записей, но в нее также были включены данные миллионов умерших избирателей.

По словам пользователя, опубликовавшего базу данных, информация была взята с официального правительственного портала voters.cec.gov[.]ge. В настоящее время ресурс отключен.

Остается неизвестным, каким образом была получена данная информация — путем взлома web-сайта voters.cec.gov[.]ge или одноименного официального Android-приложения правительственного портала». ***(Данные почти 5 млн избирателей Грузии оказались в Сети // SecurityLab.ru (https://www.securitylab.ru/news/506237.php). 30.03.2020).***

***

«Дослідники компанії F-Secure озвучили список паролів, які фахівці з кібербезпеки найчастіше використовують хакери при атаках на так звані сервера-приманки…

Як це не дивно, але в першу чергу зломщики намагаються обійти захист за допомогою стандартної комбінацій admin . За популярністю їй також не поступаються default , 123456 і root .

Зловмисники можуть використовувати і код vivx , який по замовчуванні захищає DVR від китайської компанії Dahua, які використовуються в камерах спостереження по всьому світу. Серед інших поширених паролів також виявили 1001chin і tazZ @ 23495859 – заводські паролі для багатьох пристроїв, наприклад роутерів.

Більшість виявлених в F-Secure атак відбувалися від ботів або вірусів, які сканували IP-адреси. Такі спроби злому можуть виходити від будь-якого девайса, підключеного до інтернету, включаючи комп'ютери і навіть «розумні» зубні щітки та інші пристрої з інтернету.

Фахівці рекомендують замислюватися над безпекою всіх своїх гаджетів не тільки великим компаніям, але і рядовим користувачам. Багато людей забувають поміняти стандартні заводські налаштування після покупки.

Також для багатьох пристроїв можна скинути ім'я по-замовчуванню – це ускладнить потенційному зломщикові завдання по підбору пароля. Не варто забувати і про двохфакторну аутентифікацію і постійне оновлення ПЗ». ***(Лужна Софія. Названо найгірші паролі для гаджетів // TechnoPortal.com.ua (https://technoportal.com.ua/programy/43983). 06.03.2020).***

***

«Microsoft в новом обзоре разобрала тактику и методы некоторых наиболее опасных атак ramsomware за последние годы, управление которыми осуществлялось не автоматически, а операторами-людьми с клавиатуры.

Она предупреждает , что некоторые группы вымогателей в настоящее время используют те же навыки, что и хакеры, спонсируемые государствами, демонстрируя «обширные знания системного администрирования и распространённых ошибок в настройках безопасности сети», проводят долгую и тщательную разведку и затем атакуют разрушительными «полезными» нагрузками ransomware.

Согласно исследованиям Microsoft, такие преступные группы как REvil, Samas или SamSam, Doppelpaymer, Bitpaymer и Ryuk продемонстрировали способность беспрепятственно работать в сети и мало заботятся о скрытности своих действий.

Средний размер выкупа, требуемого Revil, составляет 260 тыс. долл., а строительная компания EMCOR Group на прошлой неделе сообщила, что атака Ryuk и последовавшие убытки от простоя ИТ ухудшили её финансовые результаты в IV квартале.

Группа Parinacota, отслеживавшаяся Microsoft на протяжении 18 месяцев, имеет более скромные запросы. Она выставляет счёт от 0,5 до 2 Bitcoins ($4500 — $18268) за компьютер, в зависимости от предполагаемой хакерами важности этой машины и её данных.

Команда Microsoft Threat Protection Intelligence Team рассказала в блоге о необычной тактике, используемой Parinacota для горизонтального распространения в скомпрометированных сетях. После проникновения в такую сеть, атакующие запускают в захваченной машине тесты на системную производительность и пропускную способность подключения к Интернету.

«Они определяют, соответствует ли машина определенным требованиям, прежде чем использовать ее для проведения удалённых (RDP) атак перебором паролей против других целей. Эта тактика, не встречавшаяся у других операторов ransomware, дает им доступ к дополнительной инфраструктуре, которая с меньшей вероятностью будет заблокирована», — говорится в блоге.

Некоторые компании играют на руку взломщикам, сознательно ослабляя свою внутреннюю защиту. Microsoft заявила, что ряд успешных вымогательских кампаний с человеческим участием велись против серверов, на которых антивирусное программное обеспечение и другие средства безопасности были намеренно отключены администраторами, возможно, для повышения производительности.

«Те же сервера часто не защищены брандмауэром и мультифакторной аутентификацией, имеют слабые доменные идентификаторы и нерандомизированные пароли для локального администрирования», — утверждает компания.

Своим обзором Microsoft пытается обосновать сотрудникам отделов кибербезопасности необходимость активации функций Windows Defender ATP, таких как защита от несанкционированного доступа, а также автоматических обновлений безопасности и облачного антивируса Microsoft». ***(Многие результативные атаки ransomware контролируются хакерами вручную // Компьютерное Обозрение (https://ko.com.ua/mnogie_rezultativnye_ataki_ransomware_kontroliruyutsya_hakerami_vruchnuyu_132196). 10.03.2020).***

***

«Компания ESET сообщила о новой фишинговой атаке на пользователей популярной платежной системы MasterCard.

Мошенники отправляют сообщение с «уведомлением об обновлении», и предупреждают о внедрении новой системы безопасности, в результате чего возможны отключения аккаунтов. Во избежание этого требуется перерегистрация. Потенциальной жертве предлагается перейти по ссылке и заполнить несколько форм, сообщив персональные данные, логин, пароль и другую важную информацию. Чтобы ввести пользователя в заблуждение, мошенники имитируют процесс верификации лица и даже отправляют верификационный код.

При этом сайт не имеет никакого отношения к MasterCard. Таким образом, киберпреступники собирают необходимые им сведения, позволяющие получить доступ к счетам жертв и похитить средства.

В первую очередь следует обратить внимание на адрес электронной почты, не совпадающий ни с одним из официальных адресов MasterCard. Настораживает и используемый почтовый сервер. Данная атака подтверждает то, что фишинг все еще актуален и опасен». ***(ESET обнаружила новую кибератаку на пользователей MasterCard // Компьютерное Обозрение (https://ko.com.ua/eset_obnaruzhila_nouyu_kiberataku_na_polzovatelej_mastercard_132203). 11.03.2020).***

***

«Как сообщают исследователи ИБ-компании FireEye, 76% от всех вымогательских атак на предприятия происходят вне рабочего времени. 49% атак происходят в ночное время в течение рабочей недели, еще 27% - на выходных. Такие данные были получены исследователями в результате расследований десятков инцидентов с участием вымогательского ПО в 2017-2019 годах.

Причина, по которой вымогатели атакуют в нерабочее время, очень простая – сотрудников IT-отделов, способных отразить атаку, нет на месте, а если и они есть, то очень непродолжительное время. По словам специалистов FireEye, подобным ночным атакам обычно предшествует продолжительная компрометация корпоративной сети. Киберпреступники взламывают сеть, проникают как можно в большее число систем, а затем вручную устанавливают и запускают вымогательское ПО. Промежуток между взломом сети и заражением ее вымогательским ПО (так называемое «время ожидания») в среднем составляет три дня.

Во всех исследованных FireEye случаях вымогательское ПО запускалось вручную самими злоумышленниками, а не автоматически сразу после заражения. Автоматический запуск программы после заражения – это устаревший способ, от которого злоумышленники уже отошли. Сейчас каждый образец вредоносного ПО находится под жестким контролем злоумышленников, которые тщательно выбирают момент для его запуска.

Microsoft называет такие инциденты «управляемые человеком атаки вредоносного ПО». Как сообщают специалисты FireEye, с 2017 года число подобных управляемых атак возросло на 860%. Microsoft и FireEye призывают компании вкладывать средства в развертывание правил, позволяющих выявлять инфекции во «время ожидания». ***(Ночь – излюбленное время вымогателей // SecurityLab.ru (https://www.securitylab.ru/news/505943.php). 17.03.2020).***

***

«Компьютерные сети Министерства здравоохранения и социальных служб США (Department of Health & Human Services) подверглись кибератаке преступников…

«Атака киберпреступников не увенчалась успехом, поэтому работа наших компьютерных систем не была затронута. Мы приняли все соответствующие защитные меры, чтобы предотвратить взлом или утечку данных», — заявил министр Минздрава США Алекс Азар (Alex Azar).

По словам главы ведомства, в настоящее время определяется источник атаки, однако, предположительно, инцидент мог быть спровоцирован злоумышленниками из иностранного государства.

По словам анонимных источников издания, злоумышленники в ходе атаки пытались перегрузить работу серверов Минздрава США миллионами обращений в течение нескольких часов.

Незадолго до атаки Совет национальной безопасности США предупредил пользователей о «поддельных» текстовых сообщениях от неизвестного отправителя о введении общенационального карантина. Как отметило издание, данные сообщения были связаны с кибератакой на Минздрав и попыткой распространения дезинформации». ***(Преступники атаковали компьютеры Минздрава США // SecurityLab.ru (https://www.securitylab.ru/news/505934.php). 17.03.2020).***

***

«На фоне распространения COVID-19 в Чехии Университетская больница города Брно была вынуждена отключить свои компьютерные системы и отложить запланированные операции из-за кибератаки.

Администрация больницы не уточняет характер кибератаки, однако она оказалась достаточно серьезной для того, чтобы отложить запланированные хирургические операции и направить новоприбывших пациентов в расположенную неподалеку больницу Святой Анны, сообщает местная пресса.

По словам директора медучреждения Ярослава Штербы (Jaroslav Štěrba), кибератака произошла в пятницу, 13 марта, около двух часов ночи (четырех часов ночи по московскому времени). Компьютерные системы стали одна за другой выходить их строя, поэтому пришлось отключить всю IT-инфраструктуру больницы. Кибератака также затронула детское и родильное отделения.

В настоящее время Национальный центр кибербезопасности Чехии совместно с сотрудниками полиции и IT-отдела медучреждения работают над восстановлением компьютерных систем. Как сообщил Штерба, больница продолжает проводить тестирования образцов, взятых у пациентов с подозрением на коронавирус». ***(Тестирующая на коронавирус лаборатория подверглась кибератаке // SecurityLab.ru (https://www.securitylab.ru/news/505895.php). 14.03.2020).***

***

«Европейская электросетевая организация European Network of Transmission System Operators for Electricity (ENTSO-E) сообщила о нападении киберпреступников на ее компьютерные системы. По словам организации, критические системы управления энергоснабжением не пострадали в результате инцидента.

ENTSO-E базируется в Брюсселе (Бельгия) и ее членами являются 42 системных оператора передачи электроэнергии в 35 европейских странах. Основной обязанностью ENTSO-E является обеспечение координации между ее операторами, чтобы обеспечить стабильную электроэнергию на рынке электроэнергии ЕС.

ENTSO-E не уточнила, когда была зафиксирована кибератака, и какая группировка может быть ответственна за нее.

Как сообщил один национальный оператор энергосистемы Финляндии Fingrid Oyj изданию CyberScoop, хотя атака «не затронула клиентов Fingrid или другие заинтересованные стороны», инцидент может задержать выпуск EIC-кодов (Energy Identification Code), которые используются для поддержки торговли на европейском рынке электроэнергии». ***(Киберпреступники атаковали компьютерные системы ENTSO-E // SecurityLab.ru (https://www.securitylab.ru/news/505799.php). 11.03.2020).***

***

«Мережа Necurs відповідальна за низку кримінальних афер, викрадення персональних даних та розсилання фальшивих листів.

Як пише BBC, шахраї використали мережу ботів, щоб віддалено встановлювати на підключені до інтернету девайси шкідливе програмне забезпечення.

Надалі завдяки цій програмі здійснювалися масові спам-розсилки, збиралися дані про активність користувачів чи видалялася певна інформація з їхніх пристроїв. Про це йдеться у блозі компанії Microsoft. Ймовірно, керували мережею з Росії.

«Мережа Necurs — одна з найбільших мереж в екосистемі шкідливих спам-розсилок, жертви якої є майже у всіх країнах світу. Наприклад, протягом 58-денного періоду нашого розслідування, ми спостерігали, що один із заражених Necurs комп’ютерів надіслав загалом 3,8 мільйона спам-листів понад 40,6 мільйонам потенційних жертв», — пише компанія.

Віце-президент Microsoft з питань безпеки та довіри клієнтів Том Берт (Tom Burt) зауважив, що робота щодо блокування цієї мережі під назвою Necurs тривала вісім років. Для цього компанія співпрацювала з партнерами у 35 країнах.

«Вжиті заходи заблокують злочинцям, які стоять за цією мережею, можливість використовувати ключові елементи її інфраструктури для здійснення кібератак», — зазначив він.

BBC зазначає, що Necurs була однією з найбільших шкідливих мереж у світі, але далеко не єдиною.

Видання наводить такі ознаки того, що ваш пристрій може бути заражений шкідливою програмою: програми починають працювати повільніше або їхнє відкриття займає більше часу; комп'ютер регулярно «зависає» і потребує перезавантаження; місце на жорсткому диску комп'ютера раптово заповнюється; контактам з вашого облікового запису надсилаються спам-листи». ***(Microsoft заблокувала шахрайську інтернет-мережу. Як визначити, що ваш девайс інфіковано? // MediaSapiens (https://ms.detector.media/kiberbezpeka/post/24309/2020-03-11-microsoft-zablokuvala-***

shakhraisku-internet-merezhu-yak-viznachiti-shcho-vash-devais-infikovano/). 11.03.2020).

***

«В течение нескольких месяцев киберпреступники имели доступ к компьютерной сети канцелярии президента Чехии Милоша Земана и похищали информацию… IT-специалисты выяснили, что данные из компьютерной сети передавались на зарубежные IP-адреса. Характер похищенной информации не раскрывается. В настоящее время эксперты Управления по охране частных сведений проводят расследование.

Пресс-секретарь президента Чешской Республики Йиржи Овчачек отказался комментировать сложившуюся ситуацию. Управление по кибернетической безопасности, Национальный комитет по борьбе с оргпреступностью и Военная разведка также отказались подтвердить или опровергнуть свое участие в расследовании…». ***(Неизвестные похищали данные из компьютерной сети канцелярии президента Чехии // SecurityLab.ru (https://www.securitylab.ru/news/505582.php). 04.03.2020).***

***

«Телекоммуникационные компании чаще всего подвергались кибератакам со стороны китайских киберпреступников в 2019 году. К такому выводу пришли специалисты из компании CrowdStrike по результатам анализа спонсируемых государством и финансово-мотивированных операций, зафиксированных в прошлом году.

Многие из атак на телекомпании были приписаны китайским киберпреступным группировкам, таким как Wicked Panda (APT41), Emissary Panda (APT27, TG-3390, Bronze Union и Lucky Mouse), и Lotus Panda (Thrip).

