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

КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

№ 5 (травень)

Київ – 2018

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. 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

«Український стартап для аудиту кібербезпеки GuardYoo визнали перспективним на виставці в Ірландії

Компанія GuardYoo створена українськими підприємцями Романом Сологубом і Олегом Дерев'янко та займається розробкою інноваційних продуктів у сфері кібербезпеки. У грудні 2017 року компанія була відібрана до першого туру спеціалізованого конкурсу International Security Accelerator у м. Корк (Ірландія) …

GuardYoo посіла друге місце в номінації "most investable company" акселератора, а також отримала престижний приз "most investable team" від Sophia Business Angels Network. Тепер компанія візьме участь 15-16 травня в Entrepreneur Experience – престижному заході, який знайомить 24 найбільш перспективних нових підприємців з 24 видатними підприємцями Ірландії для 24-годинний спільної роботи над ідеями та проектами…» ***(Віталій Царьов. Український стартап для аудиту кібербезпеки отримав престижну нагороду // Національний промисловий портал (http://uprom.info/news/it/ukrayinskiy-startap-dlya-auditu-kiberbezpeki-otrimav-prestizhnu-nagorodu/). 08.05.2018).***

***

«…Конкурс «Пишем об информационной безопасности», стартовавший 1 апреля 2018 года, на данный момент собрал более 350 статей, написанных на украинском языке. Цель проекта, реализуемого компанией Cisco и общественной организацией «Викимедиа Украина», — восполнить пробелы украинских страниц Википедии в темах, касающихся ИБ-технологий…

Тематика поданных на конкурс статей охватывает разные аспекты кибербезопасности, такие как стандарты ИБ, программирование и хакерство, известные личности в сфере информационной безопасности, технологии и решения Cisco и др…» ***(Википедия активно наполняется статьями о кибербезопасности на украинском языке // ChannelForIT (http://channel4it.com/publications/Vikipediya-aktivno-napolnyaetsya-statyami-o-kiberbezopasnosti-na-ukrainskom-yazyke-30332.html#). 03.05.2018).***

***

«Пользователи уанета обнаружили на просторах Telegram бота, который позволяет узнать личность человека по номеру его телефона. В описании бота сообщается, что в базе — более 30 млн украинских номеров. Источниками данных бота указаны Work.ua, Rabota.ua, а также данные из приложений на Android… Кто разработал бота — выяснить не удалось. Его владельцем указан аккаунт @bot_creaters…» ***(В уанете обнаружили Telegram-бота, выдающего ФИО человека по номеру телефона // УНИАН (https://www.unian.net/science/10107842-v-uanete-obnaruzhili-telegram-bota-vydayushchego-fio-cheloveka-po-nomeru-telefona.html). 07.05.2018).***

***

«Группа компаний «МУК» и компания ESET, разработчик антивирусного программного обеспечения и решений в области компьютерной безопасности, объявили о подписании дистрибуторского контракта на территории Украины.

Соглашение предусматривает возможность поставки программных продуктов ESET в электронном виде. Портфель компании включает в себя программное обеспечение для защиты корпоративных и домашних пользователей. Флагманскими продуктами являются ESET Smart Security Premium для всесторонней защиты, ESET Internet Security для комплексной интернет защиты и ESET NOD32 Antivirus для базовой защиты ПК от вредоносного программного обеспечения…

Кроме того, информационный облачный сервис Threat Intelligence предоставляет сведения о целевых атаках, новых вредоносных программах, активностях ботнетов и позволяющий компаниям своевременно реагировать на инциденты кибербезопасности. Служба не требует развертывания в сетевой инфраструктуре и предоставляет экспертные отчеты об актуальных угрозах безопасности.» ***(«МУК» стала дистрибьютором решений ESET // «Компьютерное Обозрение» (http://ko.com.ua/muk_stala_distribyutorom_korporativnyh_i_domashnih_reshenij_eset_124557). 10.05.2018).***

***

«Вкладывая в различные технические средства обеспечения безопасности, украинские и международные компании часто становятся жертвами инсайдеров - опасаясь взломов, DDoS-атак и других «прелестей» цифрового мира, бизнес забывает о человеческом факторе…

Компания ESET выяснила, что почти треть (27%) сотрудников хотя бы раз за карьеру мстили бывшим работодателям – украли рабочие материалы или данные, уничтожили ценные документы либо обнародовали конфиденциальные сведения. Около 20% респондентов ESET хотя бы раз в жизни копировали рабочие материалы, базы клиентов, отчеты, планы и другие документы, чтобы впоследствии использовать их на новой работе или перепродать…» ***(Владимир Кондрашов. Инсайдер как скрытая киберугроза // Internetua (http://internetua.com/insaider-kak-skrytaya-kiberugroza). 16.05.2018).***

***

«У Вінницькому національному технічному університеті наступного навчального року з'явиться нова спеціалізація «Технології кібербезпеки в електроенергетиці». …напрямок запроваджено, враховуючи виклики часу та надзвичайно великий запит на спеціалістів у сфері енергетичної кібербезпеки. …у Вінниці навчатимуть цій спеціалізації першими в Україні…» ***(Вінницький «політех» береться за навчання спеціалістів з кібербезпеки // "iVin" (http://i-vin.info/news/vinnytskyy-politekh-beretsya-za-navchannya-spetsialistiv-z-kiberbezpeky-25275). 24.05.2018).***

***

«22 мая 2018 г. в рамках визита в ФРГ министр инфраструктуры Украины Владимир Омелян провел встречу с представителями компании Nokia…

Во время встречи была достигнута договоренность по изучению перспектив сотрудничества между Министерством инфраструктуры Украины и компанией Nokia о введении цифровой инфраструктуры в Украине…

По словам министра, в процессе развития цифровой инфраструктуры наибольшее внимание будет уделяться обеспечению высокого уровня кибербезопасности.» ***(МИУ работает над внедрением современных IT-технологий в сфере транспорта - В.Омелян // Транспортный бизнес (http://tbu.com.ua/news/miu_rabotaet_nad_vnedreniem_sovremennyh_it_tehnologii_v_sfere_transporta___v_omelian_.html). 23.05.2018).***

***

Національна система кібербезпеки

«Администрация Госспецсвязи уполномочена обеспечивать формирование и реализацию государственной политики в сферах защиты в киберпространстве государственных информационных ресурсов и информации, требование относительно защиты которой установлено законом, киберзащиты критической информационной инфраструктуры, осуществления госконтроля в таких сферах.

Изменения внесены в Положение об Администрации Государственной службы специальной связи и защиты информации, …постановлением Кабмина от 4 апреля 2018 года № 243, которое вступило в силу 9 мая 2018 года.

Так, установлено, что Администрация Госспецсвязи:

- координирует деятельность субъектов обеспечения кибербезопасности относительно киберзащиты;
- осуществляет меры по созданию и обеспечению функционирования Национальной телекоммуникационной сети;
- обеспечивает внедрение организационно-технической модели киберзащиты;
- обеспечивает внедрение системы аудита информационной безопасности на объектах критической инфраструктуры, устанавливает требования к аудиторам информационной безопасности, их аттестации (переаттестации);
- координирует, организует и проводит аудит защищенности коммуникационных и технологических систем объектов критической инфраструктуры на уязвимость;
- обеспечивает функционирование Государственного центра киберзащиты, правительственной команды реагирования на компьютерные чрезвычайные события CERT-UA…». ***(Администрация Госспецсвязи будет осуществлять госконтроль в сфере киберзащиты // Інформаційне агентство "ЛІГА:ЗАКОН (http://jurliga.ligazakon.ua/news/2018/5/10/170022.htm). 10.05.2018).***

***

«С сентября прошлого года Министерство обороны Украины ведет собственный канал в Telegram. За этот период каналу МОУ не удалось завоевать популярность у пользователей – на момент написания публикации у него всего 269 подписчиков. Однако последние события вокруг Telegram в России привлекли внимание к нему украинского экспертного сообщества…

Первым на присутствие Минобороны в мессенджере Telegram обратили внимание разработчики компании «ИТ-Лаборатория», специализирующейся на защите и анализе информации, Александр Галущенко…

– Кто-то ведёт этот канал. Он включается с рабочего места в МО. Серый/белый адрес, гейт, трассировка, агр-а, список подписчиков, номера, их точки входа, геолокация и т.д. Это саботаж, другого названия нет. Кто-то мозг включает, думает о последствиях? – прокомментировал Александр Галущенко...

– То, что Telegram использует собственный протокол, надежность которого неочевидна, уже создаёт проблемы. Криптография — не место для фантазий: малейшая ошибка может ослабить шифрование и надежность криптопротокола на порядок, – прокомментировал …спикер Украинского киберальянса, известный под ником Шон Таунсенд. – Кроме того, Telegram позволяет сопоставлять прозвища и телефоны пользователей. Я бы рекомендовал не пользоваться Telegram.

О том, что Telegram не является защищенным мессенджером, говорит и консультант по кибербезопасности Егор Папышев…

Для МОУ, считает консультант по кибербезопасности, использование Telegram может грозить компрометацией передаваемой информации и «всего, к чему имеет доступ приложение в телефоне»…

На днях недоверие к «оппозиционности» Павла Дурова и неподконтрольности мессенджера ФСБ высказали эксперты международного разведывательного сообщества InformNapalm, указав, помимо прочего, на «непрозрачных» инвесторов, от которых Telegram привлек 1,7 млрд долларов инвестиций» ***(Министерства обороны не должно быть в Telegram – эксперты // Goodnews.ua (http://goodnews.ua/technologies/ministerstva-oborony-ne-dolzhno-byt-v-telegram-eksperty/). 04.05.2018).***

***

«Секретар Ради національної безпеки і оборони України Олександр Турчинов заявив, що… ефективна система протидії кібератакам, кіберзлочинності, кібертероризму, активний розвиток державного контуру кіберзахисту та його масштабування на всю критичну інфраструктуру країни, розбудова кіберщита від гібридних агресій - одні із ключових питань для національної консолідації та міжнародної взаємодії…» ***(Анастасія Ткачук. У РНБО виступили за розбудову кіберщита України // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1732037-u-rnbo-vistupili-za-rozbudovu-kiberschita-ukrayini). 22.05.2018).***

***

«Сьогодні у силу вступив закон України "Про основні засади забезпечення кібербезпеки України"…

Закон створює засади національної системи кібербезпеки як сукупності політичних, соціальних, економічних та інформаційних відносин разом із організаційно-адміністративними та техніко-технологічними заходами державного і приватного секторів та громадянського суспільства.

Також законом визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, повноваження й обов'язки державних органів, підприємств, установ, організацій, осіб та громадян, основних засад координації їх діяльності, а також базових термінів у сфері кібербезпеки.

Документ визначає основні об'єкти кіберзахисту, які в сукупності складають критичну інфраструктуру країни, принципи забезпечення кібербезпеки та національна система кібербезпеки. Згідно з законом, президент України координує діяльність у сфері кібербезпеки через очолювану ним Раду нацбезпеки й оборони України…» ***(Анастасія Ткачук. Вступив в силу закон про кібербезпеку // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1729706-vstupiv-v-silu-zakon-pro-kiberzebpeku). 09.05.2018).***

***

«У парламенті зареєстровано проект закону № 8346 про внесення зміни до статті 5 Закону України "Про Державну службу спеціального зв'язку та захисту інформації України", яким пропонується збільшити загальну чисельність Держспецзв'язку в окремих випадках…

Як повідомляється у пояснювальній записці, метою проекту закону є законодавче врегулювання питання загальної чисельності Держспецзв'язку з урахуванням мобілізаційного розгортання територіальних органів Адміністрації Держспецзв'язку і територіальних підрозділів Держспецзв'язку при формуванні необхідної організаційної структури підрозділів за штатами воєнного часу та їх поповненні людськими мобілізаційними ресурсами…» ***(Дмитро Кропивницький. Чисельність складу Держспецзв'язку пропонують збільшити у разі мобілізації // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1730781-chiselnist-skladu-derzhspetszvyazku-proponuyut-zbilshiti-u-razi-mobilizatsiyi). 15.05.2018).***

***

«Хактивисты объединения Украинский киберальянс сегодня, 10 мая, взломали около двух сотен так называемых новостных ресурсов Российской Федерации и террористических организаций «ДНР» и «ЛНР».

Соответствующую информацию на своей странице в Facebook разместил спикер Украинского киберальянса, известный под ником Шон Таунсенд…

Среди взломанных, кроме «Мой Донецк» и «Инфорос», - новостные ресурсы большинства российских регионов от Астраханской области и Белгорода до Петербурга и Южно-Сахалинска…» ***(Владимир Кондрашов. Украинские хакеры поздравили россиян с "днем победобесия" // Internetua (http://internetua.com/ukrainskie-haker-pozdravili-rossiyan-s-dnem-pobedobesiya-). 10.05.2018).***

***

«17 и 18 мая в Киеве проходит первая практическая конференция по кибербезопасности NoNameCon 2018, первым докладчиком которой стал спикер Украинского киберальянса, известный в сети под ником Шон Таунсенд.

Единственное на данный момент «живое» появление Шона на публике было посвящено украинской наступательной кибероборонe.

… самые интересные тезисы выступления спикера УКА.

В феврале 2014 года мы поняли, что специалисты в области информационной безопасности могут помочь стране…

В 2014-м году это были разрозненные акции – не было методологии, было непонятно с кем мы имеем дело с российской стороны, но постепенно нарабатывался опыт…

В марте 2016 года появился Украинский киберальянс и мы начали работать против России уже более планомерно.

За несколько лет у нас накопились терабайты данных, взломаны тысячи аккаунтов. Часть информации публикуется, часть – получает Служба безопасности Украины и Министерство обороны, которые могут использовать её по назначению…

После атаки НеПети в Украине начала проводится определенная законодательная работа в сфере информбезопасности: появилась доктрина, принят Закон «Об основах обеспечения кибербезопасности». Около полугода назад мы решили проверить, насколько наша страна готова к массовым кибератакам.

В течении месяца мы проводили акцию #fuckresponsibledisclosure, потому что responsible disclosure просто не работал… Мы решили, что будем это делать открыто и без предупреждения: вначале всё попадет в прессу, Facebook поиздевается над «попавшимся» государственным учреждением, и останется посмотреть, сколько времени займет реакция. В течении месяца получилось взломать около десятка только центральных органов власти, включая министерства.

…Практически никто из уязвимых организаций не написал, что была атака (не важно, учебная, или настоящая). Никто публично не отчитался о закрытии уязвимости. Никто не проанализировал, что собственно, произошло…

Такая же ситуация практически со всеми «настоящими» атаками…

Чтобы эффективно участвовать в кибервойне, требуются не только технические специалисты, но и новая организационная структура.…

Две ключевых особенности современной кибервойны – относительная дешевизна и взаимодействие небольших групп технических специалистов для достижения определенных целей.

Я считаю, что существующих законодательных норм в сфере кибербезопасности недостаточно. Существующий закон очень широко разделяет ответственность и полномочия между Госспецсвязью, СБУ и полицией. Получается, что как бы за информационную безопасность отвечают все, а когда случается настоящий инцидент, - не понятно к кому обращаться…

Необходимо провести дерегуляцию в области (информационной безопасности государственных ресурсов - Ред.). Если кто-то читал НД ТЗИ по веб-сайтам, то понимает, что выполнить эти рекомендации невозможно. Документ был принят очень давно и с тех пор не обновлялся. С одной стороны рекомендации необходимо выполнять, потому что такой закон, а с другой – просто нельзя, ведь документ неактуален. Получается, что тот же самый администратор в государственном учреждении по умолчанию уже виноват.

Начать нужно с упрощения правил. Не надо пытаться придумать новые, ещё более сложные, более невыполнимые требования, а упростить существующие.

Нужно ли единое ведомство? Я думаю, что эту функцию мог бы выполнять CERT-UA, но не по тем правилам, которые действуют сейчас.» ***(Владимир Кондрашов. Спикер Украинского киберальянса: российских хакеров курирует ФСБ // Internetua (http://internetua.com/spiker-ukrainskogo-kiberalyansa-rossiiskih-hakerov-kuriruet-fsb). 18 .05.2018).***

***

«…Работникам (кроме госслужащих) Вооруженных Сил, СБУ, Службы внешней разведки и других разведывательных органов, Госспецсвязи, которые обеспечивают кибербезопасность и киберзащиту выплатят надбавку за особый характер работы в размере до 50% должностного оклада.

Соответствующие изменения предусмотрены постановлениями Кабмина от 21 февраля 2018 года № 336 и № 337, которые вступили в силу 11 мая.

Также военнослужащим указанных госорганов, которые обеспечивают кибербезопасность и киберзащиту, будут ежемесячно выплачивать вознаграждение в размере до 100% должностного оклада с учетом оклада по воинскому званию и надбавки за выслугу лет.

Предельные размеры, порядок и условия выплаты такого вознаграждения и надбавки определит Минобороны, МВД, СБУ, Служба внешней разведки, Администрация Госспецсвязи.» ***(Киберзащитникам государства выплатят надбавку // Інформаційне агентство "ЛІГА:ЗАКОН (http://jurliga.ligazakon.ua/news/2018/5/11/170058.htm). 11.05.2018).***

***

«23 мая (Рейтер) - Cisco Systems Inc в среду предупредила, что хакеры заразили высокотехнологичным вредоносным ПО как минимум 500.000 маршрутизаторов и устройств хранения данных в десятках стран…

Talos, подразделение Cisco, занимающееся анализом угроз кибербезопасности, сообщило, что в большой степени уверено в том, что за кампанией, названной VPNFilter, стоит российское правительство, поскольку установленное ПО имеет код, аналогичный использованному в предыдущих кибератаках, в которых американское правительство обвинило Москву…

VPNFilter заражает маршрутизаторы и подключенные к интернету устройства хранения данных в домашних офисах и небольших конторах, однако все зараженные устройства вместе могут быть использованы для осуществления скоординированных атак более крупных целей…

Хотя зараженные устройства были обнаружены как минимум в 54 странах, Cisco выяснила, что целью хакеров была Украина…» ***(Джим Финкл в Торонто при участии Павла Политюка в Киеве. Cisco заподозрила Россию в подготовке кибератаки на Украину // Reuters (https://ru.reuters.com/article/topNews/idRUKCN1IO2LR-ORUTP). 23.05.2108).***

***

«СБУ попереджає про можливу масштабну кібератаку на державні структури та приватні компанії напередодні фіналу Ліги Чемпіонів та надає рекомендації із захисту від неї.

…Шкідливе програмне забезпечення, яке може бути використано хакерами, отримало умовну назву VPNFilter…

Особливу небезпеку VPNFilter несе для автоматизованих систем управління технологічними процесами (SCADA), оскільки через ідентифікацію специфічних протоколів обміну технологічними даними зловмисники отримують можливість обрати такі об’єкти першочерговими цілями…

Враховуючи можливі ризики, СБУ та Нацполіція невідкладно та адресно поінформували потенційних "жертв" атаки. Зокрема, поінформувала відповідні об’єкти критичної інфраструктури та органи державної влади (у тому числі з використанням платформи MISP-UA)…

Наразі фахівцям відомо про уразливість наступних мережевих пристроїв: Linksys Devices: E1200, E2500, WRVS4400N; Mikrotik RouterOS Versions for Cloud Core Routers: 1016, 1036, 1072; Netgear Devices: DGN2200, R6400, R7000, R8000, WNR1000, WNR2000; QNAP Devices: TS251, TS439 Pro, Other QNAP NAS devices running QTS software; TP-Link Devices R600VPN…». ***(Євген Дем’янов. СБУ попереджає про можливість кібератак напередодні фіналу Ліги Чемпіонів // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1732302-sbu-poperedzhaye-pro-mozhlivist-kiberatak-naperedodni-finalu-ligi-chempioniv). 23.05.2018).***

***

«…В Росії створені кібервійська, які здатні вражати критичну інфраструктуру, наголошує експерт з міжнародної торгівлі, член Економічного

дискусійного клубу Руслан Осипенко. І Україні, на його думку, також варто створити такі…

При цьому, за словами експерта, Україні варто було б об'єднатися в цьому питанні зі світовою спільнотою…» ***(Україна має створити свої кібервійська – Осипенко // Радіо Свобода (https://www.radiosvoboda.org/a/29250713.html). 28.05.2018).***

***

«Россия не планировала хакерскую атаку против Украины, заявил пресс-секретарь президента Дмитрий Песков…» ***(Дмитрий Зубарев. Пескову задали вопрос об атаке на Украину с помощью роутеров // Деловая газета «Взгляд» (https://vz.ru/news/2018/5/24/924300.html). 24.05.2018)***.

