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

№ 6 (червень)

Київ – 2019

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І.Вернадського. – К., 2019. – №6 (червень) . – 71с.

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

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

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

ЗМІСТ

«…Зачем существует профессиональное сообщество «SkyNet», как им удается выживать и проводить профильные мероприятия без финансовых вливаний, InternetUA узнавал у главного идеолога комьюнити, ИБ-эксперта Евгения Гулака.

– Всё началось в 2017 году, во время крупнейшего киберинцидента в мире – атаки вируса PetyaA. Тогда многие компании «упали» и просто не знали, что им делать. Я тогда руководил информационной безопасностью в АТ «ТАСКОМБАНК». Когда всё это началось, я успел сделать два-три звонка, чтобы предупредить коллег в других банках, а дальше мы перешли к восстановлению и понятно, что ни на что другое времени не было…

Среди идей Евгения Гулака – создание своеобразного «профсоюза для кибербезопасников»…». ***(Владимир Кондрашов. Украинские борцы с кибертерроромъ объединились в «SkyNet» // Internetua (http://internetua.com/ukrainskie-borcy-s-kiberterrorom-ob-edinilis-v-skynet). 10.06.2019).***

***

«…Віце-премєр-міністр та міністр економічного розвитку і торгівлі Степан Кубів заявив, що в уряді збираються протестувати технологію перепису населення через гаджети — смартфони або планшети — у грудні поточного року…

«Як альтернативу паперовій анкеті ми пропонуємо громадянам самостійно заповнити відповідні дані в електронному кабінеті домогосподарства, наприклад через смартфон. Заповнена інформація буде захищена спеціальним шифруванням, щоб знеособити персональні дані під час передачі на центральний сервер», — пояснив пан Кубів.

За його словами, тим, хто не виявить бажання або ж не зможе самостійно ввести дані в електронній формі, будуть пропонувати відповісти на питання із анкети, яка буде в наявності у представників команди перепису на спеціальному смартфоні або планшеті.

«Ці дані захищені і будуть потрапляти на центральний сервер Держстату. В сумі вони дадуть нам розуміння соціології і демографії регіону, фактичної кількості жителів та іншу інформацію без її персоналізації», — зазначив віце-прем'єр.

Він також повідомив, що після аналізу ефективності такого способу можна буде не тільки провести перепис населення у 2020 році, але ще й перейти до наступного етапу — цифровізації інших подібних заходів. Нариклад, проводити важливі соцопитування за допомогою смартфонів…» ***(Степан Кубів запропонував провести перепис населення за допомогою смартфонів // MediaSapiens (https://ms.detector.media/web/cybersecurity/stepan_kubiv_zaproponuvav_provesti_perepis_naselennya_za_dopomogoyu_smartfoniv/). 10.06.2019).***

***

«Державна служба спеціального зв'язку та захисту інформації проводить тендер, умови котрого завідомо прописані під конкретну ІБ-компанію. В ДССЗЗІ не полінилися і в умовах тендеру на мільйон прописали наявність в керівника компанії-переможця наукового ступеня доктора наук та вченого звання професора у ВНЗ четвертого рівня акредитації.

На це звернув увагу експерт з кібербезпеки, засновник Української групи інформаційної безпеки Костянтин Корсун у своєму дописі на Facebook…

Мова йде про тендер на проведення досліджень щодо вимог до системи оцінки фахової підготовки аудиторів інформаційної безпеки, збору та аналізу інформації, отриманої під час аудиту інформаційної безпеки на об`єктах критичної інфраструктури та в системах обробки державних інформаційних ресурсів. Переможець тендеру має розробити технічне завдання, що міститиме технічні вимоги до інформаційно-аналітичної системи збору та аналізу інформації, отриманої під час аудиту інформбезпеки на об'єктах критичної інфраструктури та в системах обробки державних інформаційних ресурсів. Також на майбутнього переможця тендеру покладається завдання з розробки технічних вимог до апаратно-програмного комплексу підготовки та оцінки фахової підготовки аудиторів інформаційної безпеки, що міститиме тестові опитувальні листи з теоретичних питань та практичні завдання для визначення рівня знань аудиторів інформаційної безпеки з метою проведення ІБ-аудиту. Самі роботи мають пройти в два етапи – до вересня 2019 року мають бути розроблені технічне завдання та технічні вимоги до системи, а роботи з розроблення проектів тестових опитувальних листів з теоретичних та практичних завдань для визначення рівня знань аудиторів завершуються в грудні 2019 року.

Згідно нового закону «Про основні засади забезпечення кібербезпеки України», усі об'єкти критичної інфраструктури та деякі державні органи зобов'язані проходити щорічний аудит, для проведення якого потрібно відібрати аудиторів, а для того, щоб їх відібрати, необхідно розробити вимоги до них. Для цього і проводиться цей тендер. Щоб показати, типу, «ось дивіться, ми не самі це придумали, це незалежна фірма-переможець тендеру так запропонувала». Типу «приватно-державне партнерство» і все таке. – пояснює Костянтин Корсун. – Чому на «дослідження» виділяється саме мільйон гривень, а не десять чи сто мільйонів – без поняття, no idea. Може, це просто скромність? Я знаю кілька серйозних компаній, які зроблять значно дешевше, рази в два-три-чотири дешевше.