По словам CrowdStrike, атакованные телекоммуникационные компании могут быть использованы преступниками для сбора разведывательных данных и дальнейшего осуществления атак на другие организации.

Например, в ходе одной из атак в прошлом году китайская кибергруппировка APT41 использовала вредоносный инструмент под названием MESSAGETAP для мониторинга и перехвата SMS-трафика с серверов коммуникационных компаний с целью кражи контента SMS-сообщений. Преступники внедрили инструмент в сети некоего неназванного телекоммуникационного провайдера в целях шпионажа.

«Многочисленные атаки на системы телекоммуникационных компаний в Азии демонстрируют постоянный интерес преступников к соседям по региону. Хотя некоторые атаки преследовали экономические цели, другие целенаправленные проникновения в телекоммуникации использовались Китаем для отслеживания уйгуров в Центральной и Юго-Восточной Азии. Подобная деятельность была нацелена на операторов связи в Турции, Казахстане, Индии, Таиланде и Малайзии, отображая стремление к отслеживанию китайских противников», — отметили эксперты.

По словам специалистов, ориентация на телекоммуникационный сектор, особенно в регионах Центральной и Юго-Восточной Азии, также дополняет план

Китая по развитию цифрового шелкового пути. Данная инициатива направлена на расширение и углубление цифровых соединений с другими странами посредством строительства трансграничных и подводных оптических кабелей, соединительных линий и спутниковых информационных каналов, а также развития мобильных сетей пятого поколения (5G)». ***(Телекомкомпании все чаще становятся целью китайских киберпреступников // SecurityLab.ru (https://www.securitylab.ru/news/505544.php). 04.03.2020).***

***

«Крупная международная юридическая компания Epiq Global стала жертвой кибератаки с использованием вымогательского ПО. Согласно заявлению Epiq Global, консультирующей банки, крупные кредитные организации и правительства разных стран, инцидент имел место 29 февраля нынешнего года.

«В рамках нашего всеобъемлющего плана реагирования на инциденты в целях сдержать угрозу мы сразу же отключили свои системы по всему миру и начали работу со сторонней фирмой, занимающейся проведением криминалистической экспертизы, в рамках независимого расследования. Наша техническая команда тесно сотрудничает со сторонними экспертами мирового класса, чтобы решить эту проблему и максимально быстро вернуть наши системы в безопасное состояние» - говорится в заявлении компании.

По словам осведомленного источника, пожелавшего сохранить анонимность, компьютеры во всех 80 штаб-квартирах компании по всему миру были заражены вымогательским ПО. Согласно внутреннему распоряжению администрации Epiq Global, сотрудники компании не могут посещать офисы без одобрения руководства, пишет TechCrunch. В офисах работникам рекомендуется не подключать устройства к сети и отключать Wi-Fi на своих ноутбуках, не доезжая до парковки возле офисного здания.

По словам источника, корпоративные компьютеры работают под управлением устаревших версий Windows, и «нигде не установлены обновления».

О каком вымогательском ПО идет речь, источник не уточняет. По уверению Epiq Global, никаких свидетельств того, что данные были похищены, нет». ***(Вымогательское ПО вынудило международную юркомпанию отключить свои системы // SecurityLab.ru (https://www.securitylab.ru/news/505539.php). 03.03.2020).***

***

«Киберпреступники пытались проникнуть в компьютерные системы Всемирной организации здравоохранения в начале марта нынешнего года. По словам директора по информационной безопасности ВОЗ Флавио Аджо (Flavio Aggio), личность не удалось установить, а их попытка была неудачной. Попытки взлома против организации и ее партнеров резко возросли, поскольку они борются с пандемией коронавирусной инфекции, сообщило информагентство Reuters.

По словам ИБ-специалиста Александра Урбелиса (Alexander Urbelis) из юридической фирмы Blackstone Law Group, которая отслеживает регистрацию

подозрительных доменов, первая попытка взлома была зафиксирована 13 марта, когда группа злоумышленников запустила вредоносный сайт, имитирующий внутреннюю систему электронной почты ВОЗ.

Два источника агентства сообщили, что в организации данной атаки заподозрена киберпреступная группировка, известная как DarkHotel, которая занимается кибершпионажем по крайней мере с 2007 года.

«Наблюдается значительный рост целевого воздействия и кибератак, направленных на ВОЗ», — отметил Аджо.

Чиновники и эксперты по кибербезопасности предупреждают, что самые разные киберпреступники пытаются извлечь выгоду из всемирной паники по поводу распространения коронавируса. Как отметил Урбелис, он ежедневно фиксирует тысячи web-сайтов, посвященных пандемии коронавируса, многие из которых являются злонамеренными…». ***(Киберпреступники пытались взломать системы ВОЗ // SecurityLab.ru (https://www.securitylab.ru/news/506121.php). 24.03.2020).***

***

«Компанії FireEye і IBM X-Force, що працюють у сфері комп'ютерної безпеки, розповіли про зростання активності хакерів з Росії, Китаю, Північної Кореї, В'єтнаму, Індії, Бразилії і США, відзначивши, що пандемія коронавірусу відкрила нові можливості для злочинів в інтернеті…

Старший менеджер з аналізу кібершпіонажу компанії FireEye Бенджамін Рід розповів про хакерські атаки на портали державних органів, розсилки шкідливого спаму і фінансових махінаціях. У багатьох подібних випадках, за словами експерта, використовується тема пандемії коронавіруса і експлуатується страх людей перед захворюванням.

Компанії та державні органи, що протистоять кіберзлочинності, частіше за все стикаються з розсиланням листів, нібито відправлених з адрес служб охорони здоров'я, які повідомляють користувачем якусь "нову важливу інформацію" про коронавирус, карантинні заходи і методи захисту від захворювання. Такі листи заражають комп'ютери, дозволяють поширювати подібні послання далі, або дають доступ злочинцям до інформації, в тому числі й фінансової.

"Ми знаємо про випадки розсилки листів від імені ВООЗ, Міністерств охорони здоров'я Китаю і Японії, а також відправки посилань на інтернет-магазини, які нібито пропонують засоби захисту від коронавіруса, — розповів аналітик IBM X-Force Ашкан Віла. — Вони використовують страх і панічні настрої, які дозволяють подолати природний скептицизм, що виникає в нормальних умовах, коли люди отримують подібні повідомлення".

Фахівці з кібербезпеки закликають не проходити за посиланнями з підозрілих повідомлень і не відкривати вкладень в таких листах, а також намагатися перевірити адресатів, щодо яких є хоч найменші сумніви.

"Не варто використовувати робочу електронну пошту в особистих цілях, наприклад для реєстрації у соцмережах, підписок, спілкування в інших сервісах, — радить Віла. — Інакше висока вірогідність, що цим скористаються кіберзлочинці".

Одна з недавніх відомих кібератак була спрямована на сайт Міністерства охорони здоров'я і соціальних служб США. Пандемія коронавірусу стимулювала не тільки активність хакерів — в Китаї штучний інтелект використовують для оцінки зараження, в Україні діє онлайн-сервіс для відстеження поширення коронавірусу, а в інтернеті з'явився міжнародний онлайн-бар, дозволяє людям, що сидять на карантині, скоротати час у спілкуванні і завести нові знайомства». ***(Експерти з кібербезпеки розповіли про те, як хакери користуються епідемією коронавірусу // Дзеркало тижня. Україна (https://dt.ua/TECHNOLOGIES/eksperti-z-kiberbezpeki-rozpovili-pro-te-yak-hakrei-koristuyutsya-epidemiyeyu-koronavirusu-341987_.html). 19.03.2020).***

***

«Эксперты компании Trustwave опубликовали отчет, в котором рассказали, как неназванной американской компании из сферы гостиничных услуг прислали по почте поддельную подарочную карту BestBuy вместе с вредоносной USB-флешкой. В сопровождающем письме было сказано, что накопитель нужно подключить к компьютеру, чтобы получить доступ к списку товаров, для которых можно использовать подарочную карту. Подобные направленные атаки BadUSB встречаются на практике крайне редко.

Напомню, что BadUSB — это класс атак, который позволяет при помощи девайсов вроде Rubber Ducky захватить контроль над многими устройствами, у которых есть порт USB. Таким образом можно эмулировать любую периферию, но чаще всего преступники подделывают клавиатуру.

Эксперты Trustwave рассказывают, что сотрудники компании-жертвы сочли письмо подозрительным и обратились к ним за помощью в расследовании инцидента.

Как выяснили исследователи, после подключения BadUSB к тестовой рабочей станции флешка запустила команду PowerShell (посредством серии автоматических нажатий клавиш). В свою очередь эта команда загрузила более объемный PowerShell- скрипт с удаленного сайта, а затем установила на тестовую машину малварь — бота на основе JScript.

«На момент проведения анализа нам не удалось обнаружить другого подобного штамма малвари. Вредоносная программа нам неизвестна. Сложно сказать, была ли она создана по индивидуальному заказу, но, вероятно, так и есть, потому как она не очень широко распространена и, похоже, таргетирована», — рассказывают специалисты.

Эксперты Trustwave рассказали изданию ZDNet, что уже после первоначального анализа файл, похожий на анализируемую малварь, был загружен в VirusTotal. Согласно последующему анализу, проведенному специалистами Facebook и «Лаборатории Касперского», файл, вероятно, связан с известной хакерской группировкой FIN7 (она же Carbanak, Carbon Spider, Anunak). Неясно, кто загрузил файл на VirusTotal. Возможно, это сделали другие ИБ-специалисты, которые так же расследуют атаку BadUSB на другую жертву.

«Подобные атаки [BadUSB] часто моделируются во время пентестов и используются во время учений red team. Но в реальном мире атаки такого типа

встречаются гораздо реже», — говорят эксперты Trustwave…». ***(Мария Нефёдова. Американская компания подверглась редкой атаке через BadUSB // Хакер (https://xakep.ru/2020/03/27/practical-badusb/). 27.02.2020).***

***

Діяльність хакерів та хакерські угруповування

«IT-специалисты словацкой компании ESET – разработчика антивирусного программного обеспечения и эксперта в области кибербезопасности – предупреждают о новой серии атак, совершенных группой кибершпионов Turla, которые направлены на сайты правительственных учреждений в мире, сообщается на сайте компании.

«Компания ESET — лидер в области информационной безопасности — обнаружила новую активность группы Turla, которая направлена на правительственные сайты. На этот раз киберпреступники применяют методы социальной инженерии, используя фальшивое обновление Adobe Flash в качестве приманки для загрузки вредоносного программного обеспечения», - говорится в сообщении. Согласно сообщению, в результате подобных атак было инфицировано не менее четырех веб-сайтов, два из которых принадлежат правительству Армении. При этом, заражены эти веб-порталы были, минимум, с начала 2019 года. Специалисты ESET предупредили национальное подразделение CERT Армении. Таким образом, исследователи сделали вывод, что главной целью киберпреступников являются чиновники и политики. В ходе зафиксированных кибератак, злоумышленники заражают выбранный сайт вредоносным программным обеспечением, которое впоследствии передается на устройства посетителей ресурса, по тем или иным причинам интересующих киберпреступников. Потому жертвы подобной кибератаки составляют ограниченное количество. После первоначального заражения операторы Turla получают полный доступ к устройствам жертв. Специалистам ESET не удалось определить, что делали хакеры на зараженных устройствах, но, как правило, они пытаются похитить конфиденциальные документы. По данным ESET, в ходе последних атак киберпреступники группы Turla использовали совершенно новый бэкдор, который получил название PyFlash. По мнению экспертов ESET, в этом вредоносном программном обеспечении авторы Turla впервые использовали язык Python. Командный сервер посылает бэкдору команды для загрузки файлов, выполнения команд Windows, а также запуска и удаления вредоносного программного обеспечения. В компании добавили, что группа киберпреступников Turla является активной в большей части мира, но, в основном, ее деятельность направлена на страны Восточной Европы и Восточной Азии. Основными ее целями являются правительственные и военные организации. Работает группа кибершпионов уже более десяти лет. Как сообщал УНИАН, ранее специалисты компании ESET выявили новые атаки сложного банковского трояна Guildma, способного похищать данные для входа в учетные записи электронной почты, электронных магазинов и стриминговых сервисов. По данным ESET, в Украине

ежедневно фиксируется около 300 тыс. новых киберугроз для информационной безопасности. При этом, найти хакеров-злоумышленников крайне сложно, компаниям остается лишь проводить ежеминутные мониторинги на предмет выявления киберугроз с целью их дальнейшего блокирования. Компания ESET – ведущий разработчик решений в области компьютерной безопасности и эксперт в сфере IT-безопасности. Компания была основана в 1992 году в Словакии и на сегодня представлена более, чем в 180 странах мира». ***(В ESET предупредили о новых кибератаках на правительственные сайты в мире // УНИАН (https://www.unian.net/science/10914500-v-eset-predupredili-o-novyh-kiberatakah-na-pravitelstvennye-sayty-v-mire.html). 13.03.2020).***

***

«Компьютерная группа реагирования на чрезвычайные ситуации (CERT) Франции предупредила о новой киберпреступной группировке, атакующей местные органы власти с помощью вымогательского ПО.

Согласно уведомлению CERT, участились случаи заражения сетей местных органов власти новым вымогательским ПО Mespinoza (другое название Pysa). Впервые вредонос был обнаружен в октябре 2019 года – в это время в интернете стали появляться сообщения о неизвестном вымогателе, шифрующем файлы на компьютерах жертв, добавляя расширение .locked. Спустя два месяца был обнаружен новый вариант Mespinoza, добавляющий к имени файла расширение .pysa.

До недавнего времени вымогатель Mespinoza/Pysa атаковал преимущественно компании. Его операторы были заинтересованы в крупных жертвах, способных заплатить кругленькую сумму. Теперь же киберпреступники нацелились на французские организации.

Как происходит заражение, пока неизвестно. По словам специалистов CERT, некоторые факты указывают на то, что злоумышленники осуществляют брутфорс-атаки на консоли управления и учетные записи Active Directory, а затем похищают учетные данные. Некоторые ставшие жертвами Mespinoza организации также зафиксировали неавторизованное RDP-подключение к своим контроллерам домена и обнаружили подозрительные Batch- и PowerShell-скрипты.

Операторы Mespinoza также используют версию инструмента PowerShell Empire, предназначенного для проведения тестов на проникновение, блокируют работу антивирусных решений, а в некоторых случаях даже деинсталлируют Windows Defender. Как минимум в одном случае новый вариант вымогателя добавлял к имени файла расширение .newversion.

Специалисты изучили используемый Mespinoza алгоритм шифрования и не нашли каких-либо уязвимостей, которые позволили бы расшифровать файлы без ключа (то есть, без уплаты выкупа)». ***(Новый вымогатель атакует французские органы власти // SecurityLab.ru (https://www.securitylab.ru/news/506001.php). 19.03.2020).***

***

«В последние годы таинственная киберпреступная группировка почти ежедневно выпускала вредоносные инструменты, предназначенные для заражения других преступников и получения доступа к их компьютерам. Согласно опубликованному отчету специалистов из компании Cybereason, троянские инструменты были заражены версией вредоносного ПО njRAT.