***

Боротьба з кіберзлочинністю в Україні

«Уроженец Скадовска Херсонской области, лейтенант полиции – оперуполномоченный сектора криминальной полиции Левобережного отделения полиции Винницкого ОП ГУНП в Винницкой области был осужден на 3 года лишения свободы с испытательным сроком в 2 года за продажу информации с баз данных Интегрированной информационно-поисковой системы органов внутренних дел МВД Украины…

Как гласит приговор Ровенского городского суда Ровенской области, полицейский пошел на сделку со следствием и признал свою вину. Он признал, что в группе в Telegram «Темы Украина» в феврале-марте этого года размещал объявления о продаже пользователям группы информации с ограниченным доступом о персональных данных лиц…

Приговор Ровенского суда, тем не менее, оставляет достаточно вопросов открытыми.

Первый из них – откуда у обычного оперуполномоченного возможность отслеживать движение по счетам в Приватбанке, Укргазбанке, сведения от «Новой почты», получать информацию о месте пребывания мобильного телефона и от операторов без соответствующего разрешения сверху и решения суда?..

Почему за тем, какую информацию получал полицейский, никто не следил?..

Почему следствие не установило, откуда у полицейского возможность пользоваться базами банков и Новой Почты?..» ***(Владимир Кондрашов. Полицейскому дали два года за продажу базы данных МВД // Internetua (http://internetua.com/policeiskomy-dali-dva-goda-za-prodaju-bazy-dannuh-mvd). 04.05.2108).***

***

«Команда реагирования на компьютерные чрезвычайные происшествия Украины CERT-UA напоминает о необходимости принятия мер для устранения критической уязвимости CMS Drupal…

Указанная уязвимость в ядре CMS Drupal позволяет злоумышленникам выполнить произвольный код и полностью скомпрометировать файлы сайта. Все файлы могут быть удалены или изменены независимо от прав доступа… На официальном сайте Drupal указано, что рабочий эксплойт (программа для эксплуатации уязвимости) разработан и широко используется, поэтому нужно считать все сайты, которые не были обновлены до 11.04.2018 - потенциально скомпрометированными…

Для устранения уязвимости в CERT-UA рекомендуют обновить Drupal до актуальных версий: Drupal 7.x - 7.59, Drupal 8.5.x – 8.5.3, Drupal 8.4.x – 8.4.8. (Версия 8.4.x больше не поддерживается, рекомендуется обновиться до версии 8.5. или установить эти обновления), Патч для 8.5.x и ниже, Патч для 7.x…» ***(Владимир Кондрашов. CERT-UA просит собственников сайтов на Drupal немедленно принять меры против взлома // Internetua (http://internetua.com/cert-ua-prosit-sobstvennikov-saitov-na-drupal-nemedlenno-prinyat-mer-protiv-vzloma). 02.05.2018).***

***

«Є кілька категорій, які загрожують кібербезпеці України. Серед них – школярі. Таку думку висловив експерт Володимир Стиран…

«…Це може бути будь-який китайський підліток, який не в своїй юрисдикції може робити, що хоче», – сказав він.

За його словами, є ще одна категорія кіберзлочинців.

«…Кіберкримінал – це ще один щабель розвитку криміналу як такого. Хакери, які заробляють тим, що крадуть у людей гроші, вони будуть завжди», – зазначив експерт». ***(Україні варто боятися школоти і криміналу – експерт // Vse.Media (http://vse.media/ukrayini-varto-boyatisya-shkoloti-i-kriminalu-ekspert/). 10.05.2018).***

***

«В Украине вскрыли канал продаж пиратских операционных систем (ОС) Windows. Причем злоумышленники продавали компьютеры с «паленими» ОС не только рядовым украинцам, но и даже выигрывали государственные тендеры на поставку продукции министерствам и ведомствам.

…свой товар дельцы маскировали под лицензионный с помощью поддельных Сертификатов аутентичности - специальных наклеек, которые обычно присутствуют на оригинальной продукции Microsoft.

…Покупатели легко ведутся и покупают компьютеры с поддельными наклейками, поскольку цена на нее значительно ниже, нежели стоимость лицензионного софта…» ***(Безупречная подделка: украинцам вовсю продают компьютеры с "липовой" Windows // АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/236835-bezuprechnaja_poddelka_ukraintsam_vovsju_prodajut_kompjjutery_s_lipovoj_windows). 10.05.2018).***

***

«У створенні та розповсюдженні шкідливих програм працівники відділу протидії кіберзлочинності Луганщини викрили 20-річного жителя міста Рубіжне Луганської області…

Так, 20-річний студент розповсюджував серед користувачів мережі шкідливе програмне забезпечення типу криптомайнер, Стіллер і модифіковану програму для здійснення віддаленого управління персональними комп'ютерами RemoteManipulatorSystem (RMS).

Фахівці з кіберполіції встановили, що з його допомогою зловмисник втрутився в роботу близько 6000 комп'ютерів…

За даним фактом слідчі почали 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) КК України…» ***(Поліція затримала 20-річного хакера // Інформаційне агентство АСПІ (https://aspi.com.ua/ua/suspilstvo/politsiya-zatrymala-20-richnoho-khakera.html?view=item&id=11927:politsiya-zatrymala-20-richnoho-khakera). 17.05.2018).***

***

«Полтавська прокуратура завершила досудове розслідування щодо Геннадія Капканова, полтавця, якому інтерпол інкримінує ряд міжнародних кіберзлочинів.

…30 листопада 2016 року полісмени провели міжнародну спецоперацію з ліквідації кібермережі «Avalanche». Тоді в Полтаві правоохоронці затримали й організатора цієї злочинної діяльності – Геннадія Капканова…

1 грудня 2016 року Октябрським районним судом м. Полтави було розглянуто клопотання представника Генеральної прокуратури України про його арешт. У обранні саме такого запобіжного заходу суд відмовив після чого підозрюваний зник із зали суду. Пізніше його оголосили в міжнародний розшук.

Понад рік Капканов переховувався від слідства і був розшуканий у лютому 2018 року у Києві з підробленим паспортом…

Відповідно до українського законодавства, йому інкримінують причетність до вчинення кількох кримінальних правопорушень. Водночас прокуратурою Вердена і поліцією Люнебурга (Федеративна Республіка Німеччина) розслідується кримінальна справа щодо міжнародної платформи злочинної інфраструктури, відомої як «Avalanche», яка використовувалась в якості майданчика для запуску та управління масових глобальних шкідливих атак і відмивання грошей. У Німеччині, за оцінками експертів, це спричинило збитків на понад 6 мільйонів євро. Крім того, грошові втрати пов’язані з кібератаками, проведеним по мережі «Avalanche», за попередніми підрахунками, склали сотні мільйонів євро по всьому світу…» ***(Марина Левчук. Справу полтавця Геннадія Капканова, якого підозрюють у міжнародних кіберзлочинах, передали до суду // Новини Полтави (http://kolo.news/category/criminal/8751). 18.05.2018).***

***

«…Из Энергодарской местной прокуратуры в Запорожской области поступило сообщение о том, что неустановленные лица несанкционированно вмешались в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи на ОП «Запорожская АЭС» ГП НАЭК «Энергоатом», чем вызвали утечку информации, ограниченной для общего пользования, что может нанести значительный ущерб интересам указанного предприятия.

…к указанному уголовному преступлению причастны 2 технолога отдела ядерной безопасности ЗАЭС и технолог - руководитель ОЯБ ОП ЗАЭС**.**

Уголовное производство было открыто 19 марта, хотя информацию об утечке данных с Запорожской АЭС в рамках акции #fuckresponsibledisclosure, инициированной Украинским кибераьянсом, опубликовал в ещё декабре прошлого года хактивист, известный под ником Дмитрий Орлов. Ему удалось обнаружить в открытом доступе внутреннюю документацию ЗАЭС, среди которой такие документы как Акт технического состояния объекта ядерной безопасности, служебные записки, Анализ герметичности оболочек ТВЭЛ ТВС и прочее…». ***(Владимир Кондрашов. За утечкой данных Запорожской АЭС стоят сотрудники отдела ядерной безопасности // Internetua (http://internetua.com/za-utecskoi-dannh-zaporojskoi-aes-stoyat-sotrudniki-otdela-yadernoi-bezopasnosti). 22.05.2018).***

***

«Должностные лица отдела связи и коммуникации ГУ Нацполиции в Ровенской области около четырех месяцев занимались майнингом криптовалют непосредственно на рабочем месте…

Досудебным расследованием установлено, что с начала 2018 года должностные лица отдела связи и коммуникации ГУНП в Ровенской области, злоупотребляя своим служебным положением, действуя вопреки интересам службы, самовольно использовали электрическую энергию ГУНП в Ровенской области в собственных целях, для надлежащего функционирования оборудования для добычи криптовалют, чем нанесли существенный вред интересам ГУНП в Ровенской области…

Какую именно криптовалюту майнили в областной полиции, в судебном решении не уточняется. Также неизвестно, сколько электроэнергии, которую нерадивые «должностные лица» использовали на добычу криптовалют, оказалось необходимо, дабы принести «существенный вред интересам» областного управления полиции.

…помещение, где нашли работающее оборудование для майнинга, входит в комплекс зданий, используемых Ровенским городским отделом полиции и Ровенским ГУНП в области…» ***(Владимир Кондрашов. Ровенские полицейские майнили криптовалюту прямо в помещении областного ГУНП // Internetua (http://internetua.com/rovenskie-policeiskie-mainili-kriptovaluatu-pryamo-v-pomesxenii-oblastnogo-gunp). 22.05.2018).***

***

«…у Верховній Раді вже зареєстровано законопроект №8304, який має посилити відповідальність за кіберзлочини. Змінами пропонується за кіберзлочини встановити покарання у вигляді восьми років позбавлення волі. Крім того, заплановано збільшення розміру штрафу за створення і поширення шкідливого програмного забезпечення.

…Департамент кіберполіції ініціює низку змін до законодавства у сфері забезпечення безпеки у кіберпросторі. Першочергові з них стосуватимуться обов'язків і правил для постачальників контенту, зокрема покладення обов'язків на провайдерів інтернет-зв'язку із зберігання та логування незаконних процесів, які відбуваються у Мережі. Передбачається, що зберігання такої інформації відбуватиметься за запитом правоохоронних органів та триватиме до 90 діб…» ***(Відповідальність за кіберзлочини необхідно посилити, - Демедюк // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (http://day.kyiv.ua/uk/news/210518-vidpovidalnist-za-kiberzlochyny-neobhidno-posylyty-demedyuk). 21.05.2018).***

***

«Упродовж останніх чотирьох років Україна є полігоном випробування всіх можливих кіберзагроз: хакерських атак, фейкових новин, пропаганди, яка видається за медіаконтент, та інформаційних операцій за участі «тролей». До всіх цих методів (і не лише них) Росія вдається в рамках гібридної війни проти України, застосовучи деякі з них також щодо інших країн…

Саме про це говорили президент Естонії в 2006-2016 роках Тоомас Хендрік Ільвес (Toomas Hendrik Ilves), колишній директор Агентства національної безпеки США, генерал Кіт Александер (Keith Alexander), екс-радник двох Держсекретарів США та експерт із технологій Джаред Коен (Jared Cohen) за модерації американської журналістки та експертки з міжнародних відносин Енн Епплбаум (Anne Applebaum).

Відкрита дискусія на тему «Кібербезпека та дезінформація в Україні та на Заході» відбулася в Києві 24 травня в рамках проекту «Публічні лекції» Фонду Віктора Пінчука…» **(Катерина Толокольнікова. Світ зможе захищатися від кіберзагроз, тільки виробивши спільне рішення // MediaSapiens (http://ms.detector.media/web/cybersecurity/svit_zmozhe_zakhischatisya_vid_kiberzagroz_tilki_virobivshi_spilne_rishennya/?media=print). 28.05.2018).**

***

Міжнародне співробітництво у галузі кібербезпеки

«Сполучені Штати Америки збільшують допомогу Україні за напрямком кібербезпеки з 5 до 10 млн дол. Про це сьогодні заявив заступник державного секретаря США у справах Європи і Євразії Весс Мітчелл на брифінгу у Києві…» ***(Олександр Сивачук. США збільшать допомогу Україні на кіберзахист удвічі // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1728419-ssha-zbilshat-dopomogu-ukrayini-na-kiberzakhist-udvichi). 02.05.2018).***

***

«Палата представників американського Конгресу підтримала виділення 250 млн доларів на безпекову допомогу Україні у рамках законопроекту про оборонний бюджет США на 2019 рік…

Сума коштів, яку пропонується виділити, на 100 млн доларів більша, ніж Комітет пропонував надати у поточному бюджетному році. …до документа включено основні положення проекту "Закону про співпрацю з Україною з питань кібербезпеки".

"Він, зокрема, передбачає допомогу Україні у посиленні власних спроможностей щодо захисту від кібератак, забезпеченні безпеки комп'ютерних мереж органів державної влади, зменшенні залежності від російських інформаційних та комунікаційних технологій, сприянні участі у програмах обміну інформацією", — зазначили у посольстві…» ***(Олексій Супрун. Палата представників Конгресу США підтримала законопроект з 250 млн доларів для оборони України // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1732573-palata-predstavnikiv-kongresu-ssha-pidtrimala-zakonoproekt-z-250-mln-dolariv-dlya-oboroni-ukrayini). 25.05.2018).***

***

«Подвоєння допомоги США Україні для посилення кібербезпеки може бути пов'язане з тим, що сам Вашингтон зазнав атаки під час виборів, припускає економіст Ілля Несходовський. Політолог Микола Бєлєсков також цього не виключає, проте підкреслює: українська влада повинна бути готова до того, що допомога від Штатів буде поступово скорочуватись, і вчитись обходитись без неї…» ***(Кібербезпека в Україні: чому Вашингтон різко збільшив допомогу Києву // Радіо Свобода (https://www.radiosvoboda.org/a/29206027.html). 03.05.2018).***

***

«Голова Верховної Ради України Андрій Парубій під час зустрічі з делегацією парламентаріїв Саейму Латвійської Республіки на чолі зі Спікером Інарою Мурнієце зазначив, що для вивчення загроз гібридної війни та напрацювання рекомендацій і відповідей на її виклики дуже важливим є створення регіонального центру протидії гібридній агресії…

Учасники зустрічі обговорили формат подальшої співпраці на рівні парламентів обох країн, зокрема, у питаннях протистояння російській агресії, гібридній війні тощо.

Голова Верховної Ради також поінформував латвійських парламентаріїв про хід реформ в Україні, зокрема … у сфері кібербезпеки, в ухваленні Антикорупційного суду та закону про національну безпеку і оборону…

Інара Мурнієце підкреслила, що Латвія завжди підтримувала і підтримуватиме Україну в її боротьбі за свободу, та зазначила, що західні партнери зрозуміли, звідки виходить кібер- та інформаційна загроза, і відчули, як зріс її рівень...». ***(«Для протидії гібридній агресії важливим є створення окремого регіонального центру», - Голова Верховної Ради України Андрій Парубій //***

Народна Рада (http://narodnarada.info/news/dlya-protidiji-gibridniy-agresiji-vajlivim-news-98296.html). 16.05.2018).

***

«Президенты России и Франции Владимир Путин и Эммануэль Макрон обсудили необходимость разработки международных правил поведения и контроля в киберсфере.

Комментируя проблему кибератак, Путин сказал, что «действие всегда встречает противодействие», и, если кому-то противодействие «не нравится», необходимо «договориться о правилах поведения»…

… Глава российского государства призвал выработать правила совместной работы в этой сфере…» ***(Антон Антонов. Путин и Макрон решили попробовать договориться о контроле в киберсфере // Деловая газета «Взгляд» (https://vz.ru/news/2018/5/25/924427.html). 25.05.2018).***

***

«На текущей неделе делегация Госдепартамента США встретится с коллегами в Брюсселе и Лондоне. На повестке дня стоит усиление информационной защиты, а также восстановление полноценного политического диалога.

…на днях сотрудник Госдепа Дэвид Тесслер официально заявил о необходимости введения новой должности чиновника, который курировал бы киберсферу, а также имел бы рычаги, позволявшие в случае необходимости предпринять ограничительные меры. Детали не уточнялись. Ожидается, что данный вопрос будет подробнее затронут на предстоящем саммите G7, который пройдёт в июне в Канаде…

Вашингтон понимает, что санкционное противостояние лишь ухудшает трансатлантические отношения, в то время как диалог ЕС с Россией становится все более и более конструктивным. … В этой связи возвращение к педалированию темы «агрессии российских хакеров» воспринимается Госдепом как реальная возможность укрепить ухудшившиеся отношения с Европой…» ***(Александр Ходякин. США усилят давление на ЕС по вопросу кибербезопасности, пишут СМИ // «Парламентская газета» (https://www.pnp.ru/politics/ssha-usilyat-davlenie-na-es-po-voprosu-kiberbezopasnosti-pishut-smi.html). 25.05.2018).***

***

«Україна зацікавлена в чеському досвіді посилення кібербезпеки, заявила віце-прем'єр-міністр з питань європейської та євроатлантичної інтеграції України Іванна Климпуш-Цинцадзе на зустрічі з головою комітету із закордонних справ, оборони та безпеки сенату парламенту Чехії Франтішеком Бубланом…

Крім того, вона додала, що Україна розраховує на допомогу Чехії в просуванні європейських та євроатлантичних прагнень країни в інституціях ЄС та НАТО і подякувала Чехії за підтримку санкцій проти Росії і стійку позицію щодо територіальної цілісності України.

Ф.Бублан, у свою чергу, оцінив прогрес України в проведенні реформ на тлі конфлікту з Росією та наголосив, що Чехія і надалі допомагатиме Україні...» ***(Україна зацікавлена в чеському досвіді посилення кібербезпеки - Климпуш-Цинцадзе // Інтерфакс-Україна (https://ua.interfax.com.ua/news/general/507409.html). 24.05.2018).***

***

Світові тенденції в галузі кібербезпеки

«Аналитический материал от Фонда электронных рубежей (EFF) о тенденциях регулирования криптографии…

Тема шифрования снова у всех на устах, поскольку официальные лица США настойчиво требуют поставить под угрозу IT-безопасность пользователей, оставляя в системах шифрования лазейки для правоохранительных органов. Эти противники шифрования предполагают, что возможна «золотая середина»: использовать устойчивое шифрование с «исключительным доступом» на дешифрование для правоохранительных органов.

…большинство экспертов по-прежнему единодушны – «исключительный доступ» независимо от реализации ослабляет безопасность…

- Во-первых, если это будет санкционировано правительством, это нарушит Первую поправку [к конституции США] в соответствии с доктриной «принуждения к речи», которая запрещает правительству принуждать отдельного человека, компанию или организацию раскрывать какую-либо информацию.
- Во-вторых, принуждение технологических компаний к ослаблению безопасности шифрования ставит под угрозу пользователей. В 1990-х годах Белый дом представил микросхему Клиппер, поддерживающую бэкдор в системе шифрования. Исследователь безопасности компании AT&T Мэтт Блейз (Matt Blaze) обнаружил огромные недостатки безопасности в системе, показав, что метод взлома полным перебором («brute-force attack») может скомпрометировать технологию.
- В-третьих, «исключительный доступ» может нанести ущерб предприятиям США и охладить инновации. Правительство США не может остановить развитие технологий шифрования; он может просто «выдавить» его за границу.
- Наконец, исключительный доступ не срабатывает при предотвращении преступления. Независимо от требований, предъявляемых правительством к компаниям США, высокотехнологичные преступники все ещё могут получить устойчивое шифрование вне США.

Несмотря на согласие среди IT-экспертов, некоторые директивные органы продолжают искать невозможную «золотую середину». В прошлом месяце, после нескольких лет исследований, Национальная академия наук США опубликовала отчёт о шифровании и «исключительном доступе», который сузил вопрос «должно ли государство требовать «исключительный доступ» к содержанию зашифрованных сообщений?» до вопроса «как правительство может это потребовать без ущерба для безопасности пользователей?»…

Исследования ведутся не только в Академии. В прошлом месяце международный исследовательский институт EastWest Institute опубликовал отчёт, в котором предлагается «две политики «золотой середины», сбалансированные и учитывающие риски, для поддержки более конструктивного диалога».