Однак не лише очікувана вартість закупівлі привернула увагу експерта. За спостереженнями Костянтина Корсуна, для того, щоб тендер виграла потрібна фірма, у тендерній документації працівники Адміністрації Держспецзв'язку «виписали фантастичні умови» під, імовірно, заздалегідь відому компанію.

Для «проведення досліджень» спочатку вимагається «наявність обладнання та матеріально-технічної бази». Насправді ж для такої роботи потрібні знання та досвід. Ноутбук та Інтернет. Нічого більше не потрібно, але заздалегідь визначений корупціонерами з Держспецзв'язку переможець явно має купу металобрухту у якомусь ангарі яка гордо іменується «матеріально-технічної база», – вважає засновник УГІБ.

Більше того, звертає увагу експерт, в тендері ДССЗЗІ прописала особливі вимоги до керівника та консультанта проекту. Справа в тому, що організатор тендеру вимагає, аби керівник проекту був «професійним проектним менеджером, що засвідчується сертифікатом Міжнародної асоціації управління проектами рівня «В» або «А» (або ж сертифікат PMI – PgMP, PfMP, PMP».

PMP – це нормально для проектного менеджменту. Але я перепрошую, з якого дива тут у нас намалювався якийсь проектний менеджер? Проект – це щось вже дуже конкретне, з визначеними строками, сумами, дедлайнами, критеріями, вимогами, стадіями і т.ін. І ось, наприклад, PfMP – це «професіонал управління портфелями». До чого тут «дослідження щодо вимог до системи оцінки фахової підготовки аудиторів інформаційної безпеки»? Що взагалі може знати управлінець портфелями про аудит інформаційної безпеки? На моє глибоке переконання, формувати вимоги з оцінки аудитора інфо(кібер)безпеки може людина, яка, перш за все, має відповідні професійні кібербезпекові сертифікації (CISA, CISM, CISSP), а також провела 30-60 успішних аудитів інформаційної безпеки, і може це підтвердити, обов'язково з рекомендаціями (не менше трьох, незалежних, по кожному проекту), – говорить Костянтин Корсун…

Більше того, в Держспецзв'язку вирішили, що керівник проекту повинен мати «науковий ступінь доктора наук в технічній сфері (спеціальності 05.13.06, 05.13.21, 05.13.22, 21.05.01)…та вчене звання професора у вищому навчальному закладі 4 рівня акредитації (науковій установі) в Україні».

По-перше, вказані спеціальності – це про застарілі ТЗІ-КЗІ та сумновідому КСЗІ, які вже давно нікому не потрібні, але які вперто викладаються у вітчизняних вишах. По-друге: навіщо практикуючому аудитору «доктор наук» чи «професор»? Найкращі та найуспішніші фахівці з ІТ-аудиту ніколи не мали думки витрачати десятиліття свого життя на отримання оцих непотрібних псевдонаукових регалій, які потрібні лише для роботи у пострадянській системи вищої освіти. По-третє, одразу відсікаються усі іноземні фахівці, та хоч би і сам Брюс Шнаєр або ж якийсь американський розробник стандартів NIST, – пояснює експерт. – Та і взагалі: навіщо для даного суто практичного дослідження обвішаний регаліями аксакал-теоретик made in Ukraine, якщо мова йде про надсучасний світ транснаціональної області знань? І в якій вже сто раз все давно придумано? Зрозуміло, що ця вимога написана виключно під одну конкретну людину.

Останню здогадку Костянтин Корсун підтверджує ще однією вимогою, прописаною в умовах тендеру: «консультант (відповідальний виконавець) повинен мати науковий ступінь доктора наук (спеціальності 05.12.02, 05.13.06, 05.13.21, 05.13.22, 21.05.01) та власний науковий доробок у сфері кіберзахисту»…» ***(Владимир Кондрашов. Експерт: держспецзв'язку взялася «розпиляти» мільйон на імітацію заходів по кібербезпеці // Internetua (http://internetua.com/ekspert-derjspeczv-yazku-vzyalasya-rozpilyati-milion-na-imitaciua-zahodiv-po-kiberbezpeci-1). 18.06.2019).***

***

«До другої річниці атаки вірусом NotPetya експерти з кібербезпеки провели перевірку державних підприємств.

Презентацію висновків дослідження провели 27 червня. Зокрема, експерт з кібербезпеки Костянтин Корсун заявив, що Україна не зробила вагомих висновків після масштабної атаки вірусом NotPetya у 2017 році.