«Вместо того, чтобы активно взламывать системы, они просто заражают инструменты, распространяют их бесплатно и взламывают тех, кто пользуется этими программами», — пояснил исследователь Амит Серпер (Amit Serper).

Команда Cybereason Nocturnus обнаружила более 1000 образцов njRAT в ходе анализа данной группировки, но кампания оказалась намного масштабнее, чем они предполагали. Некоторые образцы существуют годами, а новые версии публикуются почти ежедневно. По словам экспертов, инструменты распространяются в Сети на подпольных форумах и в блогах, посвященных обмену бесплатным вредоносным ПО.

Обнаруженные экспертами зараженные инструменты включали скреперы сайтов, сканеры эксплоитов, генераторы поисковых запросов в Google, инструменты для выполнения автоматических SQL-инъекций, осуществления брутфорс-атак и проверки достоверности утечек учетных данных.

Специалисты также обнаружили троянские версии браузера Chrome, содержащие троян для удаленного доступа njRAT.

Большинство зараженных программ были настроены на обратную связь с одним из двух доменов. Чаще всего использовался домен capeturk.com, зарегистрированный с использованием учетных данных жителя Вьетнама. Также многие из троянских утилит были загружены на сервис VirusTotal с вьетнамского IP-адреса». ***(Вьетнамская группировка годами атаковала других киберпреступников // SecurityLab.ru (https://www.securitylab.ru/news/505686.php). 10.03.2020).***

***

«Специалисты «Лаборатории Касперского» обнаружили новую, ранее неизвестную киберпреступную группировку, которая в настоящее время нацелена на промышленные объекты на Ближнем Востоке.

Группировка получила название WildPressure. Основным оружием преступников является новый бэкдор под названием Milum, написанный на языке C++, который предоставляет его операторам полный контроль над зараженным хостом.

Компьютерные системы, зараженные Milum, впервые были зафиксированы исследователями в августе 2019 года, но позже были обнаружили следы инфекций вплоть до 31 мая 2019 года. Как показали результаты анализа кода, Milum был скомпилирован двумя месяцами ранее — в марте 2019 года.

По словам специалистов, Milum был составлен из относительно нового кода, без пересечений или сходств с любой другой APT-группировкой. В частности, вредонос способен выполнять следующие функции: загружать и выполнять команды своего оператора, собирать различную информацию с целевого устройства и отправлять ее на C&C-сервер и обновляться до более новой версии.

Эксперты предполагают, что большинство целей новой вредоносной кампании находятся на Ближнем Востоке, поскольку к C&C-серверу Milum были подключены иранские IP-адреса». ***(Новая APT-группа нацелилась на промышленный сектор на Ближнем Востоке // SecurityLab.ru (https://www.securitylab.ru/news/506145.php). 25.03.2020).***

***

«Компания Prevailion предупредила, что русскоязычная хак-группа TA505 (она же Evil Corp) стала активно использовать легитимные инструменты (в дополнение к малвари) для атак на немецкие компании. Напомню, что эту группировка в первую очередь известна благодаря использованию трояна Dridex и вымогателя Locky, но также применяет множество других вредоносных программ, включая BackNet, Cobalt Strike, ServHelper, Bart, FlawedAmmyy, SDBbot RAT, DoppelPaymer и так далее.

Исследователи из Prevailion обнаружили, что с лета 2019 года TA505 проводит кампанию, ориентированную на немецкие фирмы. Хакеры рассылают своим целям письма с фальшивыми резюме для приема на работу. В этих письмах содержится вредоносное вложение, предназначенное для кражи учетных данных и данных кредитных карт.

Но если в 2019 году злоумышленники использовали для шифрования файлов потерпевших доступный на рынке вымогатель, то в более недавних операциях они перешли на коммерческий инструмент для удаленного администрирования NetSupport, размещенный в Google Drive.

Эксперты предупреждают, что посредством использования таких легитимных инструментов, которые вряд ли получится обнаружить традиционным защитными решениями, злоумышленники могут выполнять широкий спектр действий, в том числе похищать файлы, делать скриншоты и записывать звук.

Так, на начальном этапе атаки код из вредоносного резюме запускает скрипт для извлечения дополнительных пейлоадов и сбора данных о компьютере жертвы (список установленных программ, имя компьютера, домена и так далее). Затем малварь пытается собрать сохраненные учетные данные из браузеров и почтовых клиентов, файлы cookie и данные кредитных карт.

Украденные учетные данные архивируются и отправляются на управляющий сервер злоумышленников, а затем создается запланированное задание, а BAT-файл удаляет все следы атаки.

Исследователи отмечают, что летом 2019 года атаки также имели вымогательский компонент: диски на локальных машинах шифровались с использованием открытого ключа GPG, теневые копии удалялись, а некоторые данные переправлялись на адрес zalock[@]airmail.cc.

Для новых же атак используется загрузчик (по-видимому, rekt), который был разработан для связи с Google Drive и загрузки дополнительных файлов. Пейлоад второго этапа атаки был идентифицирован как коммерческое приложение NetSupport для удаленной работы.

Некоторые из обнаруженных вариантов rekt датированы апрелем 2019 года. Также исследователи выявили образцы, подписанные цифровой подписью, которая

использовалась и для подписи двух троянов FlawwedAmmy. Их тоже ранее связывали с TA505, так что исследователи уверенно заявляют, что за обнаруженными атаками стоит именно названная хак-группа». ***(Мария Нефёдова. Группировка TA505 использует легитимные инструменты для атак на немецкие фирмы // Xakep (https://xakep.ru/2020/03/24/ta505-germany/). 25.03.2020).***

***

«Как минимум с мая прошлого года APT-группа Fancy Bear (другие названия APT28 и Pawn Storm) использует в своих операциях взломанные электронные почтовые ящики, принадлежащие руководству оборонных предприятий на Среднем Востоке и транспортных компаний, а также представителей органов власти.

Как пояснил исследователь безопасности компании Trend Micro Фейке Хакеборд (Feike Hacquebord), злоумышленники подключаются к выделенному серверу с помощью опции OpenVPN, предоставляемой коммерческим VPN-сервисом, а затем с помощью скомпрометированных учетных данных авторизуются в почтовых сервисах и рассылали вредоносные письма.

Учетные записи высокопоставленных лиц участники APT-группы взломали в ходе предыдущих кампаний. Зачем им понадобилось так рисковать и выдавать результаты своих побед, используя взломанную почту руководителей компаний, пока неизвестно. По словам Хакеборда, скорее всего, злоумышленники готовы пожертвовать сведениями о своих прошлых кампаниях ради возможности обойти спам-фильтры.

«Однако мы не заметили значительных изменений в успешной доставке входящих сообщений в групповых спам-рассылках, что затрудняет понимание причин изменения методологии», - отметил исследователь.

Согласно предположению Хакеборда, изменения в методологии могут быть связаны с неизвестными новыми техниками, появившимися в распоряжении Fancy Bear, не предполагающими использование вредоносного ПО». ***(Fancy Bear использует в новой кампании взломанную электронную почту // SecurityLab.ru (https://www.securitylab.ru/news/506055.php). 20.03.2020).***

***

«Американська компанія у галузі кібербезпеки FireEye заявила про сплеск кібершпіонажу з боку хакерського угруповання, імовірно, пов'язаного з Китаєм… Підвищення активності почалося наприкінці січня, коли коронавірус почав ширитись за межами Китаю. І за останні кілька тижнів випадки кібершпіонажу також почастішали.

Як йдеться у доповіді FireEye, хакерське угруповання APT41 пожвавило свою діяльність з 20 січня. Вони спрямували свої атаки на 75 компаній – від промислових підприємств і медіаорганізацій до медичних установ і некомерційних організацій США, Канади, Великої Британії, Мексики, Саудівській Аравії, Сінгапурі та інших країн. Назви компаній не розкривають.

Представник компанії FireEye Крістофер Глаєр пов'язує це як зі спалахом COVID-19, так і з торговельною війною між Китаєм і США й вважає це однією «з наймасштабніших кампаній з боку китайських кібершпигунів за останні роки».

Китайське міністерство закордонних справ прямо не коментує доповідь FireEye, але опублікувало заяву, в якій йдеться, що Китай став «жертвою кіберзлочинності й кібератаки». ***(Китайські хакери здійснили одну з наймасштабніших атак на світові компанії після сплеску вірусу – експерти у США // Радіо Свобода (https://www.radiosvoboda.org/a/30510397.html). 26.03.2020).***

***

Вірусне та інше шкідливе програмне забезпечення

«…Хрестовий похід Microsoft з кібербезпеки триває. Після восьми років роботи Cyber Threat Intelligence у співпраці з 35 країнами готується до завершення ботнету Necurs, розташованого в США, але російського походження, який заразив мережу з дев'яти мільйонів комп'ютерів по всьому світу і поширив шкідливе ПЗ.

У четвер, 5 березня, Окружний суд США в східному окрузі Нью-Йорка видав постанову, що дозволяє Microsoft контролювати інфраструктуру на базі США, використовувану Necurs для розповсюдження шкідливих програм і зараження комп'ютерів жертв. Цим судовим позовом і спільними зусиллями, пов'язаними з приватно-державними партнерствами по всьому світу, Microsoft проводить заходи, які не дозволять творцям Necurs реєструвати нові домени для майбутніх атак.

Microsoft також вживає додаткові кроки у партнерстві з інтернет-провайдери (ISP) та іншими організаціями по всьому світу, щоб позбавити комп'ютери своїх клієнтів від шкідливих програм, пов'язаних з ботнетом Necurs…» ***(Microsoft пообіцяла покласти край небезпечному вірусу, мільйони пристроїв під загрозою // Знай.ua (https://techno.znaj.ua/299808-microsoft-poobicyala-poklasti-kray-nebezpechnomu-virusu-milyoni-pristrojiv-pid-zagrozoyu). 12.03.2020).***

***

«Специалисты из «Лаборатории Касперского» обнаружили две новые вредоносные программы для Android, получившие названия Cookiethief и Youzicheng, способные похищать cookie-файлы, сохраненные в браузере на смартфонах и в приложениях популярных социальных сетей, в частности Facebook. Таким образом преступники могут незаметно перехватить контроль над учетной записью жертвы в социальной сети и распространять контент от ее имени.

Злоумышленники разработали два вредоноса с похожим стилем написания кода и использующих один и тот же C&C-сервер. Оказавшись на устройстве, троян Cookiethief получает права суперпользователя и передает C&C-серверу cookie-файлы браузера и установленного приложения социальной сети.

Но одного только идентификатора сессии недостаточно для перехвата контроля над чужим аккаунтом. Например, системы защиты некоторых web-сайтов предотвращают подозрительные попытки авторизации в системе. Для подобных

случаев преступники создали второй вредонос — Youzicheng. Он способен запустить прокси-сервер на телефоне и предоставить злоумышленникам доступ в интернет с устройства жертвы для обхода мер безопасности.

Как отметили эксперты, вредоносы не эксплуатируют уязвимости в мобильном браузере или приложении соцсети, и злоумышленники могут похитить cookie-файлы с любого сайта.

«Объединив два типа атак, злоумышленники нашли способ получать контроль над аккаунтами пользователей, не вызывая подозрений. Это относительно новая угроза, пока ей подверглись не более тысячи человек. Это число растет и, скорее всего, будет продолжать расти, учитывая, что web-сайтам трудно обнаруживать такие атаки», – пояснили специалисты». ***(Обнаружены новые вредоносы для кражи cookie-файлов на Android // SecurityLab.ru (https://www.securitylab.ru/news/505893.php). 13.03.2020).***

***

«Китайские киберпреступники продолжают совершенствовать троян для удаленного доступа (RAT), появившийся еще десять лет назад. Как сообщают специалисты Cisco Talos, троян Bisonal до сих пор используется в атаках на Россию, Японию и Южную Корею.

По словам исследователей, такая преданность старым инструментам редко встречается среди киберпреступников. Как правило, хакеры регулярно пополняют свой арсенал новым ПО и не занимаются улучшением старого (Bisonal был скомпиллирован 24 декабря 2010 года).

Согласно отчету, предоставленному специалистами Cisco Talos изданию ZDNet до публикации, трояном Bisonal пользуется APT-группа Tonto Team, предположительно связанная с китайскими военными. По данным исследователей из FireEye, Tonto Team имеет отношение к Бюро технической разведки военного округа Шэньян и участвовала в атаках на используемый Южной Кореей противоракетный комплекс THAAD в 2017 году.

Помимо Южной Кореи, главными целями APT-группы также являлись Россия и Япония. Специалисты Cisco Talos обнаружили, что Bisonal использовался в недавних кампаниях против этих стран с главным акцентом на русскоговорящих пользователях.

«У кампаний были очень специфические цели, судя по которым модно предположить, что их конечная игра была больше связана со сбором оперативных разведданных и шпионажем», - сообщили в Cisco Talos.

На первом этапе атаки жертве приходит фишинговое письмо с вредоносным документом. В атаках 2009 года использовались документы, посвященные исследованиям, военным технологиям, южнокорейскому правительству и российским компаниям. Теперь же исследователи обнаружили русскоязычные RTF-документы и такие же документы на корейском, загружающие на атакуемую систему файл winhelp.wll, являющийся дроппером трояна Bisonal. Документы на русском посвящены исследованиям, а на корейском – правительству». ***(Китайские кибершпионы атакуют Россию с помощью десятилетнего трояна // SecurityLab.ru (https://www.securitylab.ru/news/505623.php). 06.03.2020).***

***

«Специалисты из компании FireEye предупредили о распространении вредоносных инструментов с возможностями нацеливания на автоматизированные системы управления (АСУ ТП). Эксперты проанализировали все вредоносные инструменты для взлома АСУ ТП, выпущенные в последние годы.

«Хотя некоторые из инструментов, включенных в наш список, были созданы еще в 2004 году, большая часть разработок велась в течение последних 10 лет», — отметили эксперты.

По словам специалистов, большинство инструментов не зависит от поставщика и способно сканировать общие индикаторы, обычно присутствующие во всех сетях АСУ ТП. FireEye также нашла инструменты, разработанные для взлома систем конкретных поставщиков АСУ ТП. В данном случае в зоне риска оказался оказалась Siemens, поскольку 60% специализированных инструментов предназначались для ее продуктов.

Исследователи нашли инструменты для самых разных целей: для сканирования сетей на наличие устройств, специфичных для АСУ ТП, для эксплуатации уязвимостей в оборудовании, для взаимодействия с ячеистыми радиосетями, обычно используемыми для соединения АСУ ТП-устройств, и пр.