Наконец, на прошлой неделе журнал Wired опубликовал статью, посвящённую бывшему техническому директору Microsoft Рэю Оззи (Ray Ozzie) и его попытке найти модель исключительного доступа для телефонов, которая могла бы удовлетворить «как правоохранителей, так и поборников конфиденциальности». Хотя Оззи, возможно, действовал из лучших побуждений, эксперты Мэтт Грин, Стив Белловин, Мэтт Блейз, Роб Грэхем и другие, быстро указали на существенные недостатки его идеи. Никакая система не идеальна, а система, имеющая бэкдор и предназначенная для миллиардов телефонов, имеет огромную цену ошибки…» ***(Евгения Хотовицкая. Шифрование не терпит компромиссов // РосКомСвобода (https://roskomsvoboda.org/38703/). 10.05.2018).***

***

«На пресс-конференции в рамках форума Positive Hack Days 8 эксперт Positive Technologies, международной компании, специализирующейся на решениях по информационной безопасности, представил итоги анализа защищенности корпоративных систем российских и зарубежных компаний в 2017 году…

При проведении тестирования на проникновение от лица внутреннего злоумышленника исследователям во всех без исключения случаях удалось захватить полный контроль над инфраструктурой. При этом только в 7% систем сложность получения доступа к критически важным ресурсам оценивалась как средняя…

Исследователи Positive Technologies в ходе проектов по анализу защищенности выявляли в среднем два вектора проникновения во внутреннюю сеть организации. Максимальное число обнаруженных векторов составило 10, а возраст самой старой выявленной уязвимости CVE-1999-0532 составляет 18 лет.

Удобным способом проникновения в локальные вычислительные сети (ЛВС) являются беспроводные сети. По статистике, 40% компаний используют словарные пароли для подключения к своим сетям Wi-Fi. При этом 75% таких сетей доступны за пределами контролируемой зоны компании…

«Еще одно слабое звено в защите корпоративных сетей — сотрудники, которые легко поддаются методам социальной инженерии, — рассказывает руководитель экспертного центра безопасности Positive Technologies (PT Expert Security Center) Алексей Новиков. — К примеру, 26% сотрудников осуществляют переход по ссылке на фишинговый веб-ресурс, причем практически половина из них в дальнейшем вводят свои учетные данные в поддельную форму аутентификации. Каждый шестой сотрудник запускает приложенные к письму зловредные файлы. Кроме того, 12% сотрудников готовы вступить в диалог с нарушителем и раскрыть важную информацию»…

Для противодействия внутренним нарушителям необходим комплексный подход к защите. Как минимум следует использовать только актуальные версии ОС

и ПО, а также стойкие к подбору пароли для всех пользователей на всех ресурсах, особенно для администраторов…» ***(Positive Technologies: в 100% случаев внутренний злоумышленник может захватить полный контроль над сетью // Positive Technologies (https://www.ptsecurity.com/ru-ru/about/news/292402/). 16.05.2018).***

***

«Некоммерческая организация Open Web Application Security Project (OWASP) выпустила рекомендации для разработчиков ПО, которые хотят поддерживать актуальный уровень защиты своих продуктов. Документ содержит 10 пунктов, на которые следует обратить внимание при создании веб-приложений, чтобы не оставить в коде возможности для взлома и кражи данных.

С1. Следование актуальным требованиям безопасности…

С2. Использование безопасных фреймворков и библиотек…

С3. Обеспечение защищенного доступа к базам данных…

С4. Шифрование и безопасность данных…

С5. Проверка входящих данных…

С6. Защита “цифровой личности”…

С7. Управление доступом…

С8. Повсеместная защита информации…

С9. Мониторинг и ведение журналов безопасности…

С10. Корректная обработка ошибок и исключений…» ***(Egor Nashilov. OWASP опубликовала руководство по защите веб-приложений // Threatpost (https://threatpost.ru/owasp-released-web-apps-security-manual/26093/). 17.05.2018).***

***

«…25 мая, начинает действовать Общий регламент Европейского Союза по защите данных (GDPR). Этот документ приходит на замену ныне действующей Директиве ЕС и вносит существенные коррективы в европейскую политику защиты персональных данных…

Общий регламент Европейского Союза по защите данных призван гарантировать гражданам ЕС лучшую защиту персональных данных, вне зависимости о того, на какой территории эти данные хранятся.

Регламент, по сравнению с предыдущей Директивой, существенно расширяет понятие персональных данных, уточняет и расширяет понятие чувствительных данных…

Чувствительные данные, согласно Общему Регламенту, определяются по ряду признаков, которые базируются на информации о расовом или этническом происхождении, политическим взглядам, религиозным или философским убеждениям, профессиональном членстве, здоровье или сексуальной жизни, генетических и биометрических данных.

Новый Регламент действует в отношении любой компании, независимо от её расположения, если бизнес работает с персональными данными граждан ЕС.

GDPR существенно расширяет права частных пользователей. Им предоставляются права на перемещение, ограничение обработки, отрицание и

удаление данных. Также частным лицам предоставляется право на получение ответа на запрос.

Согласно новым правилам, компании теперь обязаны сообщать об утечках данных и вести журнал учета таких случаев.

Также GDPR устанавливает новые правила получения согласия на обработку персональных данных. В частности, предусматривается два вида согласия: простое согласие и безусловное согласие.

Простое согласие – конкретное и однозначное указание субъекта данных, при помощи заявления или четкого позитивного действия, которым выражается согласие на обработку данных.

Безусловное согласие предоставляется при обработке специальных категорий данных, перемещении данных в третьи страны и т.д…

Общий регламент Европейского Союза по защите данных устанавливает достаточно серьезные штрафы за нарушение новой европолитики. В частности, компания может заплатить 20 миллионов евро или 4% от годового дохода за нарушение ключевых положений Регламента, прав субъектов персональных данных, нормативов передачи личных данных и др…». ***(Владимир Кондрашов. Новая угроза для украинских IT компаний // Internetua (http://internetua.com/novaya-ugroza-dlya-ukrainskih-it-kompanii). 21.05.2018).***

***

«Chicago Tribune, LA Times и ряд других американских СМИ сообщили, что их сайты недоступны в большинстве европейских стран после вступления в силу новых правил ЕС по защите персданных — GDPR.

Общий регламент по защите данных (General Data Protection Regulation, GDPR) предоставляет резидентам ЕС инструменты для контроля своих персональных данных…

В связи с вступлением в силу 25 мая GDPR, были в ряде прочих затронуты новостные сайты издательств Tronc и Lee Enterprises. Наиболее популярные сайты издательства Tronc – New York Daily News, Chicago Tribune, LA Times, Orlando Sentinel и Baltimore Sun…

CNN и New York Times не пострадали. The Washington Post и Time теперь требуют от европейских пользователей ЕС принять новые условия использования сайтов…» ***(Евгения Хотовицкая. Американские новостные сайты недоступны в Европе из-за нового закона о персданных // РосКомСвобода (https://roskomsvoboda.org/39227/). 27.05.2018).***

***

«Редакторы популярного американского журнала Wired попытались предсказать семь ключевых явлений в киберпространстве, которые в ближайшем будущем повлияют на нашу реальность, а художник Сэмми Гэркем проиллюстрировал их рассуждения остроумными иллюстрациями. В центре внимания оказались кибератаки в интернете вещей (взломанный город), роботизированная доставка (верный покупатель), личные данные (нарцисс), генная

инженерия (откровение), автопилот (призрачный автопарк), виртуальная реальность (всадник в шлеме) и, конечно же, блокчейн в виде невидимого оленя…

По оценкам редакции Wired, блокчейн перестроит интернет, который мы знаем. Они отмечают, что для интернет-идеалистов блокчейн стал опьяняющей технологией…

Авторы отмечают, что как только технология созреет, она станет одной из фундаментальных систем, питающих интернет...» ***(WIRED: Блокчейн перестроит интернет, который мы знаем // BIGFIN (https://bigfin.net/23/05/2018/wired-blokchejn-perestroit-internet-kotoryj-my-znaem/). 23.05.2018).***

***

Сполучені Штати Америки

«Администрация президента США сократила созданную при Бараке Обаме должность координатора Белого дома по вопросам кибербезопасности…

«Должности киберкоординатора больше не будет»,— говорится в электронном письме Кристин Самуелиян, помощника советника Дональда Трампа по национальной безопасности Джона Болтона.

…инициатором этого решения стал сам Джон Болтон, пришедший в президентскую администрацию в марте.

Должность киберкоординатора Белого дома в президентство Дональда Трампа занял аналитик Агентства национальной безопасности США Роб Джойс…» ***(Белый дом отказался от услуг координатора по кибербезопасности // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3629618). 16.05.2018).***

***

«Американские эксперты по кибербезопасности обеспокоены тем, что после решения президента США Дональда Трампа выйти из ядерной сделки с Ираном кибертатаки из этой страны участятся…

Через сутки после заявления господина Трампа компания CrowdStrike сообщила о «заметном росте» киберактивности иранских хакеров. По информации компании, они рассылали вредоносные файлы американским дипломатам и сотрудникам телекоммуникационных компаний. Кроме того, иранские хакеры на протяжении двух месяцев исследовали интернет-адреса, которые принадлежат военным структурам США в Европе. Подробности атак не афишируют, потому что ведется расследование…» ***(NYT: в США опасаются кибератак из Ирана после выхода США из ядерной сделки // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3627839). 12.05.2018).***

***

«В Конгресс США в очередной раз внесли законопроект о защите данных. Согласно документу, любым правительственным организациям запрещается требовать от компаний внедрения бэкдоров в устройства или

приложения, а судам – принимать решения, вынуждающие производителей нарушать конфиденциальность…

Единственное исключение коснулось требований, регулируемых законом 1994 года “О помощи и содействии провайдеров телекоммуникационных услуг правоохранительным органам” (CALEA).

Политики считают, что компании, создающие возможность для обхода шифрования в своих продуктах, ставят под угрозу безопасность множества пользователей. Этого не оправдывает даже то, что время от времени бэкдоры помогают поймать преступника. Кроме того, по мнению члена Палаты представителей Зои Лофгрен (Zoe Lofgren), правительственные структуры даже без постановления суда имеют больший доступ к данным, чем когда-либо ранее. В то же время количество чувствительной информации в памяти устройств постоянно растет, и ее защита и так представляет собой непростую задачу…» ***(Julia Glazova. В США снова хотят запретить госслужбам требовать бэкдоры // Threatpost (https://threatpost.ru/congress-wants-to-prohibit-feds-from-demanding-encryption-backdoors/26048/). 15.05.2018).***

***

«Новая концепция Пентагона предусматривает возможность вывода из строя пусковых ракетных установок противника еще до удара – с помощью кибератак… зафиксирована в служебных рекомендациях Пентагона от мая 2017 года. При этом меморандум не был засекречен.

В документе подчеркивается, что «предконфликтное подавление пуска» обосновано только в случае «неизбежного ракетного удара». Что подразумевается под этим понятием, не указывается, как и не называются вероятные противники, в отношении которых возможно применение этой концепции.

Эксперты… предполагают, что целью для подобных кибератак могла стать в первую очередь КНДР…». ***(Сергей Гурьянов. Пентагон собрался уничтожать ракетные установки противника новым способом // Деловая газета «Взгляд» (https://vz.ru/news/2018/5/22/924019.html). 22.05.2018).***

***

Країни ЄС

«Европейский Центробанк (ЕЦБ) объявил о запуске программы проверки на кибербезопасность банковской системы, …в ходе которой участников финансового рынка будут проверять на прочность к кибератакам. Проект называется «Европейская программа по отражению угроз с использованием специальных экспертов, атакующих систему извне» (European Framework for Threat Intelligence-based Ethical Red Teaming — TIBER-EU). Программа носит рекомендательный характер — ЕЦБ отмечает, что страны-члены ЕС могут сами решать, когда и как проводить подобные проверки своих финансовых учреждений…

ЕЦБ отмечает, что киберзащиту проверят на прочность как штатные сотрудники, так и независимые специалисты по кибербезопасности…» ***(Евгений Хвостик, Алена Миклашевская. ЕЦБ обратится к хакерам для проверки кибербезопасности финансового сектора . Устойчивость к кибератакам протестируют на общеевропейском уровне // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3619220?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). 02.05.2018).***

***

«Міністр оборони Німеччини Урсула фон дер Ляєн має намір відмовитися від зосередження Бундесверу на участі в міжнародних миротворчих місіях, як це було в останні десятиліття...

"Концепція Бундесверу" враховує нові сценарії, зокрема кібератаки… Проект документа конкретизує положення, записані в новій "Білій книзі" - військово-політичній стратегії, схваленій урядом ФРН влітку 2016 року.

У ній ідеться, що ситуація в сфері безпеки значним чином змінилася. Криза на Сході України і анексія Росією Криму продемонстрували, що світоустрій в Європі під загрозою. РФ названо в "Білій книзі" викликом безпеці на континенті…» ***(Бундесвер підвищує пріоритет захисту країни і союзників по НАТО // Європейська правда (https://www.eurointegration.com.ua/news/2018/05/4/7081297/). 04.05.2018).***

***

«Минюст ФРГ призвал компанию Facebook принять дополнительные меры по защите личных данных пользователей соцсети.

Об этом говорится в письме, направленном министром юстиции Катариной Барли главе компании Facebook Марку Цукербергу…

По словам Барли… Facebook ранее публично объявил о проведении оптимизации в области защиты данных, в частности, в пользовательских настройках, и это "хорошее начало". Однако "процесс внесения изменений должен быть реализован как можно скорее"…

Кроме того, по словам Барли, речь идет также об обеспечении большей прозрачности для пользователей в том, что касается контроля персональных данных. Для этого Facebook предлагается установить внутренний режим контроля и введения санкций в случае нарушения правил или свободы выбора пользователей, указано в письме» ***(Наталья Селиверстова. Минюст Германии призвал Facebook усилить защиту данных пользователей // РИА Новости (https://ria.ru/world/20180503/1519852966.html). 03.05.2018).***

***

«…Британское издание «Express» опубликовало статью в которой пытается в очередной раз приписать России агрессивную позицию, в частности, речь идёт о кибератаках, которые Россия может направить не только против военных самолётов, но и против гражданских воздушных судов. В статье

специалисты предупреждают граждан о том, что полёты на пассажирских авиалайнерах могут оказаться весьма опасными, что обусловлено возможностью России проводить кибератаки на воздушные суда…

В статье также идёт речь об уязвимости аэропортов, гражданских самолётов и прочей инфраструктуре, причём, в качестве своего "противника", Великобритания видит Россию…» ***(Великобритания в панике: Россия может ронять самолёты // Avia. Pro (http://avia.pro/news/velikobritaniya-v-panike-rossiya-mozhet-ronyat-samolyoty). 07.05.2018).***

***

«Уряд Швеції почав поширення брошур з інструкціями щодо поведінки населення у разі настання війни або здійснення терористичних атак…

Автори буклетів зазначають, що навіть зараз Швеція страждає від кібератак і спроб впливу на думку громадян через поширення неправдивої інформації…

Проводити таку інформаційну компанію доручив уряд Швеції…» ***(Влада Швеції розіслала інструкції "будь готовим до війни" у всі 4,8 млн домівок // Європейська правда (https://www.eurointegration.com.ua/news/2018/05/21/7081992/). 21.05.2018).***

***

Китай

«За последние несколько лет китайские хакеры стали почти так же опасны и неуловимы, как русские: они перенаправляют трафик, читают почту через смартфоны и крадут военные тайны…

Bloomberg сообщает, что в 2016 году общее число китайских кибератак утроилось: тогда жертвами атак по всему миру стали сразу семь оборонных предприятий, специализирующихся на производстве ракет, радаров и навигационных технологий, пять министерств, четыре авиационные компании и две организации из сферы ядерной энергетики… При этом глава бюро кибербезопасности Управления киберпространства КНР Чжао Цзэлян даже не скрывает готовности Китая применить военную силу для обеспечения своей информационной безопасности.

В обнародованном в сентябре 2017-го обвинительном заключении федеральные прокуроры в Питтсбурге утверждают, что компания Boyusec (официальное название Bo Yu Guangzhou Information Technology Co.), специализирующаяся на кибербезопасности, в частности трое ее китайских сотрудников (двое из которых соучредители Boyusec), причастны к взлому трех крупных компаний: промышленного гиганта Siemens, агентства по экономическому анализу Moody's и компании-оператора GPS Trimble. Эти компании зафиксировали утечку важных данных. Согласно опубликованным данным, добычей злоумышленников стали около 407 Гб данных, относящихся к категории коммерческой тайны касательно энергетических, технологических и транспортных предприятиям Siemens…

Согласно внутреннему отчету Объединенного управления разведки J-2 Пентагона, Boyusec и Huawei работали вместе над созданием продуктов безопасности, которые были загружены в компьютерное и телефонное оборудование китайского производства, что позволяло китайской разведке собирать данные и контролировать компьютерное и телекоммуникационное оборудование.

Анонимная группа, известная как Intrusion Truth, опубликовала данные, которые связывают «подрядчика» китайской разведки Boyusec с кибератаками, которые были совершены группой кибершпионажа, известной как APT3. Согласно Intrusion Truth и Recorded Future, Boyusec является лишь одним из многих подрядчиков по кибербезопасности, которые китайское правительство использует для поддержки своих операций по сбору информации в рамках киберразведки.

…Kryptowire, специализирующаясяя на безопасности, определила несколько моделей мобильных устройств Android, содержащих прошивку, которая собирала конфиденциальные личные данные о своих пользователях и передавала эти конфиденциальные данные на сторонние серверы без раскрытия или согласия пользователей — эти устройства были доступны через крупные интернет-магазины в США (Amazon, BestBuy, например) и включали самые популярные смартфоны… New York Times оценил количество пораженных телефонов и прочих интеллектуальных устройств, которые держали связь с китайскими серверами, принадлежащими компании Shanghai Adups Technology Company, более известной как Adups, более чем в 700 млн…

Все это привело к ряду действий со стороны США и ее союзников по отключению китайских ИКТ-гигантов от американского рынка. В январе один из крупнейших американских операторов мобильной связи AT&T Inc. отказался от планов продажи телефонов Huawei в США, а в апреле власти США запретили китайской ZTE закупать продукцию американских технологических компаний, в том числе используемые компанией процессоры Intel и Qualcomm в течение семи лет…

Ранее индийские власти также запретили использование китайского оборудования от компаний Huawei и ZTE в приграничном регионе… NSA и другие американские разведывательные агентства… обеспокоены тем, что китайские ИКТ-гиганты могут получить техническую возможность контроля телекоммуникационного оборудования, которое китайская компания успешно поставляет в США, и на котором строится сетевая инфраструктура страны…

«Великая пушка» (Great Cannon) вошла в лексику кибервойны наряду с «Золотым щитом», или Великим Китайским файерволом, после того как новый инструмент цензуры в Поднебесной был назван и описан исследователями из Университета Торонто… «Великая пушка» — это оружие нападения, отличный инструмент атаки, который перехватывает зарубежный интернет-трафик, поступающий на китайские интернет-сайты, «дополняет» его вредоносным кодом и перенаправляет по своему усмотрению...

По мнению авторов исследования из Университета Калифорнии в Беркли и Университета Торонто, недавно «Большая пушка» собрала трафик, предназначавшийся для Baidu (крупнейший китайский поисковик, аналог Google),

а затем перенаправила его, уже в виде DDoS-атаки, на популярный у программистов сервис GitHub и сайт GreatFire.org, помогающий обходить применяемые в Китае интернет-блокировки, а также размещающий «зеркала» СМИ, запрещенных в Китае (например, The New York Times). Атака, которая длилась 4 дня, использовала в качестве оружия трафик обычных пользователей китайского интернета…

Возможности «Великой пушки» не ограничиваются банальными, пусть и очень мощными, DDoS-атаками. Система может быть легко модернизирована для осуществления шпионажа и за любым пользователем интернета, на чей компьютер загружается какой-либо контент с сервера, расположенного в Китае. Для этого вовсе не обязательно заходить на китайский сайт — достаточно, например, отображения на любом сайте рекламы из китайской рекламной сети.