Як передає «Укрінформ», пан Корсун вважає, що Україна залишається незахищеною перед новою кіберагресією, а агенція, яка опікується кіберзахистом держави, — Держспецзв'язку — використовує застарілі методи роботи.

Одним з головних інструментів, який використовується Держспецзв'язку, є так звана КСЗІ — комплексна система захисту інформації, яка наразі активно впроваджується на різних підприємствах та об'єктах критичної інфраструктури.

Олександр Галущенко додав, що зовнішня перевірка захисту провайдерів та державних ресурсів, що використовують КСЗІ, показала її неефективність.

«Попри її використання величезна кількість надважливих даних, зокрема про об'єкти критичної інфраструктури, персональні дані українців, дані комерційних компаній тощо, все ще знаходяться у відкритому доступі. А це абсолютно неприпустимо», — сказав пан Галущенко…» ***(Україна незахищена перед новою кіберагресією, — експерт з кібербезпеки // MediaSapiens (https://ms.detector.media/web/cybersecurity/ukraina_nezakhischena_pered_novoyu_kiberagresieyu_ekspert_z_kiberbezpeki/). 27.06.2019).***

***

«Ряд ресурсов, среди которых веб-ресурсы Министерства обороны Украины, Государственного управления делами, Генеральной прокуратуры Украины, Министерства иностранных дел Украины и ещё нескольких десятков госучреждений, не защищены от ARP-spoofing – сетевой атаки, при которой злоумышленники могут перехватывать пакеты данных в сети, изменять трафик или полностью его остановить… Особой пикантности ситуации добавляет тот факт, что все эти госучреждения подключены к провайдеру, которого Государственная служба специальной связи и защиты информации считает защищенным.

Об этом говорится в отчете по результатам одиночного сканирования всех устройств в диапазоне адресов провайдера «Адамант», опубликованном известным украинским экспертом по кибербезопасности Александром Галущенко.

…группа патриотично настроенных экспертов на протяжении месяца исследовали сети операторов, провайдеров телекоммуникаций, которые построили по требованию Государственной службы специальной связи и защиты информации так называемую комплексную систему защиты информации (КСЗИ) и имеют Аттестат соответствия системы защиты защищенных узлов доступа. «Построение КСЗИ» на данный момент является обязательным условием для провайдера, предоставляющего услуги доступа к сети Интернет государственным органам и учреждениям и стоит от 300 тысяч гривен, однако, как утверждают авторы исследования, КСЗИ – «иллюзия защищенности, очковтирательство и рассадник коррупции».

С понедельника Александр Галущенко опубликовал на своей странице в Facebook две записи с общими выводами исследования, а начиная со среды, 12 июня, публикует отчеты по каждому оператору, провайдеру телекоммуникаций,

«построившему КСЗИ», отдельно. Первым опубликованы данные о проблемах в сети провайдера ООО «Адамант».

Тестировались все устройства, находящиеся в сети конкретного провайдера, в том числе и клиентские устройства, за которые провайдер ответственности не несет. Также ряд обнаруженных проблем не является прямой ответственностью провайдера и относится, скорее, к компетенции конечных пользователей (в том числе и госорагнов). Как отметил директор по внешним связям Восточной Европы и Центральной Азии RIPE NCC Алексей Семеняка, многие обнаруженные проблемы можно объяснить некомпетентностью клиента и его нежеланием учится.

Справедливости ради, отсутствие TLS у клиента не есть проблема провайдера. Ну, то есть, как провайдер может заставить клиента получить сертификат и использовать TLS? Примерно никак, – отмечает представитель RIPE NCC. – Насколько я помню, «Адамант» предлагает клиентам помощь с получением сертификата от Let's Encrypt, но, по опыту наблюдений, клиента не убедишь, что это ему нужно, даже если это бесплатно.

Тем не менее, по мнению опрошенных нами экспертов, «клиентские» проблемы только подчеркивают, что построение КСЗИ провайдером и подключение к защищенному узлу доступа госорганов, не готовых тратить средства и время на безопасность, не более чем «театр безопасности», основную роль в котором играет желание чиновников обогатится…

В отчете по результатам сканирования всех диапазонов адресов провайдера ООО «Адамант» говорится о том, что наиболее возможный вектор атаки на госучреждения – так называемый ARP спуфинг (ARP spoofing). Это сетевая атака, при которой злоумышленник посылает поддельные сообщения протокола ARP (Address Resolution Protocol) в локальную сеть, чтобы трафик вместо необходимого IP-адреса был направлен злоумышленнику.