Широкий спектр инструментов позволяет преступникам создать полный наступательный арсенал, а также облегчает работу низкоквалифицированным злоумышленникам. По словам экспертов, не обладающие техническими знаниями о работе промышленного оборудования киберпреступники могут осуществлять атаки на АСУ ТП нажатием нескольких кнопок.

Согласно FireEye, большинство проанализированных инструментов являлись модулями для трех самых известных на сегодняшний день платформ тестирования на проникновение — Metasploit, Core Impact и Immunity Canvas.

Кроме того, с 2017 года сообщество Metasploit также работает над созданием специфической среды тестирования на проникновение, которая в основном сосредоточена на типе сетей и уязвимостях, обнаруживаемых только в средах АСУ ТП. Некоторые из наиболее заметных платформ включают Autosploit, Industrial Exploitation Framework (ICSSPLOIT) и Industrial Security Exploitation Framework.

Как предупреждают эксперты, компании должны быть осведомлены о наличии подобных инструментов и их расширенных функциях и соответствующим образом адаптировать индикаторы риска для своей области угроз». ***(Эксперты предупредили о распространении инструментов для взлома АСУ ТП // SecurityLab.ru (https://www.securitylab.ru/news/506127.php). 24.03.2020).***

***

«Специалисты из компании Palo Alto Networks обнаружили новую версию ботнета Mirai, получившую название Mukashi, которая эксплуатирует недавно обнаруженную и исправленную критическую уязвимость (CVE-2020-9054) в сетевых хранилищах (NAS) Zyxel с целью перехватить контроль над целевым устройством и использовать его для осуществления DDoS-атак.

Операторы Mukashi с помощью брутфорс-атак подбирают различные комбинации стандартных учетных данных для авторизации в Zyxel NAS, а также в UTM-, ATP- и VPN- межсетевых экранах.

Проблема затрагивает устройства с версией прошивки 5.21 и ниже. Zyxel выпустила устраняющие уязвимость обновления для четырех моделей (NAS326, NAS520, NAS540 и NAS542), однако десять других моделей (NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 и NSA325v2) больше не поддерживаются производителем и поэтому не получат обновления. Уязвимость получила максимальные 10 баллов по шкале CVSS.

Проблема связана с некорректной обработкой исполняемым файлом weblogin.cgi входных параметров имени пользователя. Благодаря этому злоумышленник может проэксплуатировать уязвимость, включив в имя пользователя определенные символы, и внедрять команды с привилегиями web-сервера. Затем с помощью встроенной утилиты setuid он может запускать команды с привилегиями суперпользователя.

Как и другие варианты Mirai, Mukashi сканирует Сеть на предмет уязвимых IoT-устройств, таких как маршрутизаторы, сетевые хранилища, камеры наблюдения и цифровые видеорегистраторы, которые защищены только заводскими настройками или ненадежными паролями». ***(Новая версия ботнета Mirai нацелена на устройства Zyxel // SecurityLab.ru (https://www.securitylab.ru/news/506100.php). 23.03.2020).***

***

«Специалисты китайской компании Qihoo 360 сообщают, что по крайней мере три ботнета эксплуатировали ряд уязвимостей нулевого дня в DVR компании LILIN. Причем это длилось более полугода, пока производитель не выпустил исправления в прошлом месяце.

Устройства DVR (digital video recorder) используются для объединения видеопотоков из локальных систем видеонаблюдения или с IP-камер и записывают их на различные носители, в том числе жесткие диски, SSD, карты памяти. DVR распространены так же повсеместно, как и сами камеры наблюдения, которые они обслуживают. К сожалению, DVR часто работают с заводскими настройками и учетными данными по умолчанию, а также с устаревшими прошивками. В итоге такие девайсы нередко становятся жертвами ботнетов, их заражают и затем используют для DDoS-атак.

По данным Qihoo 360, DRV компании LILIN имели сразу три уязвимости нулевого дня:

уязвимость в процессе NTPUpdate позволяла злоумышленникам внедрять и выполнять системные команды;

при помощи жестко закодированных учетных данных (root/icatch99 и report/8Jg0SR8K50) можно было изменить файл конфигурации DVR, а затем выполнить команды на устройстве, когда конфигурация FTP- сервера периодически синхронизируется;

практически то же самое можно было проделать, используя службу NTP.

Первым ботнетом, начавшим эксплуатировать 0-day баги, стал ботнет Chalubo, который злоупотреблял уязвимостью NTPUpdate начиная с конца августа прошлого года. Затем, в январе текущего года, две оставшееся проблемы нулевого дня стали использовать операторы ботнета FBot, а потом подключились и операторы ботнета Moobot, также злоупотреблявшие вторым 0-day.

Эксперты не сообщают, что именно операторы ботнетов делали с захваченными DVR, но перечисленные ботнеты обычно используются для проведения DDoS-атак, а также в качестве прокси (для перенаправления трафика злоумышленников).

Исследователи пишут, что дважды обращались к представителям LILIN, сначала после атак FBot, а затем, когда к атакам подключился ботнет Moobot. В прошлом месяце инженеры LILIN наконец выпустили обновления прошивок. Эксперты отмечают, что в настоящее время в сети можно найти более 5000 DRV LILIN». ***(Мария Нефёдова. DDoS-ботнет эксплуатирует 0-day уязвимости в DVR компании LILIN // Xakep (https://xakep.ru/2020/03/23/lilin-0days/). 23.03.2020).***

***

«Эксперты Bitdefender обнаружили новый модуль для известного банковского трояна TrickBot, который позволяет злоумышленникам использовать взломанные системы для запуска брутфорс-атак на RDP против Windows-систем.

Модуль был замечен экспертами еще в конце января текущего года, он называется rdpScanDll. По мнению специалистов, модуль еще достаточно новый и пока находится в стадии разработки. Однако это не помешало rdpScanDll попытаться атаковать 6013 RDP-серверов, в основном принадлежащих предприятиям в телекоммуникационном, образовательном и финансовом секторах и расположенных в США и Гонконге.

После того как TrickBot проникает в систему, он создает папку, содержащую зашифрованные пейлоады и связанные с ними файлы конфигурации, включающие список управляющих серверов, с которыми модулю необходимо связаться для получения команд. Затем rdpScanDll делится своим файлом конфигурации с другим модулем с именем vncDll, используя для связи с управляющими серверами URL стандартного формата формата: https://C&C/tag/computerID/controlEndpoint. Интерес здесь представляет controlEndpoint, связанный со списком режимов атак (check, trybrute и brute) и списком IP-адресов и портов, которые нужно атаковать через RDP.

Так, режим check проверяет RDP-соединение цели из списка, режим trybrute пытается выполнить брутфорс на выбранной цели, используя заранее определенный список имен пользователей и паролей, извлекаемый из /rdp/names и /rdp/dict. Как только исходный список целевых IP-адресов из rdp/domains будет исчерпан, модуль получит другой набор свежих IP-адресов, используя rdp/over.

Эксперты пишут, что учитывая, что модуль использует заранее определенный список имен пользователей и паролей, так все это похоже на целевые атаки.

«Тот простой факт, что они [хакеры] используют список имен пользователей и паролей, а не простую атаку по словарю, означает, что они что-то знают или имеют какой-то опыт относительно паролей, которые ИТ-администраторы используют для управления этими сетями. Они не стали бы перебирать пароли по конкретному списку, если этот список не доказал свою ценность в прошлом», — пишут аналитики.

Также в отчете Bitdefender подробно описан механизм доставки обновлений TrickBot, благодаря которому удалось понять, что модули для бокового перемещения по сети (WormDll, TabDll, ShareDll) тоже получили немало обновлений и улучшений в последнее время. Также за последние полгода активно обновлялись модули для system and network разведки». ***(SystemInfo, NetworkDll) и сбора данных (ImportDll, Pwgrab, aDll). (Мария Нефёдова. TrickBot использует взломанные машины для брутфорс-атак на RDP // Xakep (https://xakep.ru/2020/03/20/rdpscandll/).20.03.2020).***

***

«Компания Eset предупреждает о выявлении новых методов обфускации, которые используются злоумышленниками для избежания обнаружения и анализа вредоносных программ. Новые способы обфускации (запутывания кода) были зафиксированы в ходе исследования модуля ботнета Stantinko, который был обнаружен в конце 2019 г.

Среди методик, которые киберпреступники использовали для защиты своих программ от обнаружения выделяются две – обфускация строк и обфускация потока управления. В частности, запутывание строк кода опирается на создание важных строк, которые присутствуют или строятся в памяти только тогда, когда их нужно использовать. Обфускация потока управления превращает их в сложную для чтения форму, поскольку порядок выполнения основных блоков непредсказуемый без широкого анализа.

Кроме уже упомянутых способов запутывания, авторы вредоносного ПО также применяли и другие техники: мертвый код, код, который ничего не выполняет, а также мертвые строки и ресурсы. Все эти техники предназначены для предотвращения выявления, благодаря чему файлы злоумышленников выглядят более легитимными.

Киберпреступники, стоящие за ботнетом Stantinko, постоянно совершенствуют свои инструменты и разрабатывают новые. Именно поэтому специалисты Eset рекомендуют использовать надежные антивирусные решения, в состав которых входит модуль защиты от ботнетов». ***(Специалисты Eset обнаружили новые методы маскировки вредоносов // Компьютерное Обозрение (https://ko.com.ua/specialisty_eset_obnaruzhili_novye_metody_maskirovki_vredonosov_132325). 20.03.2020).***

***

«Исходный код одной из самых передовых и прибыльных на сегодняшний день вымогательских программ Dharma выставлен на продажу на двух русскоязычных хакерских форумах.

На конференции RSA в нынешнем году представители ФБР назвали Dharma вторым после Ryuk наиболее доходным вымогательским ПО в мире. За период с ноября 2016-го по ноябрь 2019 года вымогатель принес своим операторам более $24 млн. Теперь исходный код Dharma можно купить всего за $2 тыс. на подпольных форумах.

По мнению некоторых специалистов в области кибербезопасности, исходный код Dharma, вероятно, был выставлен на продажу в результате случайной утечки. Эксперты ожидают всплеска атак с использованием вымогателя, поскольку теперь его может купить любой желающий. Они обеспокоены этим фактом, поскольку Dharma – очень сложное ПО, написанное профессионалом своего дела. Специалисты бьются над расшифровкой его схемы шифрования с 2017 года, но их попытки пока не увенчались успехом. Единственный случай, когда Dharma удалось «расшифровать», произошел в результате непреднамеренной утечки мастер-ключа, но отнюдь не из-за уязвимости в шифровании.

История Dharma началась летом 2016 года. В то время вредонос назывался CrySiS и предлагался по бизнес-модели «вымогательское ПО как услуга» (Ransomware-as-a-Service, RaaS). Через две недели после того, как в ноябре 2016 года произошла утечка мастер-ключа, операторы CrySiS RaaS перезапустили сервис, но уже под названием Dharma.

Вторая утечка мастер-ключа произошла в марте 2017 года, однако на этот раз операторы вредоноса решили не менять название. Весной 2019 года появилось новое вымогательское ПО Phobos, практически идентичное Dharma. Однако, в отличие от Dharma, новый вымогатель использовался не в массовых, а целевых атаках. (Исходный код одного из самых прибыльных вымогателей выставлен на продажу // SecurityLab.ru (https://www.securitylab.ru/news/506236.php). 30.03.2020).

В начале текущего года эксперты «Лаборатории Касперского» обнаружили масштабную атаку типа watering hole, нацеленную на жителей Гонконга, в ходе которой на смартфоны жертв устанавливался многофункциональный зловред для iOS под названием LightSpy. Такие атаки названы по аналогии с тактикой хищников, которые охотятся у водопоя, поджидая добычу — животных, пришедших напиться. То есть злоумышленники размещают малварь на каких-либо ресурсах, которые посещают намеченные ими жертвы.

LightSpy проникал на смартфоны жертв, когда те посещали одну из страниц, замаскированных под местные новостные ресурсы. Создавались такие фейки просто: к примеру, злоумышленники попросту копировали код настоящих ресурсов, получая готовые клоны новостных сайтов. Ссылки на эти сайты распространялись через популярные в Гонконге форумы.

Во время посещения этих ресурсов на смартфоны посетителей загружался целый набор эксплоитов, результатом работы которых являлась установка самого LightSpy. По сути, достаточно было просто зайти на вредоносную страницу, и устройство оказывалось заражено без какого-либо дополнительного взаимодействия с пользователем.

Исследователи рассказывают, что LightSpy представляет собой модульный бэкдор, с помощью которого злоумышленник может удаленно выполнять самые разные команды на зараженном устройстве. Например, может определять

местоположение смартфона, получить список контактов и историю звонков, посмотреть, к каким сетям Wi-Fi жертва подключалась, сканировать локальную сеть и отправлять на сервер данные обо всех выявленных IP-адресах. Кроме этого, пока эксперты наблюдали за происходящим, у бэкдора появились дополнительные модули для кражи информации из Keychain, данных из мессенджеров WeChat, QQ и Telegram, а также истории браузера из Safari и Chrome.

При этом сообщается, что операторы этой кампании, которых исследователи называют группой TwoSail Junk, использовали не уязвимости нулевого дня, а так называемые уязвимости первого дня, то есть недавно обнаруженные проблемы, патчи к которым выпущены недавно и вошли только в последние обновления системы. Таким образом в группе риска оказались владельцы смартфонов под управлением iOS 12.1 и 12.2 (проблема затрагивает модели от iPhone 6s до iPhone X).

Также во время анализа инфраструктуры, связанной с распространением имплантатов для iOS, эксперты обнаружили ссылку, указывающую на вредоносное ПО для Android. По данным аналитиков, в конце ноября 2019 года эта ссылка распространялась через Telegram-каналы winuxhk и brothersisterfacebookclub, а также через посты в Instagram с приманкой на китайском языке.

Стоит сказать, что собственный отчет об этой кампании подготовили и специалисты Trend Micro. Они назвали эту схему Operation Poisoned News и пишут, что атаки не были нацелены на каких-то конкретных пользователей, но атаковали посетителей сайтов в целом.

Эксперты Trend Micro сообщают, что в своей цепочке эксплоитов злоумышленники использовали недавно исправленную ошибка в Safari, которая не имеет идентификатора CVE, а для получения root-привилегий применяли кастомизированный эксплоит для уязвимости ядра, CVE-2019-8605, которую Apple устранила летом 2019 года.

Специалисты обеих компаний связывают деятельность TwoSail Junk с более крупной китайской хак-группой Spring Dragon, также известной под названиями Lotus Blossom и Billbug (Thrip). Эта группировка, в частности, ответственна за создание такой малвари, как Lotus Elise и Evora». ***(Мария Нефёдова. Пользователи iOS в Гонконге стали жертвами многофункциональной малвари LightSpy // Xakep (https://xakep.ru/2020/03/27/lightspy/). 27.03.2020).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Гражданин России, Евгений Никулин, обвиняемый в некоторых из крупнейших хакерских атак в новейшей истории, в понедельник предстанет перед судом США.