Впрочем, есть один простой способ защититься от «Великой пушки» — шифровать все веб-сайты в интернете. Система при всей своей сложности не сможет манипулировать трафиком, который эффективно шифруется…» ***(Виртуальное господство: как китайские хакеры завоевывают мир через смартфоны // Goodnews.ua (http://goodnews.ua/technologies/virtualnoe-gospodstvo-kak-kitajskie-xakery-zavoevyvayut-mir-cherez-smartfony/). 27.05.2018).***

***

Російська Федерація та країни ЄАЕС

«…Помочь в борьбе с дропперами (лица, через чьи банковские карты хакеры выводят похищенные средства) должен законопроект, который сейчас готовится ко второму чтению в Госдуме… Обмен информацией согласно проекту предполагается через ФинЦЕРТ (подразделение ЦБ по кибербезопасности), который будет формировать единую базу о хищениях или попытках хищений денежных средств и доводить эту информацию до рынка.

Сейчас борьбу банков с дропперами затрудняет банковская тайна и невозможность отказать клиенту в обслуживании, отмечают участники рынка…

Однако в банках считают, что выбор подразделения ЦБ ФинЦЕРТ в качестве центра обмена информацией о дропперах не лучший вариант.

…Аккумулировать подобную информацию должна независимая от регулятора организация…

Кроме того, банкам нужны меры воздействия на дропперов в ситуации, когда нет материала для представления информации о них…» ***(Вероника Горячева. Помощников хакеров берут на карандаш. Банкам разрешат обмениваться информацией о дропперах // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3623829?query=%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). 10.05.2018).***

***

«Невідомі зламали сайт Росспівробітництва й залишили в ньому попередження для Роскомнагляду, написане англійською мовою.

Аноніми у своєму посланні відзначили, що «нещодавні руйнівні дії проти російського сегменту інтернету навели на думку про те, що ви [Роскомнагляд] всього лише купка некомпетентних безмозких черв'яків». Копія повідомлення залишилась доступною в інтернет-архіваторі Wayback Machine.

«Ви не повинні мати можливості продовжувати цей безглуздий вандалізм. Розглядайте це як наше останнє попередження», - також йдеться у ньому…

Таке ж повідомлення з'явилося й на піддомені, який раніше відповідав за стару версію сайту Росспівробітництва…» ***(Хакери зламали сайт Росспівробітництва й залишили в ньому послання для Роскомнагляду // MediaSapiens (http://ms.detector.media/web/cybersecurity/khakeri_zlamali_sayt_rosspivrobitnitstva_y_zalishili_v_nomu_poslannya_dlya_roskomnaglyadu/). 10.05.2018).***

***

«Холдинг НПО «Высокоточные комплексы», входящий в Ростех, представил линейку многоцелевых высокоточных токарных, токарно-фрезерных и фрезерных обрабатывающих центров с отечественной системой числового программного управления (ЧПУ) «Олимп». Разработки Ростеха позволят обеспечить кибербезопасность и технологическую независимость критически важных российских обрабатывающих производств…

В настоящий момент лидерами по производству систем ЧПУ, поставляемых в Россию, являются компании Siemens, Mitsubishi Electric, HAAS, Rexroth Bosch Group, Fagor Automation, FANUC, Fidia и другие…» ***(В России начинается производство киберзащищенных высокоточных станков // IKSMEDIA.RU (http://www.iksmedia.ru/news/5498869-V-Rossii-nachinaetsya-proizvodstvo.html#ixzz5FxsMwyAh). 16.05.2018).***

***

«Российский гигант кибербезопасности "Касперский", отчаявшись восстановить доверие после критики США о предполагаемых связях компании с российской разведкой, переводит некоторые из своих ключевых операций из Москвы в Цюрих, Швейцария, …чтобы его программное обеспечение доработала и проверила сторонняя организация.

"Касперский" также перемещает серверы, которые хранят и обрабатывают большую часть информации о безопасности, в Цюрих, включая данные клиентов США, Канады, Европы, Австралии, Японии, Южной Кореи и Сингапура…

Планируется переместить "линию сборки" Kaspersky к концу этого года, а часть обработки данных к концу 2019. Касперский также заявляет, что к 2020 году откроет центры прозрачности в Северной Америке и Азии.» ***(Из Москвы в Цюрих: "Касперский" переводит клиентские данные подальше от российского шпионажа // Goodnews.ua (http://goodnews.ua/technologies/iz-moskvy-v-cyurix-kasperskij-perevodit-klientskie-dannye-podalshe-ot-rossijskogo-shpionazha/. 16.05.2018).***

***

«Роскомнадзор ожидает ответа от представителей компании Apple по вопросу Telegram в течение месяца…

Ранее в Роскомнадзоре рассказали о том, что направили в Apple письмо с требованием удалить Telegram из магазина приложений AppStore. Кроме того, в ведомстве настаивают на блокировке push-уведомления сервиса Павла Дурова на территории России…

По данным исследования Mediascope, в апреле 2018 года в официальном приложении Telegram зафиксирован рекордный рост пользователей из России: среднее число юзеров в день составило более 3,7 миллиона человек…» ***(Apple дали месяц на блокировку Telegram // Lenta.ru (https://lenta.ru/news/2018/05/28/srok/). 28.05/2018).***

***

Інші країни

«…Правительство Канады запланировало широкие законодательные меры защиты парламентских выборов, предстоящих в 2019 году, от кибератак и "вмешательства из-за границы". Законопроект, внесенный кабинетом в понедельник, 30 апреля, предусматривает ограничение финансовых пожертвований, усиление защиты данных избирателей и ограничение срока предвыборной кампании до 50 дней…» ***(Канада готовит закон о защите от вмешательства в выборы // Українська служба швидких новин (https://sumynews.online/kanada-gotovit-zakon-o-zashhite-ot-vmeshatelstva-v-vybory-2/). 01.05.2018).***

***

Протидія зовнішній кібернетичній агресії

«Сенатор от Республиканской партии Джон Маккейн призвал власти США отомстить России за «вмешательство» в выборы американского президента в 2016 году с помощью кибератаки…

Сенатор отметил, что США должны подумать об ответе на тот способ атаки, который якобы использовала Россия, подразумевая кибератаку…». ***(Алексей Ласнов. У Маккейна возникла идея, как отомстить России за «вмешательство в выборы» // Деловая газета «Взгляд» (https://vz.ru/news/2018/5/3/920918.html). 03.05.2018).***

***

«…В Эстонии прошли международные учения Locked Shields («Сомкнутые щиты»). По сценарию учений, кибератака со стороны Кримзонии привела к тому, что Берилия лишилась мобильной связи и водоснабжения. Также

хакеры Кримзонии атаковали энергосистему Берилии, а на улицах Берилии протестующие развернули «подрывную деятельность»…

…Кримзония – это Россия, которая в 2007 году якобы совершила кибератаку против Эстонии в ответ на перенос Бронзового солдата…». ***(Антон Антонов. На учениях НАТО России дали вымышленное название // Деловая газета «Взгляд» (https://vz.ru/news/2018/5/6/921305.html). 06.05.2018).***

***

«Ровно 11 лет назад, 27 апреля 2007 года на Эстонию обрушилась волна кибератак, которые, по мнению правительства, поощрялись, спонсировались или даже организовывались Кремлем.

Тоомас Хендрик Ильвес, занимающий на то время пост президента Прибалтийского государства, назвал это «первой кибервойной»…

Министр иностранных дел Эстонии Свен Миксер в одном из недавних публичных выступлений заявил, … что Эстонии удалось достичь высоких успехов в борьбе с кибератаками после 2007 года…

Этот ряд нововведений позволил стране стать одним из лидеров в списке электронных государств: каждый гражданин имеет цифровой идентификатор личности, который можно использовать для различных операций: от покупок билетов в кино до участия в выборах.

Вместе с тем министр иностранных дел Эстонии не может гарантировать, что у их новой системе нет уязвимых мест, связанных с цифровой зависимостью…» ***(Эстония: угроза войны приводит нас в ужас // Avia. Pro (http://avia.pro/news/estoniya-ugroza-voyny-privodit-nas-v-uzhas). 02.05.2018).***

***

«На сервер Агентства цивільної авіації Міністерства економіки і стійкого розвитку Грузії здійснили кібератаку 2 травня…

«Для виправлення проблем в результаті нападу разом з агентством беруть участь усі відповідні відомства… Агентство цивільної авіації продовжує роботу в звичному режимі. Авіаційні підприємства та інші зацікавлені особи обслуговуються без затримок», – йдеться в заяві агентства.

За даними агентства, вірус пошкодив базу даних, програми та електронні адреси установи.» ***(Хакери «поклали» сервер агентства цивільної авіації Грузії // Інформаційне агентство «1NEWS» (https://1news.com.ua/svit/hakeri-poklali-server-agentstva-tsivilnoyi-aviatsiyi-gruziyi.html). 04.05.2018).***

***

«Британская компания по анализу данных Cambridge Analytica, которая незаконно получила доступ к данным более 87 миллионов пользователей Facebook, прекращает свою работу…

Фирму обвинили в ненадлежащем использовании данных пользователей соцсети от имени ее клиентов.

Социальная сеть Facebook отказалась комментировать закрытие Cambridge Analytica…» ***(Cambridge Analytica объявила о прекращении работы // «Факты и***

комментарии®» (http://fakty.ua/266944-cambridge-analytica-obyavila-o-prekracshenii-raboty). 02.05.2018).

***

«Великобритания, при помощи своих партнеров по международным организациям, намерена в 2018 году реализовать свой план по противодействию России…

Лондон прежде всего стремится усилить противодействие агрессивной российской политике, в частности - дезинформации и для этого создает негласный альянс. …Согласно сообщению, британские дипломаты планируют для усиления антироссийского альянса в мире использовать четыре крупных саммита - G7, G20, саммит НАТО и Европейского союза. Основное внимание будет уделено кибербезопасности, сдерживанию военной угрозы, санкциям и противодействию дезинформации…» ***(Британия создает альянс против России // АСН (http://asn.in.ua/ru/news/news/162227-britanija-sozdaet-aljans-protiv-rossii.html). 04.05.2018).***

***

«Рассекреченная часть доклада, подготовленного при участии ЦРУ, ФБР, а также АНБ, был обнародован Комитетом по разведке Сената США…

В документе говорится, что президент России Владимир Путин лично распорядился начать кампанию по воздействию на президентскую гонку в США в 2016 году… Кампания Кремля по вмешательству в американские выборы была разносторонней и скоординированной, проводилась с участием государственных СМИ и агентств, хакеров, проплаченных пользователей соцсетей, блогеров и спецслужб.

Связанные с российским правительством хакеры также осуществляли кибератаки на избиркомы. В частности, киберпреступники искали уязвимые места в базах данных и делали попытки взломов, иногда успешные. …Эти действия начались не позже начала 2016 года и продлились вплоть до дня голосования 8 ноября.» ***(Андрей Клименко. Путин лично распорядился начать кампанию: США обнародовали доклад о вмешательстве России // Replyua (https://replyua.net/putin/95842-putin-lichno-rasporyadilsya-nachat-kampaniyu-ssha-obnarodovali-doklad-o-vmeshatelstve-rossii.html). 09.05.2018).***

***

«Слідчі знайшли докази «зловмисного втручання» у роботу сайту місцевих виборів в Теннессі, що проводився з комп'ютера в Україні протягом спільного кібернападу, який, ймовірно, став причиною припинення роботи сайту…

Експерти з кібербезпеки залучені графством Нокс для аналізу кібернападу оголосили в п'ятницю, що користувачі з «підозріло великої кількості іноземних країн» були на сайті 1 травня.

Ця інтенсивна діяльність є серед ймовірних причин збою, наголошує компанія Sword & Shield Enterprise Security.

«З огляду на підозрілу діяльність і, особливо, доведене одночасне зловмисне втручання з IP адрес в Україні... вважаю, доцільно висунути гіпотезу, що це була умисна дія», – говорить заступник директора графства з інформаційних технологій.

…сайт не працював годину після закриття виборчих дільниць, що спричинило нерозуміння аж допоки техніки не виправили проблему…

У звіті стверджується, що сайт отримував запити на доступ з більш ніж 100 країн по всьому світу.» ***(У США підозрюють, що кібератаку на виборчий сайт здійснили з України // Західна інформаційна корпорація (https://zik.ua/news/2018/05/13/u_ssha_pidozryuyut_shcho_kiberataku_na_vyborchyy_sayt_zdiysnyly_z_ukrainy_1322991). 13.05.2018).***

***

«Влада Нідерландів вирішила відмовитися від використання «Антивірусу Касперського».

…відмовитися від цього програмного забезпечення рекомендується й приватним компаніям країни. Глава Мін'юсту Нідерландів Фердинанд Грапперхаус (Ferdinand Grapperhaus) направив до парламенту листа, в якому зазначив, що відмова від «Антивірусу Касперського» є запобіжним засобом…

В компанії «Лабораторія Касперського» заявили, що розчаровані таким рішенням Нідерландів…» ***(Влада Нідерландів відмовилася від «Антивірусу Касперського» // MediaSapiens (http://ms.detector.media/web/cybersecurity/vlada_niderlandiv_vidmovilasya_vid_antivirusu_kasperskogo/). 15.05.2018).***

***

«Канцлерка Німеччини Ангела Меркель (Angela Merkel) уважає, що її країні слід створити кібервійська через те, що гібридна війна є частиною воєнної доктрини Росії.

Про це вона сказала Бундестазі на дебатах щодо оборонного бюджету…

«Було б правильним створити кібервійська, оскільки гібридна війна є частиною воєнної доктрини Росії – абсолютно офіційно», – заявила канцлерка.

Ангела Меркель також підтримала необхідність підвищення військових витрат країни. Вона підкреслила, що це потрібно не заради озброєння, а задля закупівлі спорядження, що дасть змогу бійцям Бундесверу гідно виконувати завдання міжнародних місій, НАТО і національної оборони…» ***(Потрібно створити кібервійська, оскільки Росія офіційно веде гібридну війну – Меркель // MediaSapiens (http://ms.detector.media/web/cybersecurity/potribno_stvoriti_kiberviyska_oskilki_rosiya_ofitsiyno_vede_gibridnu_viynu_merkel/?media=print). 16.05.2018).***

***

«Власти Великобритании рекомендовали компаниям и госорганизациям усилить киберзащиту на случай возможных «хакерских атак России.

…такие меры британские власти приняли после инцидента с отравлением экс-полковника ГРУ Сергея Скрипаля и его дочери Юлии, в котором Лондон обвинил Россию…

В ходе встреч сотрудники национального центра кибербезопасности дали бизнесменам и госорганизациям рекомендации о том, какие меры по усилению защиты от хакерских атак.

…на данный момент британские спецслужбы не наблюдают никакой усиленной враждебной киберактивности со стороны России…» ***(Дмитрий Зубарев. Британия потребовала от компаний усилить киберзащиту от возможных атак России // Деловая газета «Взгляд» (https://vz.ru/news/2018/5/16/922929.html). 16.05.2018).***

***

«…Президент Відомства із захисту конституції (контррозвідки) ФРН Ханс-Георг Маасен заявив, що в останні роки число кібератак, у тому числі скоєних іноземними спецслужбами, збільшилося, тому Німеччина повинна бути здатна не допустити кібератаки на свої критичні інфраструктури і нанести противнику удар…

Це, за його словами, передбачає здатність простежити шлях вкраденої інформації та знищити її на сервері противника, здійснювати контршпионаж з метою з'ясування, що він хотів зробити з цією інформацією, а також, при відображенні кібератак з метою саботажу, завдати такої шкоди іншій стороні, щоб її спроби провалилися.

При цьому глава німецької контррозвідки не став говорити про можливої кібервійни. Гібридні загрози, за його визначенням, "стоять вище рівня дипломатичних зусиль, але нижче порога війни"…

Маасен уточнив, що Німеччина перебуває в центрі уваги служб зовнішньої розвідки, які можуть готувати акти саботажу шляхом впровадження шкідливих програм в об'єктах критичної інфраструктури…» ***(Німецька контррозвідка заявляє про збільшення кількості кібератак // «Дзеркало тижня. Україна» (https://dt.ua/WORLD/nimecka-kontrrozvidka-zayavlyaye-pro-zbilshennya-kilkosti-kiberatak-277712_.html). 14.05.2018).***

***

«Федеральные ведомства США "пока не в состоянии выполнять закон, который предписывает в срок до октября нынешнего года запретить использование ПО "Лаборатории Касперского" в компьютерных сетях правительства США"…

"Множество подразделений правительства США столкнулось с тем фактом, что программный код, написанный московской фирмой кибербезопасности, встроен в глубинные части американской инфраструктуры - в роутеры, файрволы и другое аппаратное обеспечение - и никто точно не знает, как от него избавиться", - утверждают журналисты Эндрю Десидерио и Кевин Паулсен.

"Это грязная работа, она займет намного больше года, - сказал неназванный американский чиновник. - Конгресс никому не дал денег на замену этих устройств, а в бюджете изначально не было простора для маневра"…

Пять источников в Конгрессе, которым поручен надзор за тем, как правительство выполняет раздел 1634, сообщили, что в последние недели их обеспокоило, что Министерство внутренней безопасности не забило тревогу по поводу известных проблем с аппаратным обеспечением, которые не позволяют министерству полностью выполнить положение закона NDAA; это заставляет многих усомниться, сможет ли правительство сделать все к 1 октября - крайнему сроку…» ***(Эндрю Десидерио и Кевин Паулсен. Правительство США не может удалить из своих компьютерных сетей спорное программное обеспечение "Лаборатории Касперского" // Украинское рейтинговое агентство "УРА" (http://ura-inform.com/ru/interesno/2018/05/24/pravitelstvo-ssha-ne-mozhet-udalit-iz-svoikh-kompjuternykh-setej-spornoe). 24.05.2018).***

***

«… Суд Сан-Франциско засудив його до п'яти років позбавлення волі 23-річного громадянина Канади і Казахстану Каріма Баратова… Окрім того, він також буде зобов’язаний заплатити штраф у розмірі 250 тисяч доларів.

Слідство дійшло висновку, що хакер був причетний до зламу Yahoo через російські спецслужби й що він опосередковано став частиною більш масштабної операції зі збору інформації. Каріма Баратова вважають причетним до зламів 11 тисяч акаунтів з 2010 по 2017 рік, й з них 80 тисяч пов'язані з кібератакою на Yahoo…». ***(Хакера засудили до 5 років ув’язнення за злам акаунтів Yahoo // MediaSapiens(http://ms.detector.media/web/cybersecurity/khakera_zasudili_do_5_rokiv_uvyaznennya_za_zlam_akauntiv_yahoo/). 30.05.2018).***

***

«…в документі, в якому аналізуються кіберзагрози, виявлені протягом 2017 року, Національний криптологічний центр Іспанії (CCN), підлеглий Національному центру розвідки, використовує примітку, в якій передбачається втручання Москви, хоча без надання даних.

“Присутність активістів, що були фінансовані російськими установами, схоже, було продемонстровано у медійному висвітленні конфлікту унаслідок ситуації, що виникла в Каталонії протягом 2017 року через ухилення від конституційної законності певних каталонських автономних установ”, — йдеться в доповіді…» ***(Саша Картер. Іспанська розвідка звинуватила Росію у втручанні в фінансуванні сепаратистів Каталонії // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1732124-ispanska-rozvidka-zvinuvatila-rosiyu-u-vtruchanni-v-finansuvanni-separatistiv-kataloniyi). 22.05.2018).***

***

«Китай та Росія намагалися втрутитися у роботу критичної інфраструктури Канади…

Про це йдеться у документах Міністерства громадської безпеки Канади. «Кібератаки зі стратегічною метою – більш витончені та заточені на отримання доступу й контролю над ключовими активами. Наприклад, Росія та Китай скомпрометували важливі кібернетичні системи канадської критичної інфраструктури, наразивши канадців на небезпеку», – зазначається у довідці, підготовленій в 2016 році для державного секретаря міністерства громадської безпеки Канади Монік Борегард…» ***(Росія намагалася здійснити кібератаку на сервери критичної інфраструктури Канади // Інформаційне агентство «1NEWS» (https://1news.com.ua/svit/rosiya-namagalasya-zdiysniti-kiberataku-na-serveri-kritichnoyi-infrastrukturi-kanadi.html). 09.05.2018).***

***

Захист персональних даних

«Facebook использовал свое приложение для сбора информации о пользователях и их друзьях, в том числе о тех, кто не подписан на социальную сеть, читая их текстовые сообщения, отслеживая местоположения и получая фотографии…

Претензии по поводу массового наблюдения являются частью иска против Facebook, возбужденного Six4Three…

Разработчик подает в суд на Facebook за свое приложение Pikinis. Так, Facebook завлекала разработчиков и инвесторов на платформу, преднамеренно вводя их в заблуждение относительно элементов управления данными и настроек конфиденциальности. Таким образом компания следила за пользователями без их согласия.