В основном мы говорим о возможности ARP спуфинга с уязвимых устройств в диапазонах, в которых находится гейт этих устройств. Например, если у нас в диапазоне класса C (/24, подсеть с 255 хостами, где первый – 0), то мы можем получить авторотационные данные со всех веб интерфейсов, в которых отсутствует шифрование, – объясняет Александр Галущенко. – Например, есть диапазон адресов 22.22.22.0/24, в котором по IP-адресам 22.22.22.77 и 22.22.22.88 есть два веб интерфейса, где требуется авторизация (ввод логина и пароля), а также у нас в этом же диапазоне есть уязвимый роутер/шлюз/видеокамера с адресом 22.22.22.125, который мы можем использовать для атаки по типу ARP спуфинга, – такие данные интерфейсы мы считаем уязвимыми. Возможно, кто-то скажет, что так невозможно, или попросит больше технических подробностей, просто знайте: это работает. Из нашего опыта проведения исследований и «злых» пентестов, это, пожалуй, один из самых любимых векторов исследования.

Всего в отчете по «Адаманту» Александр Галущенко опубликовал сведения о 9 клиентских веб-хостах, которые запрашивают авторизационные данные по http (нешифрованному) вместо https (шифрованному) протоколу, открытых в сеть двух базах Elasticsearch (свободное программное обеспечение, поисковый сервер, разработанный на базе Lucene), двух клиентских роутерах, и ещё о ряде проблем

(возможности провести успешную атаку на сеть МИД, неприкрытый репозитарий компонентов и т.д.)…

Как рассказал нашему изданию президент группы компаний «Адамант» Ивана Петухова, многое из отмеченного в исследовании – не относится к компетенции провайдера.

У некоторых операторов, провайдеров связи есть возможность предоставлять две разные услуги по доступу к Интернету: обычная, которая никем не регулируется, назовем это коммерческая услуга доступа в Интернет (сокращенно - КД) и услуга защищенного узла Интернет доступа (сокращенно - ЗУИД), – объясняет Иван Петухов. – Корни сегодняшнего ЗУД начинаются еще с конца 90-х, когда был разработан печально известный "Приказ трех" (УкрСат, УКРКОСМОС и Укртелеком), которые могли предоставлять доступ к ОДВ. Молодым это уже ни о чем не говорит, поэтому оставим это в истории. После «падения» «Приказа трех» появились Постановление КМУ «Об утверждении Порядка подключения к глобальным сетям передачи данных» от 12.04.2002 № 522 и Приказ Государственного комитета связи и информатизации Украины от 17.06.2002 № 122. Благодаря усилиям членов и правления ИнАУ заключением Министерства юстиции Украины № 13/71 от 04.08.2006 Приказ № 122 от 17.06.2002 был отменен, но действие Постановления 522 осталась.

Как объясняет Иван Петухов, каждый оператор / провайдер, которой построил подобный ЗУИД и прошел соответствующую проверку и сертификацию в ГСССЗИ, имеет право предоставлять доступ к сети Интернет органам государственной власти (ОГВ).

В свою очередь, ОГВ вправе получать доступ в Интернет только у операторов / провайдеров имеющих ЗУИД, и это было с 2004 года... "Адамант" в числе первых выполнил эту норму в 2005 году, и, параллельно, в составе основателей ИнАУ боролся с этим, и как основатель и как член правления ИнАУ лично я ... и это тоже есть в истории, – рассказывает Иван Петухов. – ОГВ вправе получать доступ к сети Интернет, но есть такой момент, для выполнения возложенных на них задач и на основании пола 19 Конституции Украины, Законов и нормативно-правовых актов, они выполняют свои функции и задачи и по своему усмотрению делают защиту своих сетей, поэтому могут получать доступ к Интернету как через ЗУИД и через КД, и для своей защиты почти все они имеют собственные ИТ-подразделения. Так что возлагать вину за их выбор или их "баги" (фичи), каким образом и который они получают доступ (ЗУИД и / или КД) на операторов / провайдеров лукаво и зря. В ряде ОГВ, как в нашем случае, существуют же "фичи" или ловушки для "желающих" на которые и напоролись так называемые ИТ-волонтеры…

В сообществе же некоторые ИБ-специалисты раскритиковали исследование за то, что большинство показанных примеров относятся к сервисам и зоне ответственности клиента, прямого отношения к КСЗИ и оператору связи не имеющего. Также критике подверглось отсутствие прямых доказательств того, что клиентам оказывалась именно услуга «защищенного доступа» к сети, как и то, что не приведено прямых доказательств, что предполагаемый вектор атаки через arp spoofing в конкретных сегментах оператора является рабочим…

В ответ же исследователи говорят: опубликовали только данные, в которых точно были уверены и убеждать никого не будут, ведь цель исследования - именно привлечь внимание к проблеме…» ***(Владимир Кондрашов. Исследование: Генпрокуратура, Минобразования и МИД могут пострадать от кібератак // Internetua (http://internetua.com/issledovanie-genprokuratura-minobrazovaniya-i-mid-mogut-postradat-ot-kiberatak-). 13.06.2019).***

***

«419 уязвимых устройств с возможностью удаленного доступа, множество устаревших серверов и открытых для записи папок обнаружили в рамках флешмоба #a27 украинские ИБ-эксперты в результате исследования сети провайдера «Датагруп». Среди клиентов провайдера, пренебрегающих собственной кибербезопасностью, оказались Укрзализныця, «Мотор Сич» и ряд других госучреждений и частных компаний.