Никулин предположительно украл миллионы имен пользователей и паролей, взломав системы в LinkedIn, DropBox и Formspring в 2012 году. По версии

обвинения, хакер также пытался продать взломанную информацию на черных онлайн-рынках в даркнете, где покупатели, вероятно, надеялись, что смогут использовать ее для взлома учетных записей в разных сервисах.

Никулин, который не признает себя виновным, предстанет перед судом в понедельник в окружном суде США в Сан-Франциско.

По иронии судьбы хакер был пойман из-за того, что сам не следовал простым правилам кибербезопасности: прокуратура заявляет, что они поймали 33-летнего хакера отчасти потому, что он не следовал основным протоколам безопасности. Правоохранители говорят, что он использовал пароли повторно, по той же ленивой привычке, что и обычные пользователи. Повторные учетные данные добавили доказательств того, что Никулин контролировал аккаунты, связанные с каждым из взломов.

Пробная версия, которая продлится две недели, - это больше, чем приложение A, вот почему вы не должны повторно использовать свои пароли. Киберпреступников часто не доводят до приговора, потому что о таких преступлениях недостаточно сообщается, они требуют много ресурсов для расследования, а подозреваемые часто находятся за пределами страны пострадавших. Доказательства против Никулина показывают на что способны хакеры в современном мире технологий.

«Очень важно, чтобы были такие прецеденты», - говорит эксперт по политическим вопросам Мике Эоян. По ее словам, дело Никулина может вдохновить правоохранительные органы на выделение большего количества ресурсов для профилактики и пресечения киберпреступлений, поскольку это показывает, что результат «на самом деле возможен».

Как произошли взломы

Чтобы украсть данные более чем 100 миллионов имен пользователей и паролей LinkedIn, Никулин, предположительно, взломал персональный iMac инженера LinkedIn Николаса Берри, который иногда использовал компьютер для удаленной работы. Оттуда Никулин, по версии следствия, вытащил имя пользователя Берри для корпоративного VPN LinkedIn, что позволило хакеру получить доступ к базе данных имен пользователей и паролей с серверов сайта профессиональной сети. Ожидается, что Берри даст показания в суде.

Обвинители говорят, что Никулин использовал аналогичный подход с DropBox и Formspring. Заметив подозрительные попытки войти в учетные записи пользователей DropBox из Восточной Европы, судебные следователи обнаружили, что кто-то взломал учетную запись сотрудника DropBox. Хак взломал 68 миллионов учетных записей, подтвердили более поздние сообщения. Аккаунт, стоящий за атакой, по версии следствия контролировал Никулин.

Другое расследование показало, что Никулин украл 30 миллионов учетных записей Formspring, взломав учетную запись сотрудника Formspring Джона Сандерса. Сандерс также должен дать показания в суде.

Арест подозреваемых является проблемой

Несмотря на след цифровых доказательств, оставленный киберпреступлениями, лишь небольшая часть инцидентов приводит к аресту. С учетом всех типов киберпреступлений, в том числе нарушений данных,

вымогателей, мошенничества в Интернете и кражи персональных данных в сети, только три из каждых 1000 зарегистрированных преступлений приводят к аресту.

Опрос показывает, что люди чаще сталкиваются с киберпреступностью, чем сообщают. Эоян говорит, что вероятность арестов всех киберпреступников намного ниже 0,3%.

Даже когда следствие выявляет подозреваемого, получить арест может быть проблемой, особенно если подозреваемый живет в такой стране, как Россия, Северная Корея, Китай или Иран. Никулин был в отпуске в Чехии, когда Интерпол засек его местоположение, что и привело к аресту хакера в 2016-м. Россия боролась с его экстрадицией почти два года, но США выиграли в 2018-м.

Другие россияне недавно были экстрадированы в США, находясь за пределами России, что заставило российские власти жаловаться на то, что США «охотятся» за их гражданами. Российское посольство пока не комментирует ситуацию по судебному разбирательству дела Никулина.

Почему взлом Linkedin имеет значение

Суд над Никулиным связан с преступлениями, которые все еще имеют последствия сегодня. Трой Хант (Troy Hunt), который основал веб-сайт для отслеживания нарушений данных «I have been pwned», говорит, что он по-прежнему видит информацию LinkedIn от хакера в новых кэшах украденных данных.

Вот почему вы никогда не сможете вернуться к повторному использованию старого пароля, который был взломан. Хакеры берут украденные имена пользователей и пароли и продолжают пробовать их на разных сервисах, в атаках, называемых заполнением учетных данных.

В понедельник британская сеть супермаркетов Tesco заявила, что хакеры использовали учетные данные для доступа к аккаунтам некоторых клиентов и мошенническим путем выкупали ваучеры. В декабре Amazon заявила, что хакеры получали доступ к камерам Ring и преследовали пользователей, опробовав пароли, украденные при взломе других платформ. А в ноябре хакеры попытались продать учетные данные для аккаунтов с недавно запущенным потоковым сервисом Disney+, некоторые из которых могли быть связаны с предыдущими нарушениями данных. «Если вас взломали и вы будете повторно использовать свои пароли, - сказал Хант, - вы находитесь в группе повышенного риска». ***(Романов Роман. Российский хакер предстанет перед судом США за взлом LinkedIn, DropBox и Formspring // Internetua (http://internetua.com/rossiiskii-haker-predstanet-pered-sudom-ssha-za-vzlom-linkedin-dropbox-i-formspring). 06.03.2020).***

***

«Власти США заподозрили еще одного российского айтишника в заговоре с целью продажи краденых данных. Минюст США опубликовал материалы шестилетней давности о деле главы департамента сетевой безопасности одной из известных российских компаний России в сфере информационной безопасности Group-IB Никиты Кислицина. Обвинение связано с делом хакера Евгения Никулина, которого США обвиняют в краже около 117 млн аккаунтов и паролей…

Согласно обвинительному акту, поданному в Окружной суд Северного округа Калифорнии, в 2012 году Кислицин получил от некоего сообщника (в документе он обозначен как CO-CONSPIRATOR A) похищенные данные пользователей и пытался их продать. CO-CONSPIRATOR A взломал Formspring в июне 2012 года, похитил базу данных пользователей, в том числе зашифрованные пароли, и передал их Кислицину. Используя псевдонимы Dor Fyo и Udalit, Кислицин пытался их продать другим сообщникам за 5,5 тыс. евро.

Мужчина был принят на работу в Group-IB в январе 2013 года – почти через полгода после взлома Formspring, и работает там по сей день. Прокуратура не выдвигала против компании никаких обвинений.

Хотя в обвинении против Кислицина имя сообщника не раскрывается, его дело связано с делом Евгения Никулина, в 2012 году похитившего 117 млн логинов и паролей пользователей Formspring, LinkedIn и Dropbox. В деле Никулина имя Никиты Кислицина фигурирует. Слушание по его делу назначено на 9 марта.

Ни компания Group-IB, ни ее сотрудник Никита Кислицин не получали официальных повесток, уведомлений или приглашений на предстоящие судебное заседание в Сан-Франциско, заявили “Ъ” в Group-IB. Там подчеркнули, что расценивают такие действия как недопустимые и нарушающие права их сотрудника. В компании заявили, что обвинения в отношении господина Кислицина несостоятельны, в материалах дела не содержится никаких доказательств: исследовательская деятельность в отношении киберпреступности, которую вел Никита Кислицин, не носила криминального характера.

Никита Кислицин работает в Group-IB с 2013 года, а события, которых касается указанное разбирательство, происходили около восьми лет назад, когда он был независимым исследователем по кибербезопасности и не имел отношения к компании, говорят там.

«Более того, представители компании Group-IB и, в частности, Никита Кислицин в 2013 году по личной инициативе встречались с сотрудниками министерства юстиции США для информирования их об исследовательской работе, связанной с андеграундом, которую в 2012 году проводил Никита Кислицин,— отмечают в Group-IB. — После данного общения с представителями американских властей в адрес компании Group-IB, равно как и в адрес Никиты Кислицина не было официально направлено никаких дополнительных вопросов».

По словам представителя компании, сейчас она ведет консультации с международными юристами для правовой оценки ситуации и принятия решения о дальнейших действиях». ***(В США сотрудника Group-IB подозревают в продаже взломанных данных // РосКомСвобода (https://roskomsvoboda.org/56083/). 06.03.2020).***

***

«Европол при содействии местных правоохранительных органов осуществил серию арестов в нескольких европейских странах, ликвидировав преступные группировки, занимавшиеся SIM-свопингом (подменой SIM-карт).

В ходе операции под названием Quinientos Dusim сотрудники Европейского центра по борьбе с киберпреступностью Европола (EC3), Национальной полиции Испании и Гражданской гвардии Испании арестовали 12 подозреваемых в испанских городах Бенидорм, Гранада и Вальядолид. В рамках операции Smart Cash сотрудники правоохранительных органов Румынии и Австрии арестовали 14 предположительных участников еще одной киберпреступной группировки.

Участники первой группировки подозреваются в похищении €3 млн в результате серии кибератак. С помощью вредоносного ПО злоумышленники похищали учетные данные пользователей для online-банкинга, а затем подавали запрос операторам связи на восстановление SIM-карт жертв, предъявив поддельные удостоверения личности. Получив дубликат SIM-карт, злоумышленники перехватывали проверочные коды для двухфакторной аутентификации и переводили средства с чужих банковских счетов на подставные.

В случае с Румынией и Австрией киберпреступники использовали похожую схему. Злоумышленники точно так же похищали учетные данные и с помощью SIM-свопинга перехватывали коды безопасности. Однако обналичивание средств осуществлялось через безкарточные банкоматы.

Группировка «обчистила» более 100 жертв. В каждом случае злоумышленники похищали порядка €6-137 тыс. В общей сложности было похищено около полумиллиона евро». ***(Европол пресек деятельность хакеров, укравших миллионы евро с помощью SIM-свопинга // SecurityLab.ru (https://www.securitylab.ru/news/505892.php). 13.03.2020).***

***

Технічні аспекти кібербезпеки

Виявлені вразливості технічних засобів та програмного забезпечення

«Дослідники в області кібербезпеки розкрили неприємну вразливість в смартфонах, на яких встановлені голосові помічники. Зокрема, проблема торкнулася всіх моделей iPhone з Siri і Android-девайсів з Google Assistant. Про це повідомляє Tom's Guide.

Виявилося, що смартфони з «розумними» асистентами сприйнятливі до звуків і вібрацій, які ніяк не помітить жодна людина. Таким чином за допомогою ультразвуку смартфонам можна посилати різні команди по твердих поверхнях – дереву, металу, склу. Простий стіл стає зоною максимальної вразливості для гаджета.

Таким чином можна робити дзвінки, знімати і озвучувати текст з СМС, не торкаючись до чужого гаджету. На відео нижче автори SurfingAttack показують, як можна управляти Google Pixel. Для цього використовується спеціальний софт на комп'ютері, генератор звукових хвиль і поверхня для передачі сигналу.

З 17 перевірених смартфонів 15 виявилися підкоряються такій формі управління. Серед них були iPhone 5, 5s, 6 і X, перші три покоління Google Pixel, Xiaomi Mi 5, Mi 8 і Mi 8 Lite, Samsung Galaxy S7 і Galaxy S9, а також Honor View 8. Стійкість показали Samsung Galaxy Note10 + і Huawei Mate 9, судячи з усього, за рахунок викривленої поверхні корпусу.

Дослідники рекомендують використовувати товсті чохли або класти телефони на м'яку тканину, щоб ніхто не зміг дістатися до пристрою подібним чином. Іншим варіантом може бути тільки вимкнути голосові помічники». ***(Лужна Софія. Експерти розповіли новий спосіб зламати ваш смартфон. Вразливість є і на iOS і на Android // TechnoPortal.com.ua (https://technoportal.com.ua/smartfony/43735). 04.03.2020).***

***

«Словацька компанія ESET, що спеціалізується на кібербезпеці, виявила вразливість, яка була присутня більш ніж на одному мільярді пристроїв з підтримкою Wi-Fi.

Уразливість отримала назву Kr00k. Фахівці з'ясували, що джерелом проблеми стали мікросхеми Wi-Fi, вироблені Cypress Semiconductor і Broadcom. Відзначимо, що Cypress придбала у Broadcom бізнес Wi-Fi в 2016 році.

Як виявилося, при розриві підключення Wi-Fi або поганому сигналі і наступному відновленні з'єднання, ключі шифрування «обнуляються». Цим можуть скористатися зловмисники, в тому числі і спровокувати обрив зв'язку. Уразливість охоплює як протокол WPA2-Personal, так і WPA2-Enterprise.

Крім iPhone і смартфонів Android, під загрозою опинилися планшети, включаючи iPad, ноутбуки, включаючи MacBook, розумні колонки, включаючи Amazon Echo, розумні дисплеї, електронні книги Kindle, роутери та точки доступу Wi-Fi.

Фахівці ESET протестували і підтвердили, що вразливість є на Amazon (Echo, Kindle), Apple (iPhone, iPad, MacBook), Google (Nexus), Samsung (Galaxy), Raspberry (Pi 3), Xiaomi (Redmi), а також точках доступу Asus і Huawei.

За результатами тестування виявилося, що модулі Wi-Fi виробництва Qualcomm, Realtek, Ralink і Mediate не схильні до вразливості Kr00k.

Як зазначила ESET в своєму звіті, більшість виробників пристроїв вже випустили виправлення для закриття даної уразливості. Користувачам варто перевірити наявність свіжого ПО для пристроїв і встановити його». ***(Митник Михайло. Понад мільярд iPhone і смартфонів Android під загрозою // TechnoPortal.com.ua (https://technoportal.com.ua/smartfony/43364). 01.03.2020).***

***

«Киберпреступники попытались проэксплуатировать две 0Day-уязвимости в антивирусных решениях компании Trend Micro. Обе проблемы (CVE-2020-8467 и CVE-2020-8468) содержатся в защитных решениях Trend Micro Apex One и OfficeScan. Эксплуатация первой уязвимости позволяет авторизованному злоумышленнику удаленно выполнять произвольный код на уязвимых установках, а второй — манипулировать некоторыми клиентскими

компонентами агента. Первая уязвимость является критической и получила оценку в 9,1 балла по шкале CVSS, а вторая — 8,0 балла по шкале CVSS.

Как предполагают специалисты, уязвимости были проэксплуатированы либо для отключения продуктов безопасности, либо для повышения привилегий злоумышленников на компьютерах с установленными антивирусными продуктами Trend Micro.

Компания также предупредила о наличии трех других уязвимостей (CVE-2020-8470, CVE-2020-8598 и CVE-2020-8599), каждая из которых получила максимальную оценку в 10 баллов по шкале CVSSv3.