На телефонах Android компания смогла собирать метаданные и контент из текстовых сообщений. На iPhone Facebook мог получить доступ к большинству фотографий, в том числе к тем, которые не были загружены в социальную сеть…» ***(Ирина Фоменко. Facebook следит за пользователями через свое приложение // Internetua (http://internetua.com/facebook-sledit-za-polzovatelyami-cserez-svoe-prilojenie). 25.05.2018).***

***

«…Американский союз защиты гражданских свобод (ACLU) и 40 других групп во вторник потребовали, чтобы Amazon запретил правоохранительным органам США использовать инструмент Rekognition, который, по словам компании, может определить "все лица на групповых фотографиях и в общественных местах"…

"С Rekognition правительство теперь может создать систему для автоматизации идентификации и отслеживания всех людей", - убеждены в ACLU…

В свою очередь, Amazon защищает свои технологии. "Наше качество жизни значительно ухудшится, если мы объявим вне закона новую технологию только потому, что некоторые люди могут злоупотреблять ею…", - сообщают в компании…». ***(Ирина Фоменко. Amazon и Google втихаря сотрудничают с полицией и военными // Internetua (http://internetua.com/amazon-i-google-vtiharya-sotrudnicsauat-s-policiei-i-voennmi). 24.05.2018).***

***

«Австралийский Commonwealth Bank (CBA), являющийся самым крупным в стране, допустил утечку данных 19,8 миллиона счетов своих клиентов.

…При этом сам инцидент произошел еще в мае 2016 года. В ходе демонтажа одного из устаревших дата-центров CBA компания-подрядчик Fuji Xerox утеряла два носителя со стримеров – накопителей данных на магнитных лентах…

Информация на исчезнувших носителях затрагивает 19,8 миллиона счетов в CBA, открытых 12 миллионами австралийцев – что составляет половину всего населения страны. Данные включают имена клиентов, адреса их проживания, номера счетов и информацию об истории транзакций за 16 лет – с 2000 по 2016 год. Представители CBA подчеркивают, что еще два года назад уведомили о произошедшем офис комиссара по вопросам защиты конфиденциальности граждан при правительстве Австралии. Но в результате было принято решение не уведомлять клиентов банка о произошедшем. Банк также заверяет, что с момента утечки осуществляет тщательный мониторинг всех затронутых инцидентом счетов, и за прошедшие два года не было обнаружено никаких свидетельств подозрительной активности.» ***(Австралийский банк потерял данные половины жителей страны // IKSMEDIA.RU (http://www.iksmedia.ru/news/5496646-Avstralijskij-bank-poteryal-dannye.html#ixzz5FxyMjQMH). 04.05.2018).***

***

Топ мировых утечек за апрель

«*…Данные пассажиров аэропорта Индии использовали для нелегальной торговли алкоголем*

Инцидент раскрыли во время расследования о неуплате пошлин агентством, которое управляет магазинами duty-free в аэропорту Тируванантапурам в штате Керала на юге Индии. Эпизод стал крупным делом об утечке данных пассажиров международных рейсов.

По словам таможенного комиссара, кроме неуплаты таможенной пошлины следствие выявило злоупотребление иммиграционными данными, подделку документов и нарушение мер национальной безопасности. Для продажи иностранного алкоголя на чёрном рынке агентство использовало паспортные данные 13 000 пассажиров, путешествовавших с сентября по декабрь 2017 года…

Художник купил персональные данные 346 тысяч жителей Китая для музейной экспозиции

32-летний художник из Пекина Денг Юфенг хотел создать произведение искусства, которое заставило бы зрителей задуматься о конфиденциальности личной информации. Чтобы реализовать художественный замысел, автор купил в интернете персональные данные и превратил их в экспозицию под названием «Секреты 346 тысяч жителей Уханя»…

Денг Юфенг скупал пользовательские данные, используя китайский мессенджер QQ. Всего за 800 долларов – или $0,001 за человека – он получил имена, номера телефонов, данные об онлайн-покупках, маршруты путешествий и автомобильные регистрационные знаки.

Шведская академия признала факт утечки имен лауреатов Нобелевской премии по литературе

…Имена обладателей Нобелевской премии по литературе разглашались до официального объявления минимум семь раз, начиная с 1996 года. Помимо имен победителей до официального объявления дважды были раскрыты имена новых академиков.

Первой о многократных утечках данных в академии сообщила шведская газета Dagens Nyheter. В распоряжении редакции оказались материалы внутреннего расследования. В документах речь шла о том, что информацию незаконно распространял «деятель культуры, близкий к академии»…

Данные клиентов Panera Bread больше полугода находились в открытом доступе

Американская сеть кафе-пекарен Panera Bread допустила утечку персональных данных своих клиентов. Файл с информацией о 37 миллионах покупателей лежал на сайте компании в открытом доступе на протяжении 8 месяцев.

…среди раскрытых данных были имена, домашние адреса, электронная почта, даты рождения и последние цифры из номеров банковских карт пользователей, которые размещали заказы онлайн…

Сотовый оператор Таиланда TrueMove H хранил 46 000 файлов в открытом облаке

…В папках, названных по годам, размером 14,5 Гб, 8,3 Гб и 2,2 Гб, хранились документы в форматах PDF и JPG. Среди них – отсканированные копии паспортов, водительских удостоверений и национальных идентификационных карт клиентов компании…

С того момента, как компания TrueMove H узнала о неверной конфигурации облачного хранилища AWS, до момента закрытия доступа к нему прошёл месяц. Проблему устранили 12 апреля 2018 года…» ***(Топ мировых утечек за апрель // IKSMEDIA.RU (http://www.iksmedia.ru/news/5496365-Globalnyj-IBdajdzhest-itogi-aprelya.html#ixzz5FxyreWte). 03.05.2018).***

***

«Интернет-мошенники в Западной Африке представлялись принцами и американскими солдатами для взлома корпоративной почты, что стоило предприятиям сотни миллионов долларов в год…

Согласно отчету компании по кибербезопасности CrowdStrike, мошенники получали доступ к реквизитам для входа в корпоративную электронную почту или использовали практически идентичные адреса как реальные – этот вид преступности получил название «Компромисс деловой электронной почты» (BEC)…

Нигерия стала одним из центров BEC. Местные интернет-мошенники, известные как «парни Yahoo», выдавали себя за нуждающихся в финансовой помощи или нигерийских принцев, предлагая доход от инвестиций.

Шантажистов называют «419 мошенников» из-за раздела национального уголовного кодекса, который был неэффективным в этой области.

Парни Yahoo даже выдали себя за командующего войсками США в Афганистане, чтобы обмануть обратившихся за помощью в восстановлении имущества погибших солдат. Это заставило командующего сделать заявление в Facebook, что он никогда не пытался связаться с кем-либо с просьбой о финансовой помощи …» ***(Ирина Фоменко. Нигерийские письма по-прежнему доят лохов // Internetua (http://internetua.com/nigeriiskie-pisma-po-prejnemu-doyat-lohov). 05.05.2018).***

***

«Специалисты по кибербезопасности из компании Sophos выявили новый способ мошенничества с помощью Google карт.

…жертва получает сообщение от «друга» со ссылкой на Google Maps, однако при переходе по ней пользователя перенаправляют на страницу с рекламой, имеющую российский домен.

…мошенники используют сервис goo.gl, помогающий сокращать длинные URL-адреса. При переходе по ссылке, стилизованной под URL Google Maps, пользователя переводят на вредоносный сайт с англоязычной рекламой средства для похудения.» ***(Очередная угроза: в Google картах обнаружили опасные ссылки // «Я и Закон» (https://yaizakon.com.ua/ocherednaya-ugroza-v-google-kartah-obnaruzhili-opasnye-ssylki/). 03.05.2018).***

***

«Серверы Агентства гражданской авиации Грузии 2 мая подверглись кибератаке, в результате чего компьютерный вирус повредил его базы данных, программы и электронные адреса.

Грузинские авиавласти устраняют последствия кибератаки на свои серверы…

Агентство гражданской авиации продолжает работать в обычном режиме, обслуживание авиационных предприятий и других заинтересованных лиц осуществляется без сбоев…» ***(Грузинские авиавласти устраняют последствия***

кибератаки на свои серверы // Черноморские новости (http://www.blackseanews.net/read/141093). 04.05.2018).

***

«…По данным исследования, опубликованного компанией Positive Technologies, уязвимые онлайн-ресурсы позволяли злоумышленникам оказывать влияние на дипломатические отношения, получать доступ к списку пациентов клиник пластической хирургии, похищать огромные суммы у криптовалютных бирж и осуществлять другие атаки.

Сайты государственных организаций в 2017 году вызывали устойчивый интерес нарушителей — в среднем ежедневно отмечалось 849 атак на каждую компанию. В феврале прошлого года злоумышленники успешно внедряли на веб-порталы посольств и иных ведомств по всему миру скрипт, заражающий устройства посетителей шпионским ПО, а позже с этой же целью был взломан сайт Национального совета США по внешней торговле.

…Традиционно мишенью хакеров становятся и веб-ресурсы, связанные с проведением президентских и парламентских выборов. Под угрозой находятся также веб-приложения, имеющие отношение к финальной части ЧМ-2018…

На 2017 год пришелся рост популярности криптовалют и ICO…, который немедленно привлек внимание хакеров. Большинство атак на криптовалютные биржи и площадки для проведения ICO были связаны с недостаточной защитой веб-приложений, например, взломы проектов CoinDash и Enigma Project, в рамках которых преступники подменили на сайтах ICO адреса криптовалютных кошельков.

В отчете приводится статистика и по сайтам сферы здравоохранения, на которые в среднем ежедневно совершалась 731 атака. Один из инцидентов в этой сфере произошел в литовской клинике пластической хирургии, когда хакеры опубликовали более 25 000 интимных фото пациентов до и после операций. Предварительно хакеры требовали за удаление данных выкуп в размере 344 000 евро у самой клиники и до 2000 евро — у отдельных пациентов.

В образовательной сфере атакующими, как отмечают авторы документа, являются чаще всего сами учащиеся, стремящиеся улучшить таким способом свою успеваемость… В сфере образования было выявлено в среднем по 106 атак на одну организацию.

В области энергетики и промышленности эксперты Positive Technologies зафиксировали сравнительно малое количество атак на веб-приложения (9 атак в день на одну компанию), тем не менее эти атаки представляют особую опасность, поскольку их характер говорит о высокой квалификации преступников и тщательно спланированных действиях. Целью преступников в таких случаях, как правило, является доступ не только в корпоративную сеть, но и в технологический сегмент.

Наиболее интенсивно в минувшем году атаковали веб-приложения IT-компаний и финансовых организаций (банков и электронных торговых площадок) — 1014 и 983 атак в день соответственно...» ***(Эксперты Positive Technologies***

прогнозируют волну атак на сайты, связанные с ЧМ-2018 // Positive Technologies (https://www.ptsecurity.com/ru-ru/about/news/292275/). 03.05.2018).

***

«ESET предупреждает о фишинговой атаке на пользователей сервиса аренды жилья в путешествиях Airbnb. Кампания нацелена на кражу банковских данных владельцев недвижимости.

Атака начинается с фишинговой рассылки…

В письме сообщается, что Airbnb обновляет политику конфиденциальности в связи с внедрением нового Общего регламента по защите данных (GDPR — General Data Protection Regulation). Чтобы и дальше пользоваться всеми функциями сервиса, владельцу жилья предлагается «обязательно» принять новые условия, перейдя по ссылке в письме.

Ссылка вела на фишинговую страницу, где …помимо прочих сведений, владельцу жилья нужно ввести данные банковской карты и аккаунта на Airbnb…» ***(Пользователи Airbnb под угрозой // IKSMEDIA.RU (http://www.iksmedia.ru/news/5499446-Polzovateli-Airbnb-pod-ugorozoj.html#ixzz5FxpELKD0). 18.05.2018).***

***

«Неизвестные киберпреступники успешно атаковали банковскую систему Мексики. Они сфабриковали сотни запросов на электронный трансфер средств на подставные счета. …В результате со счетов как минимум 5 мексиканских банков было похищено не менее 300 миллионов песо (около 15,4 миллиона долларов)…

Предполагается, что хакеры смогли проэксплуатировать уязвимость в программном обеспечении для соединения внутренних платежных систем, разработанном некой «третьей стороной». …многие эксперты полагают, что успех столь масштабной атаки был бы едва ли возможен без помощи инсайдеров внутри самих банков. Власти страны ведут полномасштабное расследование инцидента.» ***(Уязвимость ПО обошлась мексиканским банкам в сотни миллионов песо // IKSMEDIA.RU (http://www.iksmedia.ru/news/5499078-Uyazvimost-PO-oboshlas-meksikanskim.html#ixzz5Fxs4YMre). 17.05.2018).***

***

«Американское бюро кредитных историй Equifax раскрыло точные масштабы кражи данных, имевшей место летом 2017 г. Бюро подтвердило, что злоумышленники смогли получить имена, фамилии и даты рождения 146,6 млн резидентов США.

Помимо этого, были украдены 145,5 млн номеров социального страхования (SSN), 99 млн адресов, 20,3 млн телефонных номеров, 17,6 млн номеров водительских удостоверений и 1,8 млн адресов электронной почты. Кроме того, были похищены данные по 209 тыс. платежных карт, включая номер и дату окончания действия, а также 97,5 тыс. номеров налогоплательщика TaxID.

Также злоумышленники получили сканы или фотокопии 38 тыс. водительских удостоверений, 12 тыс. карт социального страхования или налогоплательщика и 3,2 тыс. паспортов. Эти изображения были загружены пользователями на портал Equifax…

О масштабной краже данных Equifax сообщила в сентябре 2017 г. — через 1,5 месяца после того, как узнала сама…

В ходе атаки хакеры использовали уязвимость веб-сайта компании…» ***(Хакеры украли банковские идентификаторы половины населения США // IKSMEDIA.RU (http://www.iksmedia.ru/news/5497321-Xakery-ukrali-bankovskie-identifika.html#ixzz5FxwRocZP). 10.05.2018).***

***

«В Японии бурно обсуждаются набирающие силу атаки на камеры видеонаблюдения Canon. …в минувшее воскресенье …было зафиксировано более 60 случаев взлома камер наблюдения по всей стране.

Хакеры не только не скрывают своих действий, но еще и уведомляют о них: на мониторах, куда передается сигнал с взломанных камер, появляется сообщение «I'm Hacked. bye2».

Кто стоит за атакой, и какие цели она может преследовать, в настоящий момент неизвестно. Выбор жертв также весьма широк: от общественных зданий и правительственных учреждений до водопровода, рыбного рынка и штаб-квартиры частной компании… Киберпреступники атакуют камеры, пользователи которых не позаботились изменить предустановленный производителем пароль. Это, в частности, подтвердили представители городских властей городов Агео и Ятие, где были зафиксированы одни из первых атак. Компания Canon выпустила специальное заявление, в котором напомнила пользователям о необходимости менять предустановленные пароли…» ***(Хакеры атакуют камеры наблюдения Canon по всей Японии // IKSMEDIA.RU (http://www.iksmedia.ru/news/5497215-Xakery-atakuyut-kamery-nablyudeniya.html#ixzz5FxxZZAMO). 08.05.2018).***

***

«Специалисты ESET предупреждают о новой фишинговой атаке. Злоумышленники подделали сайт Netflix и собирают с его помощью данные банковских карт пользователей.

Потенциальная жертва получает по электронной почте фишинговое сообщение о завершении срока действия подписки на Netflix. …Для «активации подписки» предусмотрена красная кнопка в письме.

…Кнопка «активации» ведет на поддельный сайт Netflix, дизайн которого копирует настоящий…

На поддельном сайте пользователю предлагается ввести email и пароль от личного кабинета Netflix, а затем заполнить анкету, включающую информацию о банковской карте. После этого пользователь будет перенаправлен на настоящий сайт Netflix, а его данные поступят в распоряжение мошенников… ***(Поддельный сайт Netflix собирает данные банковских карт // IKSMEDIA.RU***

(http://www.iksmedia.ru/news/5496705-Poddelnyj-sajt-Netflix-sobiraet-dan.html#ixzz5Fxy1j2oX). 04.05.2018).

***

«…Этой весной жулики …обещают доверчивым пользователям выплатить компенсации от энергетических компаний и медицинских учреждений.

Схема мошенничества в целом осталась прежней: злоумышленники рассылают по электронной почте спам, предлагая потенциальным жертвам перейти по ссылке на специально созданный ими сайт…

Специалисты компании "Доктор Веб" выявили более 110 доменов, зарегистрированных сетевыми мошенниками в период с февраля по май 2018 года. При этом многие домены со схожими по звучанию и написанию ключевыми словами регистрировались одновременно целыми группами и были привязаны к одним и тем же хостинговым площадкам…

При переходе по ссылке потенциальная жертва перенаправляется на мошеннический или фишинговый сайт, собирающий конфиденциальную информацию посетителей…» ***("Доктор Веб": мошенники крадут деньги обращающихся за социальными компенсациями // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=122924). 10.05.2018).***

***

«Компании по всему миру из-за действий киберпреступников в прошлом году потеряли около 1 трлн долларов.

Такие данные содержатся в отчете международного страхового концерна Allianz…

Страховщики опасаются, что уровень потерь от киберпреступлений к 2019 году может достичь 2 трлн. долларов.

По всему миру компании собирают и хранят огромные базы реальных и потенциальных клиентов. Когда большие данные попадают к хакерам, это наносит серьезный ущерб репутации компании и нарушает ее работу.

…к 2020 году рынок больших данных вырастет до $61 млрд, в 2026 году — до $85 млрд…

Ни законодательство, ни правоохранительные органы во всем мире не могут угнаться за скоростью разрабатываемых кибермошенниками технологий. Тем временем бизнес пытается защитить себя от кибератак самостоятельно, тратя около $122,5 млрд в год на защиту информационных систем. При этом страховая защита пока используется недостаточно широко. Согласно результатам исследования, страховка компенсирует потери от кражи данных и помогает справиться с последствиями хакерской атаки, что является менее затратным способом киберзащиты.» ***(Страховщики оценили мировой ущерб от кибератак в 2017 году // Закон и Бизнес (http://zib.com.ua/ru/print/132924-strahovschiki_ocenili_mirovoy_uscherb_ot_kiberatak_v_2017_go.html). 14.05.2018).***

***

«Компания Check Point® Software Technologies в отчёте Global Threat Impact Index за апрель отмечает, что …четвертый месяц подряд вредоносные криптомайнеры доминируют в топ-10 отчета Check Point Global Threat Index, причем Coinhive сохраняет первое место как наиболее распространенное вредоносное ПО с глобальным охватом 16%. Еще один криптомайнер Cryptoloot расположился сразу за лидером (14%), на третьем месте (11%) – вредоносное рекламное ПО Roughted.

Исследователи Check Point также отметили, что с начала года кибермошенники все чаще используют незакрытые уязвимости серверов приложений в целях незаконной добычи криптовалюты. Так, атаки на 46% организаций по всему миру эксплуатировали уязвимость в Microsoft Windows Server 2003 (CVE-2017-7269), а на 40% – уязвимость Oracle WebLogic (CVE-2017-10271)…» ***(Check Point: число атак криптомайнеров с помощью уязвимостей серверов растет // «Компьютерное Обозрение» (http://ko.com.ua/check_point_chislo_atak_kriptomajnerov_s_pomoshhyu_uyazvimostej_serverov_rastet_124704). 28.05.2018).***

***

«Создатель сайта BleepingComputer Лоренс Абрамс (Lawrence Abrams) обнаружил в своем электронном ящике фишинговое письмо, в котором содержалась информация о том, что его составители — мошенники. Так вымогатели хотели обелить свое имя…

…В тексте, якобы присланном из Департамента казначейства США, мошенники сообщают о сумме в 6,5 миллиона долларов, которые жертва может перевести на свой банковский счет.