Соответствующий отчет 18 июня, опубликовал один из участников флешмоба #a27, известный в сети под ником Lurca Tier…

Как прокомментировал нашему изданию уже опубликованные результаты исследования телеком-эксперт Игорь Дядюра, во многих подключенных к «защищенному» провайдеру госучреждениях считают, что одного такого подключения уже достаточно для обеспечения безопасности. На деле же клиенты таких провайдеров, как бизнес-структуры, так и обычные пользователи и госучреждения, во многих случаях игнорируют элементарные правила безопасности в сети.

Исследователи уже опубликовали информацию о проблемных клиентах в сетях таких защищенных провайдеров как «Адамант» и «Аксон 45», а в начале новой рабочей недели обнародовали сведения о проблемах у клиентов «Датагруп»…» ***(Владимир Кондрашов. У провайдера украинских властных и силовых структур клиенты имеют проблемы с кибербезопасностью // Internetua (http://internetua.com/u-provaidera-ukrainskih-vlastnyh-i-silovyh-struktur-klienty-imeuat-problemy-s-kiberbezopasnostua). 19.06.2019).***

***

«Телеком-сообщество переживает: гарантирована ли безопасность киберпространства страны? Массово стали выходить материалы на страницах фейсбук с хештегом #двадцатьсемь. Возникло много вопросов, что это такое, о чем речь? Почему оператор, который имеет сертификат КСЗИ, не может защитить информационную систему своего клиента?

Все началось с того, что ко многим государственным структурам начали поступать письма, в которых им предписывалось закупать услугу доступа к сети Интернет исключительно у оператора, который имеет в наличии сертификат КСЗИ (комплексная система защиты информации).

Начнем с того, что сама мысль потребления защищенного доступа к сети Интернет, уже попахивает несвежестью. Интернет это открытая публичная сеть.

Теперь разберем «типовые» атаки, которые могут быть нацелены на вас.

Например, вы распорядитель, создатель, хранитель информации (реестры, базы данных, и.т.д.) госпредприятия.

Вы получили письмо, где сказано, что вам предписано закупить сервис доступа к сети Интернет только через оператора, имеющего у себя КСЗИ, потому, что это безопасно для вашей информационной системы.

Покупая сервис доступа к сети Интернет, через оператора с аттестатом КСЗИ, у вас возникает заблуждение, что теперь ваша информационная сеть и информация в ней - защищены.

Я знаю прецеденты, когда сокращался ИТ персонал этих государственных предприятий!

Господа, хочу вас расстроить, при таком включении, КСЗИ относится к защите именно оператора. Оператор при создании КСЗИ, точно наведет у себя порядок, но это никак не касается ваших сетей!

Оператор этим подтвердил, что его система соответствует каким-то там «правилам» КСЗИ (определяется, модели угроз информации, модель защиты, определение программы испытаний, испытаний и.т.д.).

Пока мы работаем в текущем правовом поле, а в будущем (проект закона 9042) о защите информации в информационно-телекоммуникационных сетях, где вводится уже стандарты ISO/IEC 27001 (ДСТУ ISO/IEC 27001) – существенно ужесточит нормы безопасности.

Однако, оператор не защищает ВАШУ информационную систему. Для, вашей защиты, ваша система, должна иметь ваш соответствующий сертификат по безопасности КСЗИ.

Атаки могут быть активными, когда на ваш информационный ресурс через оператора идет внешняя атака DDoS. В этом случае, оператор сможет вас защитить от них (при наличии у него такого сервиса) ваши системы, но это не есть вопрос КСЗИ, это отдельный сервис.

Атака может быть на вашу информацию, когда атакующий в вашей системе находят внешнюю уязвимость, и далее производят какие-то действия с вашей информацией (удаление, изменение, управление, скажем атомным реактором, или насосной станцией), от таких атак, оператор вас не сможет защитить.

Это так же отдельный закупаемый сервис. Скажем SIEM, когда оператор сможет вам дать анализ видимых атак на вашу систему.

Может быть вариант, это когда вы разместили, в облаке оператора, или в датацентре оператора свою информацию. Вот тогда, конечно мы можем говорить о том, что оператор должен защитить в этом варианте сотрудничества вашу информацию.

Существует ошибочное мнение, некоторых клиентов оператора, что если его информация, передается с использованием канала Интернет оператора с сертификатом КСЗИ, то канал имеет криптованный (закодированный) уровень защиты. Это заблуждение.