Уязвимости могут быть проэксплуатированы удаленно, не требуют аутентификации и обеспечивают полный контроль над антивирусной программой. Все три проблемы содержатся в сервере Trend Micro Apex One и OfficeScan. Первые две связаны с наличием уязвимой DLL-библиотеки, который позволяет злоумышленнику удалить любой файл на сервере и выполнить произвольный код с привилегиями уровня SYSTEM. Последняя уязвимость связана с наличием EXE-файла, позволяющего записать произвольные данные в произвольный путь в уязвимых установках и обойти авторизацию суперпользователя.

Японский производитель антивирусов уже выпустил патчи для вышеуказанных уязвимостей. Проблемы были исправлены в версиях Apex One CP 2117 и OfficeScan XG SP1 CP 5474 и XG CP 1988». ***(В антивирусных продуктах Trend Micro обнаружены две 0Day-уязвимости // SecurityLab.ru (https://www.securitylab.ru/news/505963.php). 18.03.2020).***

***

«Программный инженер из Amazon Web Services (AWS) Павел Вечоркевич (Pawel Wieczorkiewicz) обнаружил в процессорах Intel очередную уязвимость, позволяющую похищать данные из внутренней памяти ЦП. Разработанная Вечоркевичем атака получила название Snoop-assisted L1 Data Sampling или просто Snoop.

В ходе осуществления атаки Snoop используются такие механизмы процессора, как многоуровневый кэш, согласованность (когерентность) кэша и слежение за шиной.

В настоящее время большинство процессоров имеют многоуровневую память (кэш), где данные хранятся во время их обработки процессором. В зависимости от характеристик ЦП кэш может быть одноуровневым (L1), двухуровневым (L2) или даже трехуровневым (L3). Чаще всего используется уровень L1, который разделяется на два. Один раздел (L1D) используется для обработки данных пользователя, а второй (L1I) – для обработки кода инструкции самого ЦП.

Из-за многоядерной архитектуры и многоуровневого кэша обычно данные одновременно хранятся в нескольких кэшах процессора и даже в оперативной памяти. Согласованность кэша – это процесс, синхронизирующий все уровни кэша таким образом, чтобы в L1, L2 и оперативной памяти хранились одни и те же данные, что и в L1D – месте, где они начинают меняться.

Слежение за шиной представляет собой операцию, в ходе которой ЦП обновляет все уровни кэша, когда в L1D начинают меняться данные.

Как выяснил Вечоркевич, при определенных условиях вредоносный код может вмешаться в процесс слежения за шиной и вызвать ошибки, способные привести к утечке данных из процесса согласованности кэша, а именно – данные, в тот момент изменяемые в L1D. Однако, в отличие от Meltdown и Spectre, Snoop не позволяет похитить большие объемы данных. Кроме того, как уверяют в Intel, необходимые для осуществления атаки условия очень сложно обеспечить.

Инженер уведомил Intel о проблеме, однако, изучив уязвимость, специалисты компании пришли к выводу, что выпущенный в 2018 году патч для уязвимости Foreshadow (L1TF) исправляет и ее. Со списком уязвимых процессоров Intel можно ознакомиться здесь». ***(Обнаружена новая уязвимость, позволяющая похищать данные процессоров Intel // SecurityLab.ru (https://www.securitylab.ru/news/505926.php). 17.03.2020).***

***

«Количество уязвимостей в программном обеспечении с открытым исходным кодом выросло почти на 50% в 2019 году. Такой вывод привели эксперты из компании WhiteSource в своем ежегодном отчете об уязвимостях. Специалисты связывают данную ситуацию с широким распространением компонентов с открытым исходным кодом и общим развитием опенсорсного сообщества в последние годы, а также вниманием СМИ к раскрытию данных.

В 2019 году было выявлено свыше 6 тыс. уязвимостей в продуктах с открытым исходным кодом против чуть более 4 тыс. в 2018 году. При этом, информация о 85% уязвимостях раскрывалась уже после выпуска необходимого исправления.

Однако информированность сообщества об уязвимостях не всегда означает, что данные о них будут раскрыты. К примеру, только 84% известных уязвимостей в открытом ПО попадают в Национальную базу данных уязвимостей США (National Vulnerability Database, NVD).

Специалисты также проанализировали количество уязвимостей в зависимости от языка программирования. По словам экспертов, проекты, написанные на языке C, содержали наибольший процент уязвимостей (30%), далее следуют PHP (27%), Java (15%), JavaScript (10%), C# (9%), Python (5%) и Ruby (4%).

Наиболее распространенными в 2019 году классами уязвимостей оказались: CWE-79 (межсайтовое выполнение сценариев), CWE-20 (некорректная проверка входных данных), CWE-119 (выполнение операций за пределами буфера памяти), CWE-125 (чтение за пределами буфера) и CWE-200 (раскрытие информации).

«CWE-79 является одним из самых простых классов уязвимостей, которые могут быть проэксплуатированы злоумышленниками, поскольку существует множество автоматизированных инструментов, облегчающих процесс взлома даже преступникам-новичкам», — отметили специалисты.

Исследователи также отметили изменения, связанные с переходом рейтинга опасности уязвимости CVSS (Common Vulnerability Scoring System) на версию 3.1. По словам экспертов, в версии 3.1 изменилась классификация уровня опасности уязвимости. То есть более половины обнаруженных уязвимостей являются либо

критическими либо высокой степени опасности, тем самым затрудняя распределение приоритетов при выпуске исправлений». ***(За последний год число уязвимостей в открытом ПО выросло на 50% // SecurityLab.ru (https://www.securitylab.ru/news/505884.php). 13.03.2020).***

***

«Чешскому производителю решений безопасности Avast пришлось пойти на радикальный шаг и отключить в своих продуктах главный компонент из-за обнаруженной уязвимости, способной поставить под угрозу всех клиентов компании.

Опасная уязвимость была обнаружена в JavaScript-движке – компоненте антивирусных решений Avast, проверяющем, не является ли JavaScript-код вредоносным, перед его выполнением в браузере или почтовой программе.

По словам специалиста Google Тэвиса Орманди (Tavis Ormandy), несмотря на то, что движок обрабатывает недоверенные данные и имеет высокие привилегии, он не защищен песочницей. «Любая уязвимость в этом процессе является критической и может легко эксплуатироваться удаленными атакующими», - отметил исследователь.

Проэксплуатировать уязвимость очень легко. Достаточно лишь отправить жертве по электронной почте JavaScript- или WSH-файл или заставить ее открыть файл со встроенным вредоносным JavaScript-кодом. Когда антивирус Avast загрузит и запустит вредоносный JavaScript-код в своем движке, на компьютере жертвы может быть выполнена вредоносная операция с привилегиями системы. Таким образом, с помощью уязвимости злоумышленник может установить на атакуемом устройстве вредоносное ПО.

Компания Avast была уведомлена о проблеме 4 марта 2020 года, но все еще не исправила ее. 11 марта было принято решение временно отключить уязвимый компонент, пока не выйдет исправление. Дата релиза патча не уточняется». ***(Avast отключила главный компонент своих антивирусов из-за уязвимости // SecurityLab.ru (https://www.securitylab.ru/news/505814.php). 12.03.2020).***

***

«Специалисты из компании Bitdefender совместно с исследователями из нескольких университетов обнаружили и протестировали новый класс уязвимостей в процессорах Intel — LVI (Load Value Injection). Эксплуатация уязвимости позволяет злоумышленнику похитить конфиденциальную информацию (ключи шифрования или пароли) из защищенной памяти и затем перехватить контроль над системой.

Как сообщили эксперты, LVI (CVE-2020-0551) отличается от других уязвимостей в процессорах Intel, таких как Meltdown , Foreshadow , ZombieLoad , RIDL и Fallout и существующие исправления не защитят систему от атак. Вместо прямой утечки данных от жертвы к атакующему, эксплуатация уязвимости осуществляется в противоположном направлении — злоумышленник внедряет данные через скрытые буферы процессора в программу-жертву для взлома и получения конфиденциальной информации.

Когда жертва попытается выполнить определенный код, злоумышленник сможет заполнить буферы MDS определенными данными, чтобы влиять на действия жертвы.

«Перехват потока управления в ходе LVI-атаки позволяет злоумышленнику обманным путем заставить жертву выполнить определенную функцию. Теоретически это работает на всех уровнях безопасности: от процесса к процессу, от пользовательского режима до режима ядра, от гостевого режима до суперпользователя и, возможно, даже от пользовательского режима до анклава», — полагают эксперты.

Исследователи успешно проверили LVI-атаки на системах, получивших патчи для защиты от Meltdown. По результатам предварительных тестов, представленные Intel исправления микрокода процессоров для новой атаки приводят к серьезному снижению производительности — от 2 до 19 раз.

Обе группы исследователей также разработали PoC-коды, один из которых позволяет поставить под угрозу безопасность анклавов Intel SGX.

Хотя исследователи не тестировали процессоры AMD или ARM, предположительно, любой процессор, уязвимый к утечке данных типа Meltdown, также будет подвержен риску LVI-атак. Как отметили специалисты, атаки LVI будет трудно осуществить на практике, особенно в сравнении с другими атаками по сторонним каналам (MDS, L1TF, SWAPGS). В настоящее время LVI-атаки рассматриваются как теоретические и не представляют прямую угрозу для пользователей». ***(LVI — новый класс уязвимостей в процессорах Intel // SecurityLab.ru (https://www.securitylab.ru/news/505784.php). 11.03.2020).***

***

«В середине марта 2020 года стало известно, что из-за ошибки Tor Browser может выполнять код JavaScript на сайтах, даже если запуск JavaScript был сознательно заблокирован пользователем.

Как мы писали, возможность блокирования выполнения JavaScript является один из важных аспектов безопасности Tor Browser. Именно из-за того, что браузер сосредоточен на сохранении конфиденциальности пользователей (в частности, он маскирует реальные IP-адреса и делает все, чтобы сохранить анонимность человека) его часто используют для обхода блокировок и цензуры журналисты, политические активисты и диссиденты в странах с репрессивным режимом.

Ошибка крылась в настройках безопасности Tor Browser Bundle. Так, даже если браузер был настроен на использование самого высокого уровня безопасности (Safest), он по-прежнему разрешал выполнение кода JavaScript в некоторых ситуациях, даже когда должен его блокировать.

Тогда разработчики рекомендовали пользователям полностью отказаться от использования JavaScript и отключить его в настройках (about:config -> javascript.enabled -> false), так как обновление NoScript до версии 11.0.17 проблему, к сожалению, не решало.

Теперь инженеры Tor Project выпустили Tor Browser версии 9.0.7, в которой использование Javascript отключается для всего браузера, если уровень безопасности установлен на значение Safest. Разработчики объясняют, что при

желании пользователи могут отдельно включить использование JavaScript в настройках.

«Это может повлиять на ваш рабочий процесс, если ранее при включенном NoScript вы разрешали JavaScript на некоторых сайтах. Мы активируем эту меру предосторожности до тех пор, пока не убедимся, что последние версии NoScript успешно блокируют выполнение JavaScript по умолчанию», — пишут представители Tor Project». ***(Мария Нефёдова. В Tor Browser исправлен баг, позволявший деанонимизировать пользователей // Хакер (https://xakep.ru/2020/03/25/tor-js-patch/). 25.03.2020).***

***

«Эксперты из Йоркского университета рассказали о том, как им удалось обнаружить уязвимости в популярных менеджерах паролей. Баги позволяли малвари похищать учетные данные пользователей.

Оказалось, что еще в 2017 году исследователи проанализировали пять популярных менеджеров паролей: LastPass, Dashlane, Keeper, 1Password и RoboForm. Анализ помог обнаружить четыре ранее неизвестные уязвимости, в том числе одну, которая вела к раскрытию учетных данных. Так, наиболее серьезная из обнаруженных проблем позволяла вредоносному приложению выдать себя за легитимную программу и обманом заставить менеджер паролей раскрыть сохраненные учетные данные. Рассказывать о своих изысканиях раньше эксперты не рисковали, так как сочли это излишне опасным.

Главная проблема затрагивала Android-приложения 1Password и LastPass, которые были признаны уязвимыми для фишинговых атак, так как весьма странно определяли, какие сохраненные учетные данные предлагать для автозаполнения. Фактически, вредоносное приложение могло выдать себя за легитимное, просто используя идентичное имя.

Так, исследователи создали PoC-приложение, которое успешно атаковало LastPass (и могло проделать то же самое с 1Password). Это приложение имело экран входа в систему, разработанный таким образом, чтобы имитировать официальный экран входа Google, и, следовательно, его было трудно отличить от настоящего. В итоге LastPass предлагал для этого фейка автозаполнение учетными данными Google.

При этом эксперты отмечают, что атака имела ряд очевидных ограничений: вредоносное приложение должно быть установлено на устройстве жертвы, а сама жертва должна использовать уязвимые менеджеры паролей и автозаполнение, а также иметь учетные данные для целевого приложения, хранящиеся в зашифрованном хранилище.

Еще одна уязвимость, которую исследователи обнаружили во всех вышеперечисленных менеджерах паролей (за исключением 1Password), заключалась в том, что те не обеспечивали достаточную защиту учетных данных, скопированных в буфер обмена. В частности, в Windows 10 учетные данные могли быть вставлены из буфера обмена в виде обычного текста, даже если компьютер заблокирован. По мнению специалистов, для защиты от таких атак менеджеры

паролей должны иметь возможность автоматически очищать буфер обмена через определенное время.

Хотя некоторые парольные менеджеры позволяют пользователям защитить свое хранилище паролей с помощью четырехзначного PIN-кода, эксперты пишут, что приложения RoboForm и Dashlane не имели счетчика количества неверных попыток ввода этого самого кода. То есть злоумышленник мог последовательно ввести два PIN-кода, затем удалить приложение из списка недавно использованных и попробовать еще два PIN-кода. Даже если атакующий вводит PIN-коды вручную, он все равно сможет подобрать PIN-код в среднем за 2,5 часа.

«Мы не полностью автоматизировали эту атаку, но полагаем, что в случае автоматизированной атаки на подбор PIN уйдет значительно меньше времени», — пишут эксперты.

Исследователи связались с разработчиками протестированных парольных менеджеров еще в 2018 году. Сообщается, что пять вендоров ответили на их запросы и прислушались к предупреждениям, однако исправления были выпущены не для всех обнаруженных проблем, так как многие найденные уязвимости получили низкий приоритет». ***(Мария Нефёдова. Уязвимости позволяли воровать учетные данные из парольных менеджеров // Xakep (https://xakep.ru/2020/03/24/pass-managers/). 24.03.2020).***

***

«Исследователь, известный в сети под псевдонимом Nullze, обнаружил, что веб-интерфейс Tesla Model 3 подвержен уязвимости отказа в обслуживании (DoS). Баг получил идентификатор CVE-2020-10558, и с его помощью злоумышленник мог заставить основной тачскрин автомобиля перестать отвечать на запросы пользователя.