В одном из разделов письма содержался список имен, с которыми адресату не следует контактировать, — они названы мошенниками. Перечень из нескольких имен приведен в качестве «доказательства» чистоты намерений преступников…» ***(Мошенники в сети прикинулись приличным банком и просчитались // Goodnews.ua (http://goodnews.ua/technologies/moshenniki-v-seti-prikinulis-prilichnym-bankom-i-proschitalis/). 24.05.2018).***

***

«Согласно Anti-Phishing Working Group (APWG), злоумышленники похитили около $1.2 млрд в криптоваютах с начала 2017 года, сообщает Reuters…

При этом, лишь 20% от украденных средств было восстановлено. Согласно отчету, Общий регламент ЕС по защите данных (GDPR), вступающий в силу сегодня, только помешает ходу полицейских расследований преступной деятельности…» ***(Похищено $1.2 млрд в криптовалютах //BIGFIN (https://bigfin.net/25/05/2018/pohishheno-1-2-mlrd-v-kriptovaljutah/). 25.05.2018).***

***

«Криптовалюта Verge (XVG) второй раз за последние два месяца подверглась хакерской атаке. Злоумышленники проэксплуатировали уязвимости в блокчейне Verge и похитили около 35 млн монет XVG на сумму $1,7 млн.

В апреле текущего года сеть Verge подверглась такой же кибератаке, в ходе которой злоумышленникам удалось похитить 250 тыс. монет XVG. И первая, и вторая атаки были обнаружены пользователем ресурса Bitcointalk.org под псевдонимом ocminer. По его словам, оба раза киберпреступники проэксплуатировали одну и ту же уязвимость в блокчейне. Как отметил пользователь Reddit под псевдонимом R_Sholes, уязвимость осталась в блокчейне даже после хардфорка Verge, осуществленного в ответ на первую атаку.

Разработчики Verge недооценивают серьезность инцидента, заявляя , что некоторые пулы для майнинга Verge просто стали жертвами DDoS-атак…» ***(Неизвестные похитили $1,7 млн в криптовалюте Verge // Goodnews.ua (http://goodnews.ua/technologies/neizvestnye-poxitili-17-mln-v-kriptovalyute-verge/). 23.05.2018).***

***

«…неизвестные совершили кибератаку на отдел представительного органа служащих и чиновников [Федерального ведомства по делам миграции и беженцев]. В пятницу неизвестные пытались попасть в систему компьютера главы отдела представительного органа Ангелики Венцль на ее рабочем месте. Представители ведомства подтвердили эту информацию. Попытка несанкционированного доступа была обнаружена представителями IT-отдела. По факту случившегося сразу было возбуждено уголовное дело…» ***(Виктория Холоденина. Хакеры пытались взломать систему BAMF // GERMANIA.one (https://germania.one/hakery-pytalis-vzlomat-sistemu-bamf/). 28.05.2018).***

***

Діяльність хакерів та хакерські угруповування

«Російські хакери з груп Fancy Bear, яких звинувачують у втручанні у вибори президента США у 2018 році, погрожували дружинам американських військових від імені терористів «Ісламської держави». Про це йдеться у розслідуванні Associated Press.

«10 лютого 2015 року 5 дружин військовослужбовців армії США отримали у соцмережах повідомлення з таким текстом: Ми знаємо все про тебе, твого чоловіка і твоїх дітей. Ми набагато ближче, ніж ти можеш собі уявити», — зазначають у виданні.

Як повідомляють журналісти, відправник називав себе хакером групи CyberCaliphate, який діє в інтересах «Ісламської держави».

За даними розслідування, хакери намагалися зламати електронні поштові скриньки дружин американських військових саме тоді, коли CyberCaliphate надсилав свої погрози…» ***(Російські хакери лякали ІДІЛом дружин американських військових // "Українські медійні системи"***

(https://glavcom.ua/world/observe/rosiyski-hakeri-lyakali-idilom-druzhin-amerikanskih-viyskovih-495968.html). 09.05.2018).

***

«…команда исследователей кибербезопасности 401TRG из компании ProtectWise …проанализировали тактику, методы и процедуры, используемые на протяжении многих лет хакерской группировкой Winnti, также известной под названиями Axiom и APT 17.

Как заявили исследователи, множество подозреваемых в кибершпионаже в пользу китайских разведслужб хакерских группировок, таких как BARIUM, Wicked Panda, GREF и PassCV, со временем начали использовать методы и инфраструктуру Winnti. На основе этих наблюдений исследователи объединили их под общим названием Winnti Umbrella…

В настоящее время часть группировок из Winnti Umbrella действует по одной и той же схемой. В первую очередь, злоумышленники предпочитают осуществлять фишинговые атаки на отдельные цели для хищения учетных данных, которые позволяют злоумышленникам проникнуть в систему с помощью чужой учетной записи, а не вредоносного ПО. Затем атакующие используют технику под названием «living off the land», представляющую собой использование локальных приложений во вредоносных целях. Использующиеся в данных атаках инструменты включают стандартные утилиты Windows, а также программы для тестирования на проникновение, такие как Metasploit и Cobalt Strike. При этом вредоносные программы используются только в случае реальной необходимости, поскольку злоумышленники опасаются обнаружения.

В 2018 году тактика претерпела небольшие изменения и атакующие сосредоточили свои усилия прежде всего на взломе учетных записей Gmail и Office 365…» ***(Стали известны подробности деятельности китайской хакерской группировки Winnti // Goodnews.ua (http://goodnews.ua/technologies/stali-izvestny-podrobnosti-deyatelnosti-kitajskoj-xakerskoj-gruppirovki-winnti/). 08.05.2018).***

***

«Неизвестные хакеры внедрили программное обеспечение для майнинга криптовалюты Monero в сотни веб-сайтов, использующих систему управления контентом Drupal. При этом многие пострадавшие страницы принадлежат различным государственным учреждениям…

Отмечается, что были скомпрометированы почти 400 сайтов — неизвестные установили на них браузерное майнинг-ПО Coinhive, которое добывает криптовалюто Monero с помощью уязвимостей в старых версиях Drupal…

При этом посетители страниц могут даже не догадываться, что их компьютеры и устройства используются для майнинга Monero…» ***(Хакеры установили криптомайнеры на сотни муниципальных веб-сайтов // Goodnews.ua (http://goodnews.ua/technologies/xakery-ustanovili-kriptomajnery-na-sotni-municipalnyx-veb-sajtov/). 09.05.2018).***

***

«Злоумышленники начали кибератаку на маршрутизаторы компании Dasan, в которых недавно обнаружили несколько критических уязвимостей...

По данным экспертов безопасности из компании Netlab 360, хакеры запустили ботнет, который сканирует и пытается использовать уязвимые устройства. Ботнет управляется с сервера, расположенного во Вьетнаме...

В конце апреля анонимные исследователи опубликовали материал, в котором рассказали о наличии двух «дыр» в системе безопасности роутеров Dasan, оборудованных технологией GPON. Обнаруженная уязвимость затрагивала более миллиона устройств южнокорейской компании.

По словам аналитиков, бреши позволяют хакерам обойти аутентификацию: это значит, что любой злоумышленник сможет получить доступ к внутренним настройкам маршрутизатора, выполнив несколько простых действий. Исследователи отметили, что большинство из уязвимых устройств расположены в Мексике, Казахстане и Вьетнаме.» ***(Миллион роутеров подверглись масштабной атаке по всему миру // Goodnews.ua (http://goodnews.ua/technologies/million-routerov-podverglis-masshtabnoj-atake-po-vsemu-miru/). 04.05.2018).***

***

«Хакер взломал серверы компании Securus, оказывающей услуги, позволяющие правоохранительным органам США с легкость отслеживать практически каждый телефон в любой точке страны….

Взломавший Securus хакер предоставил журналистам издания Motherboard несколько внутренних файлов компании. В частности, в руки сотрудников Motherboard попал фрагмент базы данных, озаглавленный "Полиция". Документ включает более 2,8 тыс. имен пользователей, адресов электронной почты, номеров телефонов, хешей паролей и проверочных вопросов пользователей Securus. Таблица охватывает период с 2011 года по 2018 год…» ***(Собирающая данные о местоположении американцев компания стала жертвой взлома // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123062). 17.05.2018).***

***

«В начале текущего месяца эксперты "Лаборатории Касперского" опубликовали исследование, посвященное кибершпионской операции ZooPark…

По данным "Лаборатории Касперского", операция ZooPark продолжается, по крайней мере, с июня 2015 года и сфокусирована на странах Среднего Востока. Кибершпионы заражают Android-устройства с помощью вредоносного ПО разных поколений…

Судя по всему, операция осуществляется в интересах некоего государства. Тем не менее, анонимному хакеру удалось похитить у кибершпионов кеш данных, собранных у их жертв на Среднем Востоке. …по словам анонимного хакера, за операцией стоит правительство Ирана…» ***(Анонимный хакер передал журналистам данные, собранные APT-группой в ходе операции ZooPark // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=122949). 11.05.2018).***

***

«Сеть криптовалюты Bitcoin Gold подверглась двойной результативной кибератаке. Хакер вывел 18,6 миллионов долларов. Директор по коммуникациям Эдвард Искра признал факт атаки и объяснил, что атаку провел майнер. Он приобрел более 51% общей хеш-мощности сети, получив контроль над блокчейном на некоторое время, которого ему хватило, чтобы провести ряд эффективных действий.

…Нет никаких препятствий к тому, чтобы хакер атаковал сеть еще раз, если он еще раз сможет обрести необходимую мощность, предупреждает Bitcoin Gold…» ***(Evgenij Novožilov. Атака 51% на сеть Bitcoin Gold привела к потере 18,6 млн долларов // BIGFIN (https://bigfin.net/24/05/2018/ataka-51-na-set-bitcoin-gold-privela-k-potere-18-6-mln-dollarov/). 24.05.2018).***

***

«…В январе 2018 года ESET опубликовала первый отчет о новой киберкампании Turla. Хакеры распространяли Mosquito, бэкдор собственной разработки, с помощью поддельного установщика Adobe Flash Player. Потенциальные жертвы группы – сотрудники консульств и посольств стран Восточной Европы.

…С марта 2018 года хакеры Turla …используют …платформу с открытым исходным кодом Metasploit. Метод не является новаторским, однако это существенный сдвиг в тактике, технике и процедурах (TTP) кибергруппы.

…Продолжительность такой атаки составляет порядка тридцати минут.» ***(Хакеры Turla меняют тактику // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5502374-Xakery-Turla-menyayut-taktiku.html#ixzz5HAN5JYed). 30.05.2018).***

***

Вірусне та інше шкідливе програмне забезпечення

«…ФинЦЕРТ (подразделение ЦБ по кибербезопасности) в рамках информационного обмена уведомил банки о новой угрозе… - фишинговой рассылке вредоносного программного обеспечения (ВПО) с трояном intel security.exe. Эксперты уверены, что данный вредонос принадлежит преступной группировке Silence («Тишина»), которая в 2017 году атаковала банки в России, Армении и Малайзии. «Специфика данного вредоносного вложения более чем сходна с теми, что использует Silence»,— отметил руководитель экспертного центра безопасности Positive Technologies Алексей Новиков…

В Банке России подтвердили факт сообщения о вредоносе. «Использование ВПО этого типа наблюдается с весны 2017 года, ФинЦЕРТ фиксировал случаи его распространения еще до того, как оно было классифицировано как Silence,— отметили в ЦБ…» ***(Вероника Горячева. Банки атакуют в тишине. Забытая киберугроза вернулась на рынок // АО «Коммерсантъ» (https://www.kommersant.ru/doc/3619240?query=%D0%BA%D0%B8%D0%B1%D0%***

B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C). 03.05.2018).

***

«…Как сообщают аналитики «Лаборатории Касперского», обнаружена новая версия уже известного зловреда SynAck. …он первым из шифровальщиков начал использовать так называемую технику Doppelgänging, которая позволяет вредоносной программе маскироваться под легитимный процесс. Если учесть, что в этом ПО применяются также и другие методы «обмана» антивирусных решений, то задача обнаружения его присутствия в системе становится довольно сложной.

…Как полагают исследователи, SynAck выбирает своих жертв довольно тщательно, поэтому сейчас атаки шифровальщика носят целевой характер. К настоящему моменту заражения зафиксированы в США, Кувейте, Германии и Иране. Средний размер выкупа, который требует зловред, составляет 3000 долларов США…» ***(Обнаружен крайне избирательный шифровальщик // IKSMEDIA.RU (http://www.iksmedia.ru/news/5497619-Obnaruzhen-krajne-izbiratelnyj-shif.html#ixzz5Fxvtrgt2). 11.05.2018).***

***

«Специалисты компании Qihoo 360 Total Security предупредили о новой вредоносной кампании по распространению майнера WinstarNssmMiner, который только за три дня наблюдений заразил порядка 500 000 машин.

WinstarNssmMiner представляет собой обычную для наших дней майнинговую малварь, построенную на основе опенсорсного и легитимного майнера криптовалюты Monero XMRig…

…после заражения WinstarNssmMinerищет ищет в системе процессы защитных решений Avast или "Лаборатории Касперского". Если таковые были обнаружены, майнер сворачивает активность и прекращает работу. Если же защитных решений нет, малварь запускает два процесса svchost.exe, один из которых является скрытым майнером. Второй svchost.exe продолжает "присматривать" за другими антивирусными процессами и может попытаться ликвидировать их, чтобы избежать обнаружения…

По данным исследователей, группировка, создавшая WinstarNssmMiner, в настоящее время заработала 133 Monero, что по текущему курсу равняется примерно 26 000 долларов США.» ***(Майнер WinstarNssmMiner заразил 500 000 систем за 3 дня и способен вызвать сбой в работе ПК при обнаружении // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123085). 18.05.2018).***

***

«Специалисты MalwareHunterTeam и Bleeping Computer предупредили о появлении нового локера и вайпера, который получил название StalinLocker, так как демонстрирует пользователю портрет Сталина и проигрывает гимн СССР…

StalinLocker дает своим жертвам 10 минут на ввод правильного кода. …код – это разница между текущей датой выполнения программы и 1922.12.30 (вероятно,

автор вредоноса имел в виду дату утверждения договора об образовании СССР). Если код введен верно, локер удалит себя из автозапуска и завершит работу.

Если же не ввести код, отсчет дойдет до нуля, а после этого StalinLocker предпримет попытку удаления все файлов из системы жертвы, последовательно перебирая буквы томов от A до Z.

Специалисты отмечают, что пока StalinLocker определенно находится в разработке и еще не завешен до конца, но, к сожалению, малварь доведена на функционального состояния и уже представляет угрозу для пользователей.» ***(StalinLocker удаляет файлы пользователя, если тот не введет правильный код // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123058). 17.05.2018).***

***

«**…**исследователи, в свое время обнаружившие уязвимости Meltdown и Spectre, …представили свой вариант атаки Rowhammer, получивший название Nethammer. По словам исследователей, Nethammer работает без какого-либо управляемого злоумышленником кода и атакует системы, использующие при обработке сетевых запросов некэшированную память…

Nethammer позволяет атаковать удаленно с помощью памяти, используемой для обработки пакетов (при условии их достаточного количества)...

При нормальных условиях кэширование существенно усложняет осуществление атаки, однако исследователи разработали метод, позволивший им обойти кэш и атаковать непосредственно DRAM с целью разбиения ячеек памяти, необходимого для атаки Rowhammer.

QoS (quality-of-service) – технология предоставления различным классам трафика различных приоритетов в обслуживании.» ***(Представлен очередной вариант атаки Rowhammer – Nethammer // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123049). 17.05.2018).***

***

«Киберпреступники экспериментируют с новым методом обхода ряда решений по защите от DDoS-атак, используя протокол Universal Plug and Play (UPnP), чтобы замаскировать исходный порт сетевых пакетов, отправленных в ходе атаки…

Протокол Universal Plug and Play (UPnP) - технология, разработанная для упрощения обнаружения соседних устройств в локальной сети. Одной из возможностей протокола является его способность пересылать соединения из Интернета в локальную сеть. Он делает это, сопоставляя входящие соединения IP/порт с локальными. Данные функции позволяют сетевым администраторам получать доступ к службам, доступным только во внутренней сети.

Однако, если злоумышленнику удастся изменить таблицу сопоставления портов, он может использовать маршрутизатор в качестве прокси и перенаправить входящие соединения. Таким образом, киберпреступники могут изменять таблицы сопоставления портов уязвимых маршрутизаторов и использовать их для маскировки исходного порта DDoS-атак.

Специалисты разработали собственный PoC-код, с помощью которого им удалось успешно протестировать и воспроизвести одну из двух DDoS-атак, использующих данный метод…» ***(Хакеры используют протокол UPnP для осуществления DDoS-атак // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123025). 16.05.2018).***

***

«Эксперты компании Radware предупредили о новой вредоносной кампании, в рамках которой злоумышленники через ссылки в социальной сети Facebook распространяют вредоносное ПО Nigelthorn, способное красть учетные данные пользователей и устанавливать майнеры криптовалюты. Исследователи обнаружили 7 вредоносных расширений для Google Chrome, содержащих Nigelthorn, причем все они были размещены в официальном магазине Chrome Web Store.

Вредоносная кампания активна по меньшей мере с марта нынешнего года. С момента ее начала от Nigelthorn пострадало более 100 тыс. пользователей по всему миру…

Nigelthorn распространяется через ссылки в Facebook, при переходе по которым пользователи попадают на фальшивую страницу в YouTube, предлагающую загрузить расширения для дальнейшего просмотра видео. После установки вредоносное расширение выполняет скрипт JavaScript, в результате устройство пользователя становится частью ботнета. Основная задача вредоноса заключается в краже учетных данных для аккаунтов жертвы в Facebook и Instagram и хищения содержащейся в них информации. Данные сведения используются для отправки вредоносных ссылок друзьям пользователя.

Кроме прочего, Nigelthorn загружает и устанавливает майнер криптовалюты для добычи цифровых средств, в том числе Monero, Bytecoin или Electroneum…

В настоящее время все указанные выше расширения уже удалены из Chrome Web Store…» ***(Пользователям Facebook угрожает новая вредоносная кампания // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=122955). 11.05.2018).***

***

«Исследователи в области кибербезопасности прогнозируют появление в ближайшие несколько месяцев значительного количества новых вредоносов для PoS-терминалов, разработанных на основе исходного кода вредоносной программы TreasureHunter, который был опубликован на одном из русскоязычных киберпреступных форумов в марте нынешнего года.

...Согласно исследованию компании FireEye, автором TreasureHunter является некто под псевдонимом Jolly Roger, который разработал вредонос для группировки BearsInc, занимающейся продажей данных кредитных карт на одном из киберпреступных форумов.

Само по себе вредоносное ПО не слишком сложное и работает по принципу всех PoS-вредоносов. Инфицировав систему под управлением Windows, TreasureHunter добавляет DLL-библиотеку для сохранения присутствия при загрузке, проводит сканирование на предмет процессов, связанных с платежными

терминалами, извлекает данные платежных карт из памяти компьютера и загружает информацию на удаленный сервер, подконтрольный злоумышленникам.» ***(Авторы PoS-вредоноса TreasureHunter раскрыли его исходный код // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=122950). 11.05.2018).***

***

«…Специалисты компании "Доктор Веб" изучили несколько новых модификаций троянца Trojan.PWS.Stealer.23012, распространявшегося по ссылкам в комментариях к видеороликам на популярном интернет-ресурсе YouTube. Эти ролики были посвящены использованию специальных программ, облегчающих прохождение компьютерных игр, — читов и "трейнеров". Под видом таких приложений злоумышленники и раздавали троянца-шпиона, оставляя с поддельных аккаунтов комментарии к видеороликам со ссылкой на Яндекс.Диск…

Все исследованные модификации шпиона написаны на языке Python и преобразованы в исполняемый файл с помощью программы py2exe. Одна из новых версий этой вредоносной программы, получившая наименование Trojan.PWS.Stealer.23370, сканирует диски инфицированного устройства в поисках сохраненных паролей и файлов cookies браузеров, основанных на Chromium. Кроме того, этот троянец ворует информацию из мессенджера Telegram, FTP-клиента FileZilla, а также копирует файлы изображений и офисных документов по заранее заданному списку. Полученные данные троянец упаковывает в архив и сохраняет его на Яндекс.Диск.

Другая модификация этого троянца-шпиона получила наименование Trojan.PWS.Stealer.23700. Эта вредоносная программа крадет пароли и файлы cookies из браузеров Google Chrome, Opera, Яндекс.Браузер, Vivaldi, Kometa, Orbitum, Comodo, Amigo и Torch. Помимо этого, троянец копирует файлы ssfn из подпапки config приложения Steam, а также данные, необходимые для доступа к учетной записи Telegram. Кроме того, шпион создает копии изображений и документов, хранящихся на Рабочем столе Windows. Всю украденную информацию он упаковывает в архив и загружает в облачное хранилище pCloud.