Да, оператор может виртуализировать ваши каналы связи (VPN), это уже приведет к какой-то минимальной защите, но защита информации в канале, это уже непосредственно ваша ответственность, как распорядителя этой информации, если мы говорим об информации критического уровня, передаваемая между объектами

посредством сетей Интернет, она должна уже выходить от распорядителя зашифрованная…» ***(Александр Федиенко. Что вызвало бурю обсуждений проблем кибербезопасности в соцсетях // Internetua (http://internetua.com/csto-vyzvalo-burua-obsujdenii-problem-kiberbezopasnosti-v-socsetyah). 14.06.2019).***

***

«208 уязвимых сетевых устройств пользователей, которые можно использовать для атаки ARP спуфинга в диапазоне провайдера «Аксон 45» обнаружили украинские исследователи в рамках флешмоба #a27, направленного на исследование сетей провайдеров, которые построили по требованию Госспецсвязи так называемую комплексную систему защиты информации (КСЗИ) и получили Аттестат соответствия системы защиты защищенных узлов доступа.

Кроме уязвимых пользовательских устройств, исследователи обнаружили проблемы с безопасностью в ЖК «Gelios» в столице, незащищенную АТС и несколько интерфейсов веб-почты…

Уже опубликованные результаты исследования показывают: клиенты, подключившись к защищенному, по мнению ГСССЗИ, провайдеру, во многих случаях игнорируют элементарные правила безопасности. Это касается как бизнес-структур, обычных пользователей, так и госучреждений, для которых подключение к провайдеру с аттестатом соответствия системы защиты ЗУИД является обязательным…

В отчете ИБ-специалисты показали несколько «интересных» уязвимостей, демонстрирующих наплевательское отношение клиентов провайдера к безопасности. InternetUA приводит самые интересные примеры с комментариями из отчета.» ***(Владимир Кондрашов. У "рекомендованных" провайдеров клиенты оказались беззащитными перед взломом // Internetua (http://internetua.com/u-rekomendovannyh-provaiderov-klienty-okazalis-bezzasxitnymi-pered-vzlomom). 14.06.2019).***

***

«Во время обыска в известного украинского эксперта по кибербезопасности, ведущего разработчика компании «ИТ-Лаборатория» Александра Галущенко правоохранители изъяли оборудование и получили полный доступ к исходникам всех программных продуктов «ИТ-Лаборатории» стоимостью в десятки миллионов долларов…

Сегодня, 21 июня, около 6-30 утра в квартиру, где фактически проживает Александр Галущенко, с обыском пришли правоохранители. Они показали определение Печерского районного суда, вынесенное судьей В. Карабань о проведении обыска старшим следователем по особо важным делам ГСУ Нацполиции майором Лютым А.Б. и другими следователем группы (по данным нашего издания, в обыске также принимали участие сотрудники Департамента защиты экономики НПУ)…

Не смотря на определение суда, в котором прописано, что изыматься должны только носители информации, полицейские во время обыска, длившегося более

шести часов, изъяли также исходники всего программного обеспечения, разрабатываемого «ИТ-Лабораторией» на протяжении последних 9 лет, а также мастер-ключ, дающий правоохранителям полную свободу действий с ним.

Программное обеспечение, которое мы делаем, привязывается к «железу». В качестве привязки используются аппаратные ключи HASP, для программирования которых используется ключ-мастер. Они забрали этот ключ, хотя в постановлении говорилось о возможности изъятия носителей информации. Я объяснял им, что это не носитель информации, но мне сказали «экспертиза разберется». Они забрали исходники всех наших продуктов, которые мы делали с 2011 года и мастер-ключ к этому ПО. Стоимость изъятого имущества я оцениваю в десятки миллионов долларов, – рассказал Александр Галущенко…

Судя по определению суда, с которым пришли полицейские, во время обыска у одного из фигурантов другого уголовного дела в мобильном телефоне обнаружили переписку в мессенджере WhatsApp с пользователем «Алекс К», который, как сказано в определении «в дальнейшем оказался Александром Галущенко». В этой переписке мужчины якобы обсуждали «несанкционированное вмешательство в работу электронно-вычислительных машин, компьютерных сетей, сетей интернет связи» и «пытались по предварительному сговору получить доступ к почтовому ящику сотрудника правоохранительных органов». Судье такой аргументации оказалось достаточно для вынесения определения об обыске и изъятии носителей информации…

Отметим, что в Едином государственном реестре судебных решений в открытом доступе нет ни одного определения суда по делу, в рамках которого к ИБ-эксперту пришли правоохранители. Это довольно странно, учитывая, что в рамках этого уголовного производства, судя по определению, уже проводились обыски и даже были сообщения о подозрении его фигурантам.

На данный момент Александр Галущенко проходит в деле как свидетель. Адвокат Александра будет оспаривать изъятие техники в суде.

Тем временем в ИБ-комьюнити не исключают, что поводом для столь пристального внимания правоохранителей мог стать флэш-моб #двадцатьседьмое, инициатором которого был Александр Галущенко…» ***(Владимир Кондрашов. У ведущего украинского специалиста по кибербезопасности изъяли технику и программное обеспечение // Internetua (https://internetua.com/u-vedusxego-ukrainskogo-specialista-po-kiberbezopasnosti-iz-yali-tehniku-i-programmnoe-obespecsenie). 21.06.2019).***

***

Національна система кібербезпеки

«12 июня в Администрации президента Владимира Зеленского состоялось первое экспертное обсуждение концепции «Государство в смартфоне». В нем приняли участие представители «Коалиции электронного государства», объединяющей 65 различных организаций и экспертов в области IT, сообщает пресс-служба президента.