«Уязвимость позволяет злоумышленникам убрать спидометр, веб-браузер, климат-контроль, поворотники, навигацию, уведомления автопилота, а также другие функции с главного экрана», — объясняет специалист в своем блоге.

Чтобы воспользоваться уязвимостью, атакующий должен вынудить пользователя перейти на специально созданную вредоносную веб-страницу. Эта страница спровоцирует сбой интерфейса Chromium-браузера и, по сути, обрушит весь интерфейс Tesla Model 3. Водить автомобиль при этом по-прежнему можно, а вот чтобы вернуть дисплею работоспособность придется выключить и повторно включить автомобиль.

Исследователь уведомил компанию о проблеме через официальную bug bounty программу на Bugcrowd. Известно, что компания вознаградила Nullze за обнаружение бага, но сумма вознаграждения не раскрывается (обычно Tesla предлагает от 100 до 15 000 долларов за уязвимости). Уязвимость была устранена с релизом прошивки версии 2020.4.10, в феврале текущего года.

Владельцы Tesla, которые еще не установили обновление, могут изучить уязвимость, используя proof-of-concept эксплоит, опубликованный Nullze. Впрочем, можно удовольствоваться и видеодемонстрацией, которую выложил исследователь». ***(Мария Нефёдова. Тачскрин Tesla признали уязвимым для DoS-атак // Xakep (https://xakep.ru/2020/03/24/tesla-dos/). 24.03.2020).***

***

«Microsoft предупреждает, что в составе Adobe Type Manager Library (atmfd.dll) обнаружены сразу две 0-day уязвимости, которые уже эксплуатируют хакеры. Данная библиотека используется, в частности, для рендера шрифтов PostScript Type 1 в Windows.

По информации специалистов, обе уязвимости позволяют удаленно выполнить произвольный код, то есть злоумышленники могут запустить в системе жертвы свой код и предпринимать различные действия от лица пользователя. Атакующий может добиться эксплуатации уязвимости по-разному, например, может убедить пользователя открыть специально созданный документ или просмотреть его на панели Windows Preview.

Перед проблемами уязвимы все поддерживаемые в настоящее время версии Windows и Windows Server уязвимы (включая Windows 10, 8.1 и Server 2008, 2012, 2016 и 2019). Windows 7, чья поддержка была прекращена в начале текущего года, тоже подвержена уязвимостям.

О текущих атаках пока известно мало. В компании характеризируют их как «ограниченные» и «целевые», но не вдаются в подробности.

Так как патчей пока нет (вероятно, их релиза можно ждать только в составе апрельского вторника обновлений), инженеры Microsoft рекомендуют предпринять следующие шаги:

отключить Preview Pane и Details Pane (панели предварительного просмотра и сведений) в проводнике Windows;

отключить службу WebClient;

переименовать ATMFD.DLL.» ***(Мария Нефёдова. Всем версиям Windows угрожают две уязвимости нулевого дня // Xakep (https://xakep.ru/2020/03/24/windows-0days-2/). 24.03.2020).***

***

«Microsoft розповіла про критичні вразливості Windows, які можуть бути використані для злому ОС. Під загрозою злому виявилися всі останні версії операційної системи, повідомляє TechCrunch.

Знайдені уразливості пов’язані з обробкою і відображенням шрифтів бібліотекою Adobe Type Manager Windows. Помилка може бути використана хакерами, коли користувач відкриває текстові документи або запускає їх в режимі попереднього перегляду на своєму комп’ютері. Після запуску інфікованого документа зловмисник може отримати віддалений доступ до ОС і встановити шкідливі програми.

У заяві Microsoft йдеться, що компанія в курсі обмеженого числа цільових атак, пов’язаних з уразливостями. Відповідно до опису проблеми, якій присвоєно критичний рівень небезпеки, уразливості піддаються всі операційні системи, включаючи Windows 10. Компанія заявила, що працює над патчем безпеки.

Microsoft не уточнила, коли випустить оновлення, однак наступний регулярний апдейт запланований на 14 квітня. Як пише TechCrunch, одними з найменш захищених користувачів операційних систем від Microsoft є власники

копій Windows 7. Зокрема, користувачі стандартних версій ОС не отримають оновлення безпеки через старіння системи…». ***(Користувачі Windows опинились в небезпеці, особливо Windows 7 // TechnoPortal.com.ua (https://technoportal.com.ua/bez-kategori%d1%97/45660). 28.03.2020).***

***

«Эксперты Positive Technologies подсчитали, что всего за три недели (с конца февраля 2020 года) количество ресурсов, доступных через RDP, увеличилось на 9% и составило более 112 000. При этом свыше 10% таких ресурсов уязвимы перед проблемой BlueKeep (CVE-2019-0708), которая позволяет атакующему получить полный контроль над компьютером на базе Windows.

Для атаки достаточно отправить специальный RDP-запрос к уязвимым службам удаленного рабочего стола (RDS). Аутентификации при этом не требуется. В случае успеха злоумышленник сможет устанавливать и удалять программы в скомпрометированной системе, создавать учетные записи с максимальным уровнем доступа, читать и редактировать конфиденциальную информацию. Уязвимости подвержены операционные системы Windows 7, Windows Server 2008 и Windows Server 2008 R2.

По динамике роста числа открытых по RDP узлов на сегодняшний день лидирует Уральский федеральный округ: оно увеличилось на 21%, а общая доля узлов, уязвимых для BlueKeep, составляет 17%. Далее идут Сибирский (21% и 16% соответственно), Северо-Западный (19% и 13%), Северо-Кавказский (18% и 17%), Южный (11% и 14%), Приволжский (8% и 18%), Дальневосточный (5% и 14%) и Центральный федеральные округа (4% и 11%).

«На сетевом периметре российских компаний начало увеличиваться число ресурсов, атака на которые позволит злоумышленникам получить контроль над сервером и проникнуть в локальную сеть, — отметил директор экспертного центра безопасности Positive Technologies Алексей Новиков. — Мы связываем это, в первую очередь, с поспешным переводом части сотрудников на удаленную работу. Независимо от выбранного типа удаленного подключения разумно обеспечить удаленный доступ через специальный шлюз. Для RDP-подключений это Remote Desktop Gateway (RDG), для VPN — VPN Gateway. Удаленное подключение напрямую к рабочему месту использовать не рекомендуется».

В Positive Technologies предупреждают, что открытие доступа к отдельным подсетям сразу всем пользователям VPN существенно снижает защищенность организации и не только дает широкие возможности внешнему атакующему, но и повышает риск атаки со стороны инсайдера. Поэтому IT-специалистам необходимо сохранять сегментацию сетей и выделять необходимое число VPN-пулов.

Помимо этого, Positive Technologies рекомендует обратить внимание на критически опасную уязвимость (CVE-2019-19781) в ПО Citrix, которое используется в корпоративных сетях, в том числе для организации терминального доступа сотрудников к внутренним приложениям компании с любого устройства через интернет. В случае эксплуатации этой уязвимости злоумышленник получает прямой доступ в локальную сеть компании из интернета. Для проведения такой атаки не требуется доступ к каким-либо учетным записям, а значит, выполнить ее

может любой внешний нарушитель». ***(Мария Нефёдова. Злоумышленники могут получить доступ к каждому десятому открытому удаленному рабочему столу // Xakep (https://xakep.ru/2020/03/30/bluekeep-still-dangerous/). 30.03.2020).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

"Датагруп" активно развивает сервис защиты от DDoS-атак. В этом году компания усовершенствовала услугу и существенно повысила уровень защиты сетей от атак различного типа и мощности

Напомним, что в конце осени 2019 года компания "Датагруп" представила корпоративным клиентам новейшее комплексное решение в области кибербезопасности - DataProtect. С его помощью клиенты "Датагруп" из корпоративного и государственного секторов имеют возможность выбирать разноуровневые сервисы, в том числе защиту сети от DDoS-атак. Компания использует инфраструктуру, подключенную к глобальной системе мирового лидера в области предоставления решений по защите от DDoS - NETSCOUT Arbor. Эта сверхмощная система использует информацию об атаках, собранную из различных уголков планеты, включая почти 40 % мирового интернет-трафика.

"Осенью, во время презентации DataProtect, представители крупнейших компаний Украины говорили о возросшей мощности DDoS-атак на их бизнес. Хотя предыдущее решение "Датагруп" имело достаточный запас ресурсов для защиты клиентов, специалисты нашей компании зафиксировали этот клиентской запрос. И уже в начале нынешнего года мы вдвое увеличили уровень защиты, - говорит Михаил Шелемба, CEO "Датагруп". - Когда клиент покупает нашу услугу защиты от DDoS-атак, мы подключаем его интернет-канал к оборудованию, которое мониторит трафик. Также наши клиенты могут выбирать из предлагаемых специалистами "Датагруп" различных модулей: защищенный узел доступа к сети Интернет, SOC (Security Operations Center), защита электронной почты, веб-приложений и телефонии, сканирование на уязвимости, тестирование на проникновение и т. п.

Кроме инновационного программно-аппаратного обеспечения комплексных решений в сфере кибербезопасности, компания "Датагруп" располагает мощной командой специалистов и экспертов с многолетним опытом в этой области.

DataProtect от "Датагруп" является решением, которое не только эффективно защищает все компоненты IT-инфраструктуры и каналы передачи данных от известных и неизвестных угроз, но также интегрирует все системы ИБ в единую консоль для обеспечения мониторинга и аналитики. ***("Датагруп" увеличивает уровень защиты от DDoS-атак // DsNews (https://www.dsnews.ua/future/-datagrup-uvelichivaet-uroven-zashchity-ot-ddos-atak-13032020124500). 13.03.2020).***

***

«Приложение для двухэтапной аутентификации Google Authenticator защищает учетную запись от взлома: благодаря системе одноразовых паролей злоумышленник не может использовать данные чужого аккаунта. Однако недавно обнаружили новый вид вредоносного программного обеспечения, способного похищать коды безопасности, которые генерирует система защиты Google.

Что известно о новой уязвимости

Компания Threat Fabric, специализирующаяся на решениях в области кибербезопасности, обнаружила новый троян, позволяющий хакерам удаленно получать доступ к устройству жертвы.

Вредоносное программное обеспечение, получившее название Cerberus, дает доступ к дисплею гаджета и делает скриншоты одноразового пароля, сгенерированного приложением Google Authenticator.

Исследователи отметили, что большинство Android-приложений по умолчанию используют настройки FLAG_SECURE, которые запрещают создавать снимки экрана во время работы. Но, как оказалось, Google при создании фирменного софта такой возможности не предусмотрела.

В своем отчете эксперты указали, что Google уже исправляла подобную уязвимость в системе двухфакторной авторизации еще в 2014 году, но позже она опять себя проявила.

Уязвимой оказалась и другая популярная программа – Microsoft Authenticator.

Как злоумышленники получают коды

После заражения устройства, злоумышленники, используя полученные данные, могут использовать коды подтверждения для совершения различных операций от имени пользователя, включая денежные переводы.

Как себя защитить

До исправления ошибки специалисты порекомендовали владельцам Android-гаджетов использовать альтернативные способы аутентификации, включая аппаратные ключи». ***(Злоумышленники нашли способ обхода двухфакторной защиты // Телеканал новостей «24» (https://24tv.ua/techno/ru/zloumyshlenniki_nashli_sposob_obhoda_dvuhfaktornoj_zashhity_n1295056). 10.03.2020).***

***

«Платформа SecureX использует возможности всех решений Cisco по информационной безопасности для обеспечения осведомленности об угрозах, а также предоставляет аналитику и автоматизирует рабочие процессы, ускоряя обнаружение и отражение кибератак.

Cisco SecureX

Создает единое пространство для обзора функционирования средств кибербезопасности заказчика на базе простой, эргономичной облачной платформы, включая обнаружение неизвестных угроз и нарушений политик для принятия более обоснованных решений.

Повышает эффективность и точность действий благодаря автоматизации стандартных рабочих процессов кибербезопасности, включая выявление целей угроз и принятие ответных мер.

Предлагает новый функционал управляемого обнаружения угроз с привлечением аналитических ресурсов Cisco Talos.

Cisco представляет облачную платформу кибербезопасности Cisco SecureX, которая радикально упрощает работу со всеми продуктами компании в области информационной безопасности (ИБ) и решает проблему излишней сложности систем, ставшей одной из приоритетных для директоров по кибербезопасности.

Cisco SecureX предлагает пользователям возможность полнофункциональной работы со всем портфолио продуктов Cisco для обеспечения информационной безопасности (ИБ) и существующей инфраструктурой заказчика. Cisco SecureX формирует единую прозрачную среду, выявляет неизвестные угрозы и автоматизирует рабочие процессы, укрепляя кибербезопасность на уровне сети, оконечных точек, облака и приложений. Так как простота имеет существенное значение для защиты процессов цифровой трансформации, сервисы Cisco SecureX включаются в состав всех продуктов портфолио Cisco Security.

Распространение Интернета вещей и высокоскоростного беспроводного доступа существенно расширяют потенциальную площадь для атак. Защита такой комплексной среды усложняется из-за наличия разнообразных технологий, не взаимодействующих между собой. Опрос 2800 профессионалов в области кибербезопасности, проведенный в рамках исследования Cisco 2020 CISO Benchmark Study, показал, что 28% ИТ-директоров считают управление мультивендорной средой очень сложным (в прошлом году этот показатель был на 8% меньше).

Основные возможности Cisco SecureX

Осведомленность об угрозах с использованием всех составляющих портфолио кибербезопасности заказчика, решений Cisco и третьих фирм.

Облачное многопользовательское решение демонстрирует результаты уже через 15 минут работы.

Анализ событий и данных в корпоративном сегменте, включая более 150 млн оконечных точек, сетевой трафик коммутаторов и маршрутизаторов, в том числе зашифрованный, облака Google, AWS и Azure, а также частные центры обработки данных.

Выявление целей атак занимает всего несколько минут, для противодействия используются данные продуктов безопасности и обновления аналитической информации об угрозах.

Информация подразделения Cisco Talos о новейших угрозах поступает в центр управления кибербезопасностью заказчика.

«Отрасль захлестнули тысячи продуктов в области ИБ, однако вместо помощи организациям они создают неуправляемые среды с плохо взаимодействующими элементами обеспечения безопасности. Из-за этого в ИБ-системах предприятий возникают белые пятна, — комментирует Джи Риттенхауз (Gee Rittenhouse), старший вице-президент и генеральный менеджер подразделения информационной безопасности Cisco. — Теперь службам обеспечения

безопасности приходится противостоять не только злоумышленникам, но и сложности, которая стала еще одним риском. Cisco SecureX кардинально меняет взаимодействие заказчика с системами безопасности, устраняя сложность и предлагая унифицированную среду анализа, отражающую состояние сервисов и инцидентов кибербезопасности. Теперь службы ИБ могут эффективнее использовать ресурсы и содействовать развитию и цифровой трансформации бизнеса».