Третья модификация шпиона получила наименование Trojan.PWS.Stealer.23732. …Он ворует на инфицированном устройстве конфиденциальную информацию. Все остальные компоненты троянца написаны на языке Go. Один из них сканирует диски в поисках папок, в которых установлены браузеры, а еще один упаковывает похищенные данные в архивы и загружает их в хранилище pCloud…» ***("Доктор Веб" провел расследование и выявил автора троянцев-шпионов // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=122989). 15.05.2018).***

***

«Эксперты в области кибербезопасности компании McAfee выявили ряд вредоносных приложений из Google Play, используемых властями Северной Кореи для отслеживания действий перебежчиков. Как только самовольный мигрант устанавливал программу на свое устройство, она делала копию всех данных пользователя, отправляя ее создателям.

К настоящему моменту удалось выявить три приложения-шпиона, отслеживающих действия беглецов из Северной Кореи. Создатели сделали ставку на желание мигрантов защитить свои данные, а потому спрятали троян в программы для блокировки доступа к отдельным приложениям. Все они уже удалены из каталога Google Play.

…К моменту удаления от вредоносного ПО пострадали не более 100 человек.» ***(В Google Play найдены приложения-шпионы для слежки за незаконными мигрантами // Goodnews.ua (http://goodnews.ua/technologies/v-google-play-najdeny-prilozheniya-shpiony-dlya-slezhki-za-nezakonnymi-migrantami/). 22.05.2018).***

***

«Министерство внутренней безопасности США совместно с ФБР предупредило о неизвестных ранее зловредах, которые позволяют удаленно контролировать IT-инфраструктуру, перехватывать данные и устанавливать стороннее ПО. По мнению американских ИБ-аналитиков, за атаками стоит северокорейская APT-группировка Hidden Cobra (также известна под именем Lazarus).

Информацию опубликовала Компьютерная команда экстренной готовности США (US-CERT) — подразделение по вопросам кибербезопасности. В отчете описаны два образца зловредного ПО — троян Joanap и червь Brambul...

В случае Joanap эксперты обнаружили 87 зараженных сетевых узлов в 17 странах Европы, Азии, Латинской Америки и Африки. Этот вредонос способен скрытно перемещаться внутри скомпрометированной инфраструктуры, отправлять на удаленный сервер информацию о составе ее участников и перехватывать данные пользовательских компьютеров…

Второй зловред атакует сетевой протокол SMB (Server Message Block), подбирая пароль по встроенному в код списку. При успешном проникновении Brambul собирает и передает своим хозяевам IP-адреса, имена хостов, логины и пароли пользователей, которые можно использовать для последующих атак…

Возможные негативные последствия от атак Joanap и Brambul включают потерю важной информации, сбои в работе IT-систем…» ***(Dmitry Nazarov. US-CERT нашла в арсенале Hidden Cobra два новых зловреда // Threatpost (https://threatpost.ru/us-cert-found-new-hidden-cobra-malware/26348/). 31.05.2018).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Влада США встановила підозрюваного у витоку великого масиву даних Центру кіберрозвідки Центрального розвідувального управління ресурсу Wikileaks в 2017 році.

Ним став 29-річний Джошуа Адам Шульте (Joshua Adam Schulte), …який до 2016 року працював у групі ЦРУ із розробки комп'ютерного коду для розвідки за іноземними супротивниками, але пішов звідти у приватний сектор…

Нагадаємо, торік у березні ресурс Wikileaks опублікував понад 8 тисяч документів та файлів, що відкривають подробиці інструментарію американського кібершпигунства…

Попри те, що розслідування витоку даних триває вже багато місяців, прокурори досі не змогли висунути звинувачення підозрюваному….

Пан Шульте стверджує, що працюючи в ЦРУ, він повідомив про «некомпетентне керівництво та бюрократію» Генерального інспектора цього агентства, а також наглядовий комітет Конгресу США. За його словами, це створило йому образ незадоволеного співробітника, а підозри пали на нього через то, що він був «єдиним, хто нещодавно залишив [інженерну групу ЦРУ] на поганих умовах». Джошуа Шульте також повідомив, що тоді планував провести відпустку в Мексиці, що могло посприяти враженню, що він хотів втекти з країни…» ***(У США назвали підозрюваного у витоку даних Центру кіберрозвідки ЦРУ Wikileaks // MediaSapiens (http://ms.detector.media/web/cybersecurity/u_ssha_nazvali_pidozryuvanogo_u_vitoku_danikh_tsentru_kiberrozvidki_tsru_wikileaks/). 16.05.2018).***

***

«…полиция Нидерландов захватила десять серверов, принадлежащих владельцу так называемого “пуленепробиваемого” (bulletproof) хостинг-сервиса MaxiDed.

…услугами MaxiDed, существующего с конца 2008 года, неоднократно пользовались создатели порносайтов, авторы шпионских и malvertising-кампаний, а также операторы ботнетов, используемых для проведения DDoS-атак, рассылки спама и распространения вредоносного ПО.

Согласно архивной копии maxided[.]com …в его клиентской базе числилось около 2,5 тыс. серверов, размещенных в 82 странах…

За последнее время рынок bulletproof-услуг заметно расширился, однако правоохранительным органам редко удается пресечь подобный бизнес…

Одновременно с захватом голландских серверов MaxiDed в Таиланде и Болгарии были произведены аресты. Расследование показало, что отдыхавший на тайском курорте уроженец Молдовы является владельцем не только bulletproof-сервиса, но также файлообменника DepFile. Другой молдаванин, задержанный в Болгарии, предположительно входил в команду администраторов MaxiDed.

Сайт maxided[.]net теперь перенаправляет визитеров на страницу с сообщением голландской полиции о текущем расследовании. Информация, обнаруженная на захваченных серверах, уже передана в Европол.» ***(Maxim Zaitsev. Bulletproof-услуги MaxiDed более не доступны // Threatpost (https://threatpost.ru/bulletproof-service-maxided-shut-down/26125/). 18.05.2018).***

***

«В минувшую среду сербская полиция сообщила, что совместно с ФБР осуществила арест подозреваемого, который, вероятно, является членом нашумевшей хакерской группы The Dark Overlord. …в документах он фигурирует под инициалами S.S., ему 38 лет и он проживал в Белграде…

The Dark Overlord – группа известная не только в узких андеграундных кругах. Никто не знает наверняка, один это человек, или группа хакеров, однако TDO сделал себя имя еще в 2015 году, когда атаковал медицинские организации, похищал их данные, а затем шантажом вынуждал жертв заплатить, в противном случае угрожая обнародовать всю украденную информацию…

В 2017 году TDO …похитили ряд еще не вышедших на экраны фильмов и телевизионных шоу, а после попытались шантажировать компании Netflix и Larson Studios…

При этом TDO предупреждали, что следующими жертвами станут компании ABC, Fox, National Geographic IFC и по-прежнему Netflix, так как похищен был далеко не один сериал…

Теперь правоохранители пишут, что арестованный гражданин Сербии обвиняется в получении несанкционированного доступа к защищенным компьютерам и сетям, хищении личных данных американских граждан, хищении интеллектуальной собственности, конфиденциальной медицинской информации, включая данных о страховках, а также в шантаже и вымогательстве. Сообщается, что от действий TDO пострадали как минимум 50 человек, а вымогательство принесло злоумышленникам не менее 275 000 долларов (выкупы группировка обычно принимала в биткоинах)…» ***(В Сербии арестован участник хакерской группы The Dark Overlord // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123070). 18.05.2018).***

***

«Двое румынских хакеров были экстрадированы в США, где им предъявлено 31 обвинение…

40-летний Теодор Лаурентиу Костеа (Teodor Laurentiu Costea) и 40-летний Роберт Кодрут Думитреску (Robert Codrut Dumitrescu), фигурирующие в деле как "международные компьютерные хакеры", предположительно похитили у граждан США более $18 млн с помощью сложной фишинговой схемы.

Еще один сообщник злоумышленников, 28-летний Космин Драгичи (Cosmin Draghici), в настоящее время находится в тюрьме в Румынии и ожидает экстрадиции в США.

Согласно обвинительному заключению, с октября 2011 года по февраль 2014 года Костеа и Думитреску взломали уязвимые компьютеры и установили интерактивное программное обеспечение для голосового сообщения для осуществления тысяч автоматических телефонных звонков и отправки текстовых сообщений.

В сообщениях и звонках жертв обманом заставляли позвонить по определенному номеру якобы для того, чтобы решить проблему, связанную с их банковскими счетами. Если жертва звонила, автоответчик просил их назвать свои номера банковских счетов, PIN-коды и номера социального страхования, которые

затем Костеа, Думитреску и Драгичи продали или использовали в личных целях...» ***(Двое румынских хакеров экстрадированы в США за кражу более $18 млн. // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=122903). 08.05.2018).***

***

«…В Азербайджане задержали гражданина Украины Андрея Серба и россиянина Павла Лунина по подозрению в хищении "миллионных сумм" у банков с помощью кибератак…

"Серб и Лунин арестованы, против них возбуждено два уголовных дела по подозрению в краже и незаконном получении компьютерной информации (ст. 177 и 272 УК Азербайджана)", - говорится в сообщении.

…подозреваемые в мошенничестве использовали POS-терминалы (устройства для приема к оплате платежных карт) азербайджанских банков для осуществления киберпреступлений, в результате чего им удалось заполучить миллионы, которые переводились в банки в СНГ…» ***(В Азербайджане задержали украинца и россиянина за миллионные хищения // Единый информационный портал (http://ua-ru.info/news/128145-v-azerbaydzhane-zaderzhali-ukrainca-i-rossiyanina-za-millionnye-hischeniya.html). 23.05.2018).***

***

«ФБР заблокувало мережу з 500 тисяч WiFi-роутерів, зламаних хакерською групою Fancy Bear, яку пов'язують з Російською Федерацією. Ці роутери були заражені шкідливою програмою VPN Filter…

Так, ФБР встановило, що всі шкідливі плагіни зникають, якщо перезавантажити роутер, однак основний код вірусу залишається. Він звертається до контрольної точки резервного копіювання, що знаходиться на сайті ToKnowAll.Com. ФБР за рішенням суду отримало контроль над цією адресою. Зараз співробітники відомства збирають інформацію про кожний заражений роутер, щоб видалити вірус.

Шкідливе програмне забезпечення VPN Filter використовує відомі уразливості для зараження домашніх і офісних роутерів таких компаній як Linksys, MikroTik, NETGEAR і TP-Link. Шкідлива програма може керувати інфраструктурою роутерів і встановлювати шкідливі плагіни…». ***(Дар'я Чабанова. ФБР заблокувало вірус VPN Filter, що вражає WiFi-роутери // Інформаційне агентство «Українські Національні Новини» (http://www.unn.com.ua/uk/news/1732425-fbr-zablokuvalo-virus-vpn-filter-scho-vrazhaye-wifi-routeri). 24.05.2018).***

***

«За хищение персональных данных пользователей с целью продажи королевский суд Сазерка приговорил хакера-рецидивиста к тюремному заключению на срок 10 лет и 8 месяцев.

Согласно материалам дела, британец Грант Уэст (Grant West), известный в сетевом андеграунде как Courvoisier, в течение двух с половиной лет торговал в

дарквебе краденой информацией в виде так называемых fullz — исчерпывающих наборов персональных данных владельцев кредитных карт.

Эту личностную и финансовую информацию хакер собирал, взламывая аккаунты на сервисах брутфорсом, а также посредством рассылки поддельных писем…

Мошеннические и фишинговые сообщения Уэст распространял от имени известных компаний, таких как Sainsbury's, Argos, Uber, Groupon, T-Mobile… По свидетельству лондонской полиции, эта кампания по сбору информации принесла Уэсту 180 тыс. фунтов стерлингов…

…Совокупный ущерб от противозаконной деятельности Уэста прокуратура оценила в 1 млн фунтов стерлингов…» ***(Maxim Zaitsev. Десять лет за взломы и торговлю краденым // Threatpost (https://threatpost.ru/10-years-for-hacking-websites-and-selling-personal-data-on-dark-web/26324/). 30.05.2018).***

***

Технічні аспекти кібербезпеки

«Інтернет-користувачі дедалі частіше намагаються захистити свої персональні дані. Одним із способів є використання VPN…

VPN розшифровується як Virtual Private Network — віртуальна приватна мережа…

VPN дозволяє приховати особу і місце розташування в мережі, захищає дані, гарантує безпеку інформації. Користувач може заходити на сайти, заблоковані у його країні…

VPN-сервіс приховує з'єднання від стороннього ока, але сам він бачить усе. Якщо сервісом володіють зловмисники, вони отримають усю інформацію користувача.

Атаки всередині VPN можна поділити на два види: пасивні та активні.

Пасивні — це збирання даних без втручання в процес передавання інформації. Вони дозволяють бачити історію переглядів сайтів і листи без шифрування. Активні — це викривлення та викрадення даних, що передаються…

Відрізнити перевірений додаток від неперевіреного можна кількома способами.

По-перше, потрібно звернути увагу на власника VPN-сервісу.

В описі кожного додатка мусить бути ім'я автора і цифровий підпис перевіреної контрольними органами організації…

По-друге, треба звернути увагу на кількість серверів та країн, які використовує VPN: чим їх більше, тим краще…

По-третє, варто уважно прочитати умови конфіденційності. У них вказані підстави, за яких сервер видає персональні дані користувачів, а також інформація про термін їх зберігання. Довіряти можна сервісу, який оприлюднює дані лише за рішенням суду і зберігає інформацію протягом одного-десяти днів…

Існує багато інструментів, які можуть замінити VPN: TOR Browser, I2P, Freenet, GNUnet, HTTP проксі-сервери, SOCKS проксі-сервери, CGI-проксі або

"анонімайзери". Усе залежить від того, для чого потрібен сервіс. Найбільш анонімним є TOR Browser. Його недолік — низька швидкість передавання даних.

…Найбільш безпечним є VPN-сервіс, створений користувачем самостійно…

Втім, одного лише VPN для захисту даних від кібератак недостатньо. VPN-сервер буде безсилим, якщо користувач завантажуватиме неперевірені додатки, використовуватиме однакові паролі та заходитиме на підозрілі інтернет-сторінки.» ***(За вами стежать: чим небезпечні VPN-сервіси // Goodnews.ua (http://goodnews.ua/technologies/za-vami-stezhat-chim-nebezpechni-vpn-servisi/). 17.05.2018).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Эксперты в области кибербезопасности компании VUSec рассказали о новой форме атаки на Android-смартфоны…

Ранее считалось, что Rowhammer поражает лишь компьютеры. Уязвимость позволяет взломать смартфон с помощью стандартных расширений мобильного браузера и языка программирования JavaScript. Для этого в браузер необходимо ввести вредоносный код, который поражает микроархитектуру устройства.

А затем хакеры получают доступ к данными, хранящимися в ячейках памяти. …Сотрудники Google и Firefox уже исправили уязвимость в браузере.» ***(Хакеры нашли новый простой способ взломать смартфон // Finance.ua (https://news.finance.ua/ru/news/-/425833/hakery-nashli-novyj-prostoj-sposob-vzlomat-smartfon). 07.05.2018).***

***

«В серверах Lantech IDS, использующихся в промышленных системах, обнаружены две опасные уязвимости, одна из которых является критической и позволяет удаленному злоумышленнику выполнить произвольный код.

Первая уязвимость CVE-2018-8869 представляет собой проблему некорректной проверки входных данных. В частности, практически все поля ввода позволяют злоумышленнику вводить произвольные данные на устройстве.

Вторая уязвимость CVE-2018-8865 является критической проблемой переполнения буфера в стеке. Проэксплуатировав данную уязвимость, злоумышленник может удаленно выполнить произвольный код на устройстве.

Уязвимости затрагивают модели Lantech IDS 2102 2.0 и более ранние…» ***(В промышленных серверах Lantech IDS 2102 обнаружена критическая уязвимость // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=122841). 04.05.2018).***

***

«Соцмережа мікроблогів Twitter у ніч на п'ятницю, 4 травня, надіслала своїм користувачам лист із закликом змінити свої паролі. У заяві компанії йдеться, що вона виявила "баг" у системі зберігання паролів підписників - через технічну помилку вони опинились у внутрішній мережі компанії в незахищеній формі. За даними Twitter, жодних відомостей про можливий витік даних користувачів, кількість яких перевищує 300 мільйонів людей, немає…» ***(Стас Соколов. Twitter закликав усіх користувачів змінити паролі // Deutsche Welle (http://www.dw.com/uk/twitter-%D0%B7%D0%B0%D0%BA%D0%BB%D0%B8%D0%BA%D0%B0%D0%B2-%D1%83%D1%81%D1%96%D1%85-%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D1%83%D0%B2%D0%B0%D1%87%D1%96%D0%B2-%D0%B7%D0%BC%D1%96%D0%BD%D0%B8%D1%82%D0%B8-%D0%BF%D0%B0%D1%80%D0%BE%D0%BB%D1%96/a-43649654). 04.05.2018).***

***

«В реализации DHCP-клиента дистрибутива Red Hat Linux и его веток, таких как Fedora, обнаружена критическая уязвимость, позволяющая выполнить произвольные команды с привилегиями суперпользователя на целевой системе.

Проблема (CVE-2018-1111) содержится в скрипте интеграции с NetworkManager, входящего в состав пакета DHCP-клиента. Злоумышленники, располагающие собственным вредоносным DHCP-сервером, или находящиеся в той же сети, что и жертва, могут проэксплуатировать уязвимость путем подмены ответов DHCP и выполнить произвольные команды с правами суперпользователя на системах, использующих уязвимый клиент.

Ряд исследователей в области кибербезопасности уже опубликовали PoC-коды для эксплуатации уязвимости.…» ***(В DHCP-клиенте Red Hat Linux обнаружена критическая уязвимость // Goodnews.ua (http://goodnews.ua/technologies/v-dhcp-kliente-red-hat-linux-obnaruzhena-kriticheskaya-uyazvimost/). 17.05.2018).***

***

«Обнаружили две новые, ранее неизвестные уязвимости в Adobe Reader и Microsoft Windows. Эксплойты, использующие «двойную уязвимость», были внедрены во вредоносный PDF-файл.

…Сочетание двух уязвимостей крайне опасно, поскольку позволяет злоумышленникам выполнять произвольный код на компьютере жертвы с максимальными привилегиями и минимальным необходимым участием пользователя.

…Чтобы сработала «двойная уязвимость», пользователю достаточно открыть вредоносный PDF-файл на компьютере с уязвимой версией Adobe Reader и операционной системы…» ***(В программах Adobe и Microsoft найдены новые уязвимости // IKSMEDIA.RU (http://www.iksmedia.ru/news/5498860-V-programmax-Adobe-i-Microsoft-najd.html#ixzz5FxsrpIaS). 16.05.2018).***

***

«В свободном доступе оказались личные данные 3 млн пользователей Facebook, воспользовавшихся популярным приложением myPersonality.

…Приложение содержит множество психологических тестов самой разной направленности. За время его размещения на Facebook им воспользовались более 6 млн пользователей, и около половины из них дали согласие на предоставление приложению доступа к своему профилю.

По условиям соглашения разработчики myPersonality имеют право использовать и распространять данные «анонимно, так чтобы по имеющейся информации нельзя было выйти на конкретного пользователя». Они выкладывали все эти данные, предварительно убрав имена пользователей, на специальный сайт, доступ к которому могли получить представители научно-исследовательского сообщества…

Но, как выяснилось, выйти на эти данные могли не только исследователи, но и все желающие. Действующий логин и пароль на протяжении четырех последних лет можно было легко найти в интернете, задав соответствующий запрос, а скачивание полного пакета данных не заняло бы и минуты…

Между тем британские регуляторы уже начали расследование по факту утечки данных…» ***(В Facebook обнаружена новая утечка // IKSMEDIA.RU (http://www.iksmedia.ru/news/5498586-V-Facebook-obnaruzhena-novaya-utech.html#ixzz5Fxtv4E3a). 15.05.2018).***

***

«…На прошлой неделе появилась информация о критической уязвимости в системах шифрования электронной почты PGP и S/MIME. Одни из худших уязвимостей — в почтовых клиентах Thunderbird и Apple Mail, — дают блестящую возможность злоумышленникам, которые смогут перехватить ранее отправленное сообщение. Преступник, встраивая перехваченный зашифрованный текст в невидимые части нового ответного сообщения, отправленного автору или получателю исходного электронного письма, может заставить почтовый клиент слить исходное сообщение как незашифрованный текст. Уязвимости Thunderbird и Mail ещё не исправлены, но недостаток Thunderbird был смягчён обновлением плагина Enigmail GPG.