К обсуждению также присоединился глава государства…

По словам советника главы государства Михаила Федорова, переведение государственных услуг в онлайн поспособствует не только комфорту граждан, но и уменьшению коррупции.

«Наш план очень амбициозен. Например, до 2024 года мы стремимся перевести 90% всех государственных услуг в режим онлайн, втрое уменьшив количество взаимодействия граждан и бизнеса с властью и достигнув нулевого уровня коррупции в этой сфере», — заявил он…

Отметчается, что представители «Коалиции» предоставили президенту свои рекомендации и обсудили приоритетные проекты цифровизации.

Ключевые предложения касались развития инструментов электронного государства и демократии, цифровых инфраструктур, цифровой идентификации, кибербезопасности, наведение порядка в государственных реестрах, электронного народовластия (электронных социологических опросов и даже выборов).

Также говорилось о важности создания возможностей для украинских технологических стартапов.

Все эти задачи будут включены в единый план действий. Зеленский заверил, что такие встречи будут регулярными.

На следующей неделе запланирована серия обсуждений концепции «Государство в смартфоне» с участием международных доноров, представителей бизнеса и тому подобного. Затем документ будет обнародован в формате плана конкретных действий и ожидаемых целей…» ***(«Государство в смартфоне»: у Зеленского хотят к 2024 году перевести 90% госуслуг в онлайн // Капитал (https://www.capital.ua/ru/news/128796-gosudarstvo-v-smartfone-u-zelenskogo-khotyat-k-2024-godu-perevesti-90-gosuslug-v-onlayn). 13.06.2019).***

***

«Президент України Володимир Зеленський призначив секретаря Ради національної безпеки і оборони України Олександра Данилюка керівником Національного координаційного центру кібербезпеки.

Указ № 415 / 2019 про призначення Данилюка опублікований на офіційному сайті глави держави в середу, 19 червня.

«На зміну статті 2 Указу Президента України від 7 червня 2016 року № 242 Про Національний координаційний центр кібербезпеки призначити Данилюка … керівником Національного координаційного центру кібербезпеки», — йдеться в документі.» ***(Данилюк очолив Національний координаційний центр кібербезпеки // БлинКом (https://blin.mk.ua/news/105433). 20.06.2019).***

***

Правове забезпечення кібербезпеки в Україні

«Государственная служба специальной связи и защиты информации опубликовала проект постановления Кабинета Министров Украины «Об утверждении Протокола совместных действий основных субъектов

обеспечения кибербезопасности, субъектов киберзащиты и владельцев (распорядителей) объектов критической информационной инфраструктуры во время предупреждения, выявления, пресечения кибератак и киберинцидентов, а также при устранении их последствий»…

Проект постановления Кабмина подготовлен Администрацией Госспецсвязи на выполнение Решения СНБОУ от 29 декабря 2016 «Об угрозах кибербезопасности государства и неотложные меры по их нейтрализации» и Плана мероприятий на 2017 год по реализации Стратегии кибербезопасности Украины.

Протокол совместных действий основных субъектов обеспечения кибербезопасности, субъектов киберзащиты и владельцев (распорядителей) объектов критической информационной инфраструктуры во время предупреждения, выявления, пресечения кибератак и киберинцидентов, а также при устранении их последствий определяет:

- перечень взаимосвязанных во времени и по целям обязательных действий основных субъектов обеспечения кибербезопасности, субъектов киберзащиты и владельцев (распорядителей) объектов критической информационной инфраструктуры во время предупреждения, выявления, пресечения кибератак и киберинцидентов и устранения их последствий;

- фазы взаимодействия при предупреждении, выявлении, пресечении кибератак и киберинцидентов и устранения их последствий;

- основных субъектов обеспечения кибербезопасности по выполнению действий, установленных настоящим Протоколом.

Как отметил телеком-эксперт, юрист Юрий Котляров, проектом устанавливается перечень полномочий и обязанностей на каждой фазе взаимодействия, но именно о порядке взаимодействия речь пока не идет.

Проект Постановления уже согласован без замечаний ГФС, Минсоцполитики, Госфинмониторингом, ГМС , СВР, Мининфраструктуры, Государственным агентством по вопросам электронного правительства Украины, Минрегионом, Минобороны и СБУ. Генеральным штабом ВСУ, Минэкономразвития, МИД и МВД согласован проект Постановления с замечаниями, которые учтены частично. Минэнергоугля согласован проект Постановления с замечанием, которое не учтено.