Глобальная доступность Cisco SecureX запланирована на июнь текущего года. Заказчики могут присоединиться к листу ожидания бета-версии программы или запросить демонстрационную информацию». ***(Cisco представила облачную платформу кибербезопасности SecureX // ChannelForIT (http://channel4it.com/publications/Cisco-predstavila-oblachnuyu-platformu-kiberbezopasnosti-SecureX-36937.html#). 05.03.2020).***

***

«В MaxPatrol SIEM загружен очередной [1] (пятнадцатый) пакет экспертизы с 55 правилами для выявления признаков работы распространенных инструментов киберпреступников. Правила детектирования нацелены на обнаружение многофункциональных инструментов — фреймворков, часто используемых злоумышленниками, в том числе в целевых атаках. Пакет экспертизы поможет пользователям MaxPatrol SIEM выявлять активные действия злоумышленников в сети до достижения ими целей атаки.

Злоумышленники используют фреймворки для выполнения задач на разных этапах атаки, от получения доступа в сеть до кражи данных и воздействия на инфраструктуру. Для этого фреймворки могут задействовать встроенные утилиты операционных систем или запускать собственные зловредные модули.

Правила в составе пакета экспертизы детектируют активность отдельных модулей распространенных инструментов. В частности, среди этих инструментов Cobalt Strike (используется злоумышленниками для скрытой коммуникации, проведения фишинговых атак и атак через веб-приложения, для закрепления на ресурсах и развития присутствия внутри сети; группировка Cobalt с его помощью атаковала банки), Koadic и Sliver (свободно распространяемое ПО с большим набором функций, от удаленного выполнения команд до повышения привилегий), SharpSploit (набор инструментов для постэксплуатации), SharpWMI (ПО, которое использует механизм Windows Management Instrumentation для удаленного выполнения команд через подписки на события WMI), Rubeus (инструмент для атак на инфраструктуру, использующую протокол Kerberos для аутентификации [2]).

«Наши исследования хакерских фреймворков показывают, что в одном инструменте могут сочетаться несколько подходов, которые усложняют детектирование его работы, — комментирует Антон Тюрин, руководитель отдела экспертных сервисов PT Expert Security Center . — Один из популярных методов атак — living off the land, когда злоумышленники для атаки используют легитимные инструменты, которые уже присутствуют в атакуемой системе. Второй метод, набирающий популярность, — bring your own land, когда атакующие

создают и доставляют на взломанный узел свои собственные инструменты. Мы учли эти методы при разработке правил детектирования, которые выявляют активность хакерских инструментов на разных этапах, в том числе в момент запуска их модулей или отправки команд».

[1] В MaxPatrol SIEM доступны 15 пакетов экспертизы, которые содержат 300 правил обнаружения атак. Поставка пакетов экспертизы в MaxPatrol SIEM — это регулярная автоматизированная передача знаний в области обнаружения инцидентов ИБ в виде алгоритмов, позволяющих выявлять даже сложные нетиповые атаки. Соответствующие наборы правил и рекомендаций формируют эксперты Positive Technologies (R&D и PT Expert Security Center), которые непрерывно анализируют актуальные угрозы, исследуют полный цикл атак и разрабатывают способы их обнаружения. Эти наборы объединяются в пакеты и передаются в базу знаний Positive Technologies Knowledge Base, которая входит в состав MaxPatrol SIEM. Далее пользователь может в интерфейсе PT KB выбрать интересующие его пакеты и применить их в рамках своей инсталляции продукта.

[2] Используется по умолчанию во многих современных корпоративных сетях». ***(MaxPatrol SIEM обнаруживает работу популярных хакерских инструментов // SecurityLab.ru (https://www.securitylab.ru/news/505998.php). 19.03.2020).***

***

«Международная некоммерческая организация OWASP представила версию 1.0 платформы моделирования киберугроз Threat Dragon. Инструмент является кросс-платформенным и доступен в форме web-приложения и в виде десктопной версии.

Функционал Threat Dragon включает возможность создания диаграмм потоков данных; автоматического определения и ранжирования угроз; возможные методы защиты от угроз; указания мер по предотвращению атак и противодействию им.

Десктопная версия платформы доступна на GitHub.

OWASP (Open Web Application Security Project) - международная некоммерческая организация, сосредоточенная на анализе и улучшении безопасности программного обеспечения. Сообщество OWASP включает в себя корпорации, образовательные организации и частных лиц со всего мира. Сообщество работает над созданием статей, учебных пособий, документации, инструментов и технологий, находящихся в свободном доступе.

Моделирование угроз - процесс обнаружения угроз и уязвимостей на ранних стадиях разработки приложений». ***(Представлена платформа моделирования киберугроз OWASP Threat Dragon // SecurityLab.ru (https://www.securitylab.ru/news/505644.php). 08.03.2020).***

***

«Проект abuse.ch запустил новый сервис, позволяющий исследователям безопасности обмениваться образцами вредоносного ПО и дополнительными сведениями о них. Сервис MalwareBazaar разрешает публиковать только

проверенные образцы известных вредоносов, рекламное и потенциально нежелательное ПО к публикации не допускаются.

Ограничений по количеству загружаемых образцов нет. Исследователи могут добавлять в репозиторий столько образцов, сколько пожелают, находить нужные им образцы по семействам вредоносного ПО, фаззи-хэшу и тегам, а также запрашивать информацию о них по электронной почте. Сервис предоставляет API для автоматизации, поддерживает экспорт хэшей и ежедневно предоставляет набор образцов вредоносного ПО для скачивания.

По словам создателей MalwareBazaar, в настоящее время исследователи используют разведку из открытых источников (OSINT), однако она не всегда позволяет загружать образцы вредоносных программ, на которые есть ссылки, для проведения собственного анализа. Для того чтобы заполучить заветный образец для анализа, исследователям приходится регистрировать несчетное количество различных антивирусных online-сканеров, песочниц или баз данных. Более того, многие платформы ограничивают количество загрузок в сутки, а некоторые и вовсе являются исключительно платными.

MalwareBazaar упрощает жизнь исследователям, позволяя им загружать неограниченное количество образцов. Сервис является бесплатным как для коммерческого, так и для некоммерческого использования.

В отличие от VirusTotal, MalwareBazaar не использует антивирусный сканер, а позволяет исследователям бесплатно скачивать образы вредоносного ПО, загруженные их коллегами (VirusTotal позволяет скачивать загруженные файлы только платным пользователям).

OSINT – разведывательная дисциплина, включающая в себя поиск, выбор и сбор разведывательной информации из общедоступных источников, а также ее анализ. В разведывательном сообществе термин «открытый источник разведывательных данных» означает общедоступный источник, который в то же время не является «просто источником информации», означающим любую находящуюся в пространстве СМИ информацию». ***(В Сети появился новый бесплатный репозиторий вредоносного ПО // SecurityLab.ru (https://www.securitylab.ru/news/506144.php). 25.03.2020).***

***

«Компания Google анонсировала ужесточение защиты от вредоносного ПО для всех обладателей её эккаунта. Она кардинально расширяет масштабы действия программы Advanced Protection Program (APP), которая до сих пор предоставляла дополнительную защиту главным образом пользователям, входящих в группу повышенного риска вторжения – знаменитостям, журналиста, политическим деятелям, активистам и руководителям бизнеса.

Система Play Protect компании Google ежедневно сканирует более 100 миллиардов приложений, включая все программы, установленные на пользовательских устройствах, в поисках возможного вредоносного кода и прочих факторов риска. С момента её запуска в 2017 году, Play Protect предлагалась как опция, но теперь Google требует, чтобы данная служба была активирована по умолчанию, и будет блокировать возможность её отключения.

Пользователям будет запрещено загружать приложения из источников за пределами Play Store. Обращения приложений к Gmail или Google Drive будут блокироваться. Доступ к службам Google, таким как Gmail и Photos, станет возможен только через браузеры Chrome и Firefox.

В порядке исключения допускается пользование предустановленным ПО и загрузка дополнительных приложений через предустановленные на телефоне сторонние платформы. Кроме того, опытные пользователи по-прежнему смогут устанавливать сторонние приложения через Android Debug Bridge.

Новые ограничения не распространяются на популярные программы, такие как Mail, Calendar и Contacts.

AAP бесплатна для каждого обладателя учётной записи Google. На их устройствах должны быть установлены Android 7+ или iOS 10+ с бесплатным приложением Google Smart Lock. Для других конфигураций пользователи могут приобрести аппаратный ключ Titan Security Key по цене от $25 до $40.

С этой продвинутой защитой «даже если вы станете жертвой фишинговой атаки, которая раскроет ваши логин и пароль, неавторизованный пользователь не сможет получить доступ к вашей учетной записи без одного из ваших ключей безопасности». ***(Google укрепляет безопасность всех пользователей своих сервисов // Компьютерное Обозрение (https://ko.com.ua/google_ukreplyaet_bezopasnost_vseh_polzovatelej_svoih_servisov_132341). 23.03.2020).***

***

«Платформа кибербезопасности Fidelis Elevate победила в номинации “Лучшее обнаружение угрозы” по версии журнала SC Magazine на церемонии вручения 2020 Trust Awards.

Спросите любого пилота – и он скажет, что плохая видимость может испортить лучшие планы полета. То же самое относится и к стратегиям кибербезопасности, где видимость поверхности атаки имеет решающее значение для обнаружения угроз и реагирования на них.

Fidelis Elevate стремится обеспечить такую видимость по всей “Killchain”, используя несколько методов обнаружения. Платформа объединяет анализ сетевого и “облачного” трафика (NTA), обнаружение угроз на конечных точках и реагирование на них (EDR), а также технологии обмана злоумышленников (DDP) с открытыми каналами сбора информации об угрозах, песочницей и усовершенствованным анализом вредоносных программ в качестве средства автоматизации обнаружения угроз, их расследования и реагирования на них.

Fidelis Elevate использует богатые контентом и контекстом метаданные о трафике (более 300 параметров описания трафика) – и хранит их до 360 дней для автоматического ретроспективного анализа, и 90 дней хранит метаданные о процессах и событиях на конечных точках. Многие этапы процесса обнаружения, расследования и реагирования на угрозы автоматизированы, что сокращает время реагирования и минимизирует воздействие на бизнес.

Платформа автоматически проверяет события на всех уровнях, консолидируя похожие оповещения, что обеспечивает занятым аналитикам упорядоченный

рабочий процесс и фокусирует их на наиболее важных обнаружениях. Полная интеграция между продуктами на платформе Fidelis создает мультифункционал, такой как автоматический обмен информацией между компонентами, защита конечных точек, инвентаризация программного обеспечения и управление уязвимостями на конечных точках, используя его совместно с решениями анализа сетевого трафика и решениями для обмана злоумышленников. Открытая информационная лента об угрозах, поддерживающая сетевые решения и решения для конечных точек, включает в себя внутреннюю информацию об угрозах,а также настраиваемые индикаторы компрометации и правила, которые разрабатываются пользователями.

Fidelis предлагает более низкую совокупную стоимость владения по сравнению с другими рыночными предложениями благодаря интеграции EDR, анализа сетевого трафика и технологии обмана злоумышленников». ***(Fidelis Elevate - лучшее решение для обнаружения угроз по версии журнала SC Magazine // AMC Ukraine (http://channel4it.com/publications/Fidelis-Elevate-luchshee-resheniedlya-obnaruzheniya-ugroz-po-versii-zhurnala-SC-Magazine-37124.html#). 26.03.2020).***

***

«Компания Mozilla планирует ввести защиту для сохраненных паролей пользователей с помощью мастер-пароля в выпуске браузера Firefox 76. Данная функция уже реализована в сборке Nightly, но большинство пользователей смогут использовать ее с 5 мая нынешнего года.

В настоящее время если пользователь оставит свой компьютер незащищенным, любой человек с доступом к устройству может перейти к меню «Логин и пароли», а затем начать просматривать учетные записи и пароли. При желании можно установить мастер-пароль для повышения безопасности, но многие пользователи не делают этого. А те, кто не обладает достаточными техническими знаниями, даже не подозревают, что могут установить мастер-пароль.

Новая функция будет доступна в версиях браузера для Windows и MacOS. Если пользователь не установил мастер-пароль в Firefox, ему будет предложено ввести пароль операционной системы. Биометрическую аутентификацию, например, с помощью отпечатка пальца, также можно использовать. Пользователи Linux пока не имеют доступа к данной функции и неясно, будет ли она когда-либо реализована на платформе.

После ввода пароля операционной системы пользователь сможет получить доступ к сохраненной информации для авторизации в течение пяти минут, прежде чем система попросит пройти повторную аутентификацию». ***(Новая функция в Firefox 76 будет защищать все сохраненные пароли // SecurityLab.ru (https://www.securitylab.ru/news/506210.php). 27.03.2020).***

***

Грановський М.В. Державна політика у сфері запобігання та протидії кібернетичним загрозам – досвід Республіки Польща / Грановський Микола Володимирович // Теорія та практика державного управління. - 2019. - Вип. 4. - С. 212-220.

Проаналізовано дії, спрямовані на запобігання та протидію кібернетичним загрозам на прикладі Республіки Польща

Шифр зберігання НБУВ: Ж72481

***

Котух Є.В. Особливості національної та регіональної політики у сфері кібербезпеки / Котух Євген Володимирович // Теорія та практика державного управління. - 2019. - Вип. 4. - С. 40-47.

Розглянуто організаційний механізм та способи боротьби з кіберзагрозами. Проаналізовано досвід зарубіжних країн щодо залучення суб'єктів публічно-управлінських відносин до кібербезпеки через різні закони та регламенти дій. Визначено переваги та недоліки електронного уряду та його потенціал у протидії кіберзлочинам.

Шифр зберігання НБУВ: Ж72481

***

Матеріали Міжнародної науково-практичної конференції «Актуальні питання розвитку державності та правової системи в сучасній Україні» (25-26 жовтня 2019 року). - Запоріжжя, 2019. - 119 с.

Зі змісту:

- Веселова Л.Ю. Щодо адміністративно-правового статусу суб'єктів адміністративно-правових відносин у кіберсфері.

Шифр зберігання НБУВ: ВА840485

***

Прогностичне моделювання комп'ютерних вірусних епідемій : монографія / Шевченко В.Л., Нестеренко О.В., Нетесін І.Є., Шевченко А.В. - Київ : УкрНЦ РІТ, 2019. - 152 с.

Досліджено методи створення прогноз-моделей розвитку комп'ютерних вірусних епідемій. Проаналізовано основні види інцидентів інформаційної безпеки. Надано основні класифікації щодо комп'ютерних атак та способів захисту. Встановлено зв'язок між параметрами математичних моделей та прикладними заходами протидії зараженню інформаційних систем.

Шифр зберігання НБУВ: ВА840108

***