Другая группа исследователей раскрыла уязвимость в настольной версии мессенджера Signal. Она позволяла злоумышленникам отправлять сообщения, содержащие вредоносный HTML и JavaScript, который выполнялся приложением. Разработчики Signal опубликовали обновление безопасности через несколько часов после конфиденциального уведомления об обнаруженной уязвимости. А разработчики Signal выпустили новый патч, поскольку обнаружили, что обновление не смогло полностью исправить ошибку (это независимо и примерно одновременно установили исследователи)…

На днях исследователи из команды Cisco Talos рассказали о существовании вредоносного ПО, заражающего тысячи людей, использующих десктопный Telegram. Зловред похищает реквизиты учётных записей, текстовые файлы и

другие потенциально конфиденциальные данные и сохраняет их в аккаунтах, к которым может обращаться любой, кто проанализирует код зловреда. Вредоносная программа устанавливается, обманом, заставляя пользователей запустить исполняемые файлы…» ***(Евгения Хотовицкая. Уязвимости в защищённых сервисах как урок для пользователей // РосКомСвобода (https://roskomsvoboda.org/39062/). 22.05.2018).***

***

«Исследователи из калифорнийского университета в Беркли выявили и наглядно показали, каким образом хакеры могут красть данные пользователей, используя приложения с такими голосовыми помощниками, как Siri, Alexa и Google Assistant.

Все это можно осуществить с помощью секретных команд, …которые могут быть вставлены в музыкальные произведения, в видео на YouTube или быть просто неким шумом, который ваши устройства будут "слышать" и распознавать. И в этих звуках будут содержаться команды, которые отдадут управление в руки злоумышленников. Пользователи даже не будут знать, что их голосовые помощники помогли украсть личные и платежные данные, перевели куда-то деньги со счета, оплатили чью-то покупку в интернет-магазине, поделились с кем-то информацией по кредитным картам и т. д.

Эксперты выявили этот критический недостаток в уязвимости у всех распространенных голосовых помощников. Достаточно, чтобы к смартфону, компьютеру или планшету были подключены наушники с микрофоном или умные колонки…

Как отмечает издание The Daily Mail, все крупнейшие хайтек-гиганты – Apple, Google, Amazon – знают о существовании этой проблемы и работают над ее разрешением…» ***(Голосовые помощники могут помогать хакерам красть данные пользователей // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=123082). 18.05.2018).***

***

«На минувшей неделе группа исследователей кибербезопасности обнаружила опасную уязвимость в протоколе OpenFlow, позволяющую злоумышленнику перехватить коммуникации между затронутыми SDN - контроллерами при условии, что заранее скомпрометированное устройство будет внедрено в сеть. …ответственная за поддержку протокола организация Open Networking Foundation (ONF) не будет вносить изменения в OpenFlow, ограничившись рядом рекомендаций, позволяющих снизить риск эксплуатации.

По словам представителей ONF, данная уязвимость представляет угрозу для сетей в следующих случаях: злоумышленник обращается к порту управления устройства и может проэксплуатировать уязвимость в коммутаторе для получения доступа к его сертификату; уязвимость существует на передающем уровне коммутатора, также позволяя получить доступ к сертификату; злоумышленник может "сгенерировать или приобрести сертификат, которому доверяет контроллер". Все сценарии предполагают защиту соединения переключателя-контроллера

сертификатами TLS/SSL, которая является рекомендуемой в данном оборудовании…» ***(Разработчики OpenFlow не будут вносить изменения в протокол ради исправления уязвимости // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=122999). 15.05.2018).***

***

«В начале мая текущего года стало известно о двух уязвимостях в домашних маршрутизаторах с поддержкой технологии GPON (в частности, в устройствах производства Dasan Networks), позволяющих получить контроль над устройством. Данные уязвимости почти сразу оказались под прицелом злоумышленников и, по информации экспертов китайской компании Qihoo 360 Netlab, в настоящее время по меньшей мере пять ботнетов (в том числе Hajime, Mettle, Mirai, Muhstik и Satori) предпринимают попытки инфицировать уязвимые устройства.

Что интересно, пока ни одному из ботнетов не удалось заразить маршрутизаторы…» ***(На уязвимые маршрутизаторы GPON ведут охоту сразу 5 ботнетов // ООО "Гротек" (http://www.itsec.ru/newstext.php?news_id=122951). 11.05.2018).***

***

«…В последнее время все больше железнодорожных компаний по всему миру настраивают в своих поездах сети Wi-Fi для пассажиров. Тем не менее, возможность пользоваться интернетом не только делает поездки гораздо комфортнее, но и развязывает руки хакерам. К такому выводу пришли исследователи безопасности на основании ряда тестов на проникновение, результаты которых опубликовал специалист компании Pen Test Partners Кен Манро (Ken Munro).

В процессе тестирования исследователи обнаружили отсутствие разделения между сетями для пассажиров, сотрудников железной дороги и для управления поездом. Получив доступ к пассажирской сети, исследователям затем удалось получить доступ и к управлению поездом.

Вторая обнаруженная исследователи проблема заключалась в учетных данных по умолчанию. С их помощью специалисты смогли получить персональную информацию пассажиров и данные их платежных карт (в поездах некоторых компаний пассажиры второго класса должны платить за пользование Wi-Fi).

Манро… дал несколько рекомендаций по их исправлению. Прежде всего, отмечает исследователь, необходимо изолировать пассажирскую сеть от остальных (трафик должен проходить только между пользовательскими устройствами и интернетом). Интерфейс панели управления беспроводным маршрутизатором не должен быть доступен для пассажиров, поэтому администраторам рекомендуется настроить список тех, кому разрешен доступ…» ***(Wi-Fi для пассажиров позволяет хакерам захватить управление поездом // SecurityLabRu (https://www.securitylab.ru/news/493276.php). 15.05.2018).***

***

«…Крупнейший британский сотовый оператор EE (насчитывает порядка 30 млн абонентов) был вынужден принять меры по обеспечению безопасности своего ключевого репозитория кодов после того, как обнаружилось, что авторизоваться в нем мог любой желающий с помощью дефолтных учетных данных.

Исследователь безопасности под псевдонимом Six обнаружил на поддомене EE портал Sonarqube, использующийся сотовым оператором для аудита кода и поиска уязвимостей на своем сайте и портале для клиентов. Авторизоваться на портале мог кто угодно, используя оставленные по умолчанию логин и пароль (admin/admin).

С помощью дефолтных учетных данных Six авторизовался в репозитории и получил доступ к двум миллионам строк кода, в том числе к частным API сотрудников EE и разработчиков, а также к закрытым ключам Amazon Web Services. По словам исследователя, с помощью закрытых ключей злоумышленник может получить еще больший доступ к хранилищам компании, web-серверам и другим конфиденциальным данным, таким как отчеты об отладке…» ***(Британский сотовый гигант забыл поменять пароль для своего репозитория кодов // SecurityLabRu (https://www.securitylab.ru/news/493232.php). 11.05.2018).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«…Apple добавила в iOS новую функцию безопасности…

Первыми новую функцию безопасности под названием «Режим ограничения USB» (USB Restricted Mode) обнаружили исследователи компании Elcomsoft в ходе анализа кода iOS 11.4. В этом режиме устройство по-прежнему может заряжаться через USB, однако передача данных становится невозможной, если оно было заблокировано в течение семи дней. Когда пользователь самостоятельно разблокирует устройство, режим отключится.

«Режим ограничения USB» позволит пользователю защитить конфиденциальность своих данных и предотвратит возможность получения их с устройства без его согласия. Как правило, изъяв iPhone подозреваемого, сотрудники правоохранительных органов вынуждены использовать для его разблокировки специальный эксплоит. Если на момент изъятия таковой отсутствует, правоохранители просто регистрируют устройство как вещественное доказательство и кладут на полку до появления эксплоита…» ***(Новая функция в iOS защитит iPhone от взлома правоохранителями // SecurityLabRu (https://www.securitylab.ru/news/493182.php). 10.05.2018).***

***

«Современная компания обрабатывает и хранит большие объемы информации в графических форматах. Прежде всего, это касается сканов различных документов. Для предотвращения утечек такой информации необходимо использовать DLP-системы с модулями распознавания.

Аналитический центр InfoWatch составил дайджест утечек фотографий…

В зоне особого риска находятся компании, которые работают с большим количеством клиентских документов и делают их скан-копии…

С утечками изображений сталкивались даже руководители государств. Так, в 2014 г. в Интернет попали сканы страниц паспорта президента Франции Франсуа Олланда. В частности, пользователи узнали, что рост французского лидера составляет 170 см, а также смогли увидеть информацию о его визе в Ирак…» ***(Отпечатки на миллион: утечки конфиденциальных изображений // IKSMEDIA.RU (http://www.iksmedia.ru/news/5497957-Utechki-konfidencialnyx-izobrazheni.html#ixzz5FxumOGpu). 14.05.2018).***

***

«…Компания HID Global объявляет о продолжении сотрудничества с Microsoft. Компании предлагают решение, дающее возможность пользователям использовать смарт-карты для входа в Microsoft Windows, устройства и облачные приложения и исключающее использование для этих целей только логина и пароля.

FIDO 2.0 – это открытая, основанная на стандартах система аутентификации пользователей, которая заменяет пароли на продвинутые идентификаторы FIDO, предназначенные для более эффективного противодействия кибератакам, включая фишинг и утечки данных. Пользователи могут использовать смарт-карты HID, содержащие идентификаторы FIDO 2.0, без каких-либо дополнительных настроек. Microsoft обеспечивает поддержку FIDO 2.0 в веб-браузерах, облачных приложениях и в самой ОС Windows, расширяя возможности для более безопасной аутентификации в масштабах всего Интернета…

FIDO представляет собой перспективную модель аутентификации, в которой требуется предоставление криптографического подтверждения учетных данных. В то же время повышается удобство для пользователей, которым до появления решения FIDO приходилось многократно авторизовываться в различных сервисах, например, для доступа к банковскому счету или электронной почте. Система FIDO также способствует сохранению конфиденциальности данных, повышая уровень доверия…» ***(Новое решение для идентификации и управления доступом // IKSMEDIA.RU (http://www.iksmedia.ru/news/5497704-Novoe-reshenie-dlya-identifikacii.html#ixzz5FxvV7i3g). 11.05.2018).***

***

«На всё более тесном и конкурентном рынке кибербезопасности стартап Tanium занял очень весомые позиции. Его клиентами числятся 12 из 15 крупнейших банков США, 6 из 10 ведущих розничных торговцев и военное ведомство США. Tanium предоставляет им сервисы защиты граничных точек, то есть обеспечивает безопасность всех типов компьютерных устройств.

…последний раунд финансирования сделал Tanium самым обеспеченным стартапом кибербезопасности: инвестиционная компания TPG вложила в него ещё 175 млн долл., подняв общую капитализацию до 5 млрд долл.

…это свидетельствует, что кибербезопасность считается одной из наиболее выгодных возможностей для вложения средств…

Рохит Кулкарни (Rohit Kulkarni), директор SharesPost Financial, в мае отметил, что аппетиты инвесторов и их интерес к кибербезопасности достигли рекордного уровня благодаря участившимся инцидентам со взломами защиты.» ***(Новая инвестиция довела стоимость Tanium до 5 млрд долл. // «Компьютерное Обозрение»(http://ko.com.ua/novaya_investiciya_dovela_stoimost_tanium_do_5_mlrd_doll_124664). 18.05.2018).***

***

«С введением в действие «Общего регламента по защите данных» (General Data Protection Regulation) компании рискуют столкнуться с проблемами, полагаясь лишь на существующие разрозненные меры безопасности.

Такое мнение высказывается в отчете, опубликованном компанией Aruba (входит в Hewlett Packard Enterprise). Согласно документу, большинство существующих средств защиты, которые применяют методы бизнес-правил для обнаружения угроз, не могут выявлять новые атаки, использующие реальные учетные данные пользователей для доступа к конфиденциальной информации. Это означает, что компании рискуют оказаться не в состоянии обнаружить и сообщить о нарушениях в течение 72 часов, предусмотренных General Data Protection Regulation (GDPR). В результате несоблюдения регламента максимальные штрафы могут составить до 20 млн евро или 4% годового оборота.

…компания подчеркивает необходимость дополнения этих средств защиты еще одним уровнем мониторинга, который использует новые методы обнаружения атак, такие как сценарный анализ и машинное обучение, предназначенные для анализа всей сети в совокупности и нахождения даже небольших изменений, которые свидетельствуют об атаке.

…Платформа сетевой безопасности Aruba 360 Secure Fabric предлагает комбинацию инструментов контроля доступа в сеть для наблюдения за миллионами устройств, которые подключаются к ней, и обеспечения доступа на основе политик, специфичных для устройства, которые могут значительно ограничить доступ к персональным данным пользователя…» ***(Традиционных методов защиты может оказаться недостаточно // IKSMEDIA.RU (http://www.iksmedia.ru/news/5498784-Tradicionnyx-metodov-zashhity-mozhe.html#ixzz5FxtSbsXU). 16.05.2018).***

***

«…В своем настоящем виде Python не позволяет инструментам безопасности видеть, что происходит в среде выполнения кода.

Злоумышленники могут использовать это для выполнения на системе вредоносных операций в обход аудиторских инструментов…

В Python Enhancement Proposal 551 (PEP-551) главный разработчик ядра Python Стив Доуэр (Steve Dower) предложил добавить в язык программирования два новых API, позволяющих инструментам безопасности обнаруживать, когда Python выполняет потенциально опасные операции. Новые API (Audit Hook и Verified Open Hook) будут деактивированы по умолчанию.

Audit Hook сможет отправлять предупреждения о некоторых операциях Python. Инструменты безопасности будут понимать эти предупреждения как сигнал о потенциальной опасности и останавливать операции в целях предотвращения возможного ущерба. Verified Open Hook представляет собой механизм, позволяющий среде выполнения Python знать, каким файлам разрешено выполняться…» ***(Python разрешит инструментам безопасности «заглядывать» в среду выполнения // SecurityLabRu (https://www.securitylab.ru/news/493625.php). 28.05.2018).***

***

«…автомобили уже сегодня становятся потенциальным объектом для хакерских атак, поэтому актуальной проблемой автомобильной отрасли является обеспечение защиты информации и важных компонентов, отвечающих за безопасность.

Необходимо защитить транспортные средства от атак хакеров, в частности, важные для безопасности компоненты, такие как, например, тормозная система. Для реализации концепции безаварийного вождения Vision Zero важно, чтобы автомобили могли взаимодействовать с друг с другом и с инфраструктурой, например, по цифровым каналам связи. И потенциально это открывает двери хакерам, а значит, цифровые системы должны быть не только надежными и функциональными, но и устойчивыми к возможным внешним атакам. В связи с этим технологическая компания Continental использует технологии кибербезопасности для защиты от возможных хакерских атак — как важных для безопасности компонентов автомобилей, так и производственных предприятий…

Технология криптографических процессов для обеспечения безопасности была впервые внедрена в новейшую тормозную систему MK C1, в которой функции активации тормозов, усилителя тормозного привода и системы управления (ABS и ESC) объединены в одном компактном облегченном модуле…

Continental укрепляет все возможные для атаки направления, внедряя решения в области кибербезопасности на множестве уровней: первый уровень представляет защиту компонентов отдельных электронных систем, второй — коммуникаций между системами внутри автомобиля, третий — внешних интерфейсов, а на четвертом уровне обеспечивается защита данных внешнего взаимодействия от кражи и манипуляций. Также этот уровень включает облачные и серверные решения. Теперь наше предложение пополнилась разнообразными комплексными решениями, разработанными компанией Argus Cyber Security — экспертом в области обеспечения кибербезопасности автомобилей, недавно приобретенной концерном Continental…» ***(Continental защищает компоненты и***

производство от хакерских атак // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5502660-Continental-zashhishhaet-komponenty.html#ixzz5HALqkIvF). 31.05.2018).

***

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

Гончар С. Ф. Особливості забезпечення кібербезпеки об'єктів критичної інфраструктури / С. Ф. Гончар // Моделювання та інформаційні технології. - 2017. - Вип. 80. - С. 27-32.

Наведено особливості автоматизованих систем управління технологічними процесами, які необхідно враховувати при розробці та впровадженні заходів забезпечення кібербезпеки об'єктів критичної інфраструктури.

Шифр зберігання НБУВ: Ж69991.

***

Комаров М. Ю. Методика побудови системи управління інформаційною безпекою на об'єктах критичної інфраструктури / М. Ю. Комаров, С. Ф. Гончар // Моделювання та інформаційні технології. - 2017. - Вип. 81. - С. 12-19.

Проведено аналіз алгоритму створення системи управління інформаційною безпекою на об'єкті, де циркулює інформація з обмеженим доступом. Наведено перелік основних документів, що мають бути розроблені в процесі створення системи управління інформаційною безпекою.

Шифр зберігання НБУВ: Ж69991.

***

Матеріали XIII Всеукраїнської наукової конференції «Теорія та практика сучасної юриспруденції». - Харків, 2017. - 296 с.

Зі змісту:

- Макаренко А.С. Проблема кіберзлочинності в Україні.

Шифр зберігання НБУВ: ВА818603.

***

Матеріали XIV Всеукраїнської наукової конференції «Теорія та практика сучасної юриспруденції». - Харків, 2017. - Т. 2. - 309 с.

Зі змісту:

- Зайва Ю.Р. Міжнародно-правове співробітництво у сфері протидії кіберзлочинності.

Шифр зберігання НБУВ: В357003/2.

***

Матеріали Всеукраїнської наукової конференції студентів та аспірантів «Верховенство права очима правників-початківців», 18 листопада 2017 року. - Одеса, 2017. - 639 с.

Зі змісту:

- Басалюк Н.В. Інформаційно-технічна війна й кібертероризм: поняття, особливості;
- Шишацька Ю.С. Кримінально-правові засоби протидії кіберзлочинності в Україні;

Шифр зберігання НБУВ: ВА818429.

***

Матеріали Міжнародної науково-практичної конференції "Проблеми становлення інформаційної економіки в Україні", 19-21 жовтня 2017 року, м. Львів : [зб. доп.] / Львів. нац. ун-т ім. Івана Франка. - Львів : Левада, 2017. – 270 с.

Зі змісту:

- Браєр В. Сутність інформаційної безпеки та захисту інформації в Україні;
- Полюга Л., Жовтанецький М. Інформаційна безпека та хмарні технології в економіці;
- Приймак В., Смаль Т. Інформаційна безпека України та Польщі в сучасних умовах.

Шифр зберігання НБУВ: ВА818337.

***

Правові засади діяльності правоохоронних органів : зб. наук. пр. за матеріалами IV Міжнар. наук.-практ. конф. (15 груд. 2017 р.). - Харків, 2017. - 189 с.

Зі змісту:

- Матюхіна Н.П. До проблеми створення національної системи кібербезпеки України (організаційно-правовий аспект);
- Дядюша А.Р. Міжнародне співробітництво служби безпеки України щодо забезпечення кібербезпеки (окремі аспекти дослідження);
- Лиманський В.Ю. Правові засади забезпечення інформаційної безпеки в департаменті кіберполіції.

Шифр зберігання НБУВ: СО35622

***

Самойленко О.А. Співвідношення термінів, що застосовуються для позначення злочинів, учинених з використанням обстановки кіберпростору / Самойленко О.А. // Науковий вісник Херсонського державного університету. Сер. : Юридичні науки. - 2017. - Вип. 5(2). - С. 155-159.

Проаналізовано терміни та терміносполучення, що використовуються для позначення злочинів, учинених з використанням обстановки кіберпростору.

Шифр зберігання НБУВ: Ж73149/юр.

Виготовлено в друкарні
ТОВ «Видавничий дім «АртЕк»
04050, м. Київ, вул. Мельникова, буд. 63
Тел.. 067 440 11 37
artek.press@ukr.net
www.artek.press

Свідоцтво про внесення суб'єкта видавничої справи
до державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції –
серія № ДК №4779 від 15.10.14р.