Замечания и предложения к проекту акта принимаются в течение месяца с даты его обнародования.» ***(Владимир Кондрашов. Кибератаки на Украину будут отражать по новой методике // Internetua (http://internetua.com/kiberataki-na-ukrainu-budut-otrajat-po-novoi-metodike). 07.06.2019).***

***

«Постановою Кабінету Міністрів України № 518 затверджено Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури. Рішення прийняте на виконання вимог Закону України «Про основні засади забезпечення кібербезпеки України».

Кіберзахист об’єкта критичної інфраструктури є складовою частиною робіт із створення (модернізації) та експлуатації об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Заходи з кіберзахисту

передбачаються та впроваджуються на всіх стадіях життєвого циклу об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

Кіберзахист об’єкта критичної інфраструктури забезпечується власником та/або керівником об’єкта критичної інфраструктури відповідно до цих Загальних вимог та законодавства в сфері захисту інформації та кібербезпеки.

У випадку, якщо на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, положення цих Загальних вимог повинні бути враховані під час створення (модернізації) на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури комплексної системи захисту інформації, а їх відповідність перевіряється під час її державної експертизи в сфері технічного захисту інформації.

Створення комплексної системи захисту інформації об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та її державна експертиза здійснюються відповідно до вимог законодавства в сфері захисту інформації та охорони державної таємниці.

Власник та/або керівник об’єкта критичної інфраструктури організовує невідкладне інформування урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA (у разі наявності — галузевої команди реагування на комп’ютерні надзвичайні події), а також функціонального підрозділу контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління СБУ (Ситуаційний центр забезпечення кібербезпеки СБУ) або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

Державні органи отримують доступ до Інтернету через систему захищеного доступу державних органів до Інтернету Державного центру кіберзахисту, через операторів, провайдерів телекомунікацій, які мають захищені вузли доступу до глобальних мереж передачі даних із створеними комплексними системами захисту інформації з підтвердженою відповідністю, або через власні системи захищеного доступу до Інтернету із створеними комплексними системами захисту інформації з підтвердженою відповідністю. Ця вимога не поширюється на інформаційно-телекомунікаційні системи закордонних дипломатичних установ України.

Державні органи з метою здійснення захищеного інформаційного обміну, зберігання резервних копій інформаційних ресурсів, підключення до системи захищеного доступу державних органів до Інтернету Державного центру кіберзахисту використовують ресурси Національної телекомунікаційної мережі.

Організаційні та технічні заходи з кіберзахисту, які впроваджуються на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, повинні забезпечувати:

– формування на об’єкті критичної інфраструктури загальної політики інформаційної безпеки;

– управління доступом користувачів та адміністраторів до об’єктів захисту об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

– ідентифікацію та автентифікацію користувачів та адміністраторів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

– реєстрацію подій компонентами об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та їх періодичний аудит тощо.

Міністерства та інші центральні органи виконавчої влади можуть розробляти конкретизовані вимоги з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування об’єктів критичної інфраструктури, які відносяться до сфери їх управління. Такі вимоги з кіберзахисту погоджуються з Адміністрацією Держспецзв’язку.

СБУ має право подавати міністерствам та іншим центральним органам виконавчої влади обов’язкові для розгляду пропозиції щодо таких вимог з кіберзахисту.

Також затверджено Перелік базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури.» ***(Уряд затвердив загальні вимоги до кіберзахисту // Українське право (http://ukrainepravo.com/news/ukraine/uryad-zatverdyv-zagalni-vymogy-do-kiberzakhystu/). 24.06.2019).***

***

«Кабинет Министров Украины принял постановление, которым, среди прочего, обязал на объектах критической инфраструктуры устанавливать средства сетевой защиты, которые как минимум защищают от атак «нулевого дня», то есть от уязвимостей ПО, которые ещё не известны пользователям и разработчикам программного обеспечения и против которых не существует механизмов защиты…

На прошлой неделе во исполнение требований закона «Об основах обеспечения кибербезопасности Украины» Кабинет Министров принял постановление «Об утверждении Общих требований к киберзащите объектов критической инфраструктуры». Согласно документу, общие требования определяют организационно-методологические, технические и технологические условия киберзащиты объектов критической инфраструктуры, являются обязательными к выполнению предприятиями, учреждениями и организациями, которые в соответствии с законодательством отнесены к объектам критической инфраструктуры. Сам документ разрабатывался в Администрации Государственной службы специальной связи и защиты информации.

ИБ-эксперт,организатор конференции по практической кибербезопасности NoNameCon Владимир Стыран проанализировал документ и обнаружил в нем множество проблем.

Чтиво похоже на пробу пера студента-третьекурсника, которому поручили написать его первую политику информационной безопасности. Хотя нет, скорее трех студентов, ведь текст местами совершенно несовместим. Состоит из более или менее предсказуемых тезисов, скопированных из различных источников нормативки, и переформулированных в лучших традициях украинского

законодательства (то есть, можно язык сломать). Но у него при этом каким-то образом попали не то, что непрофессиональные, а откровенно идиотские требования и очевидные даже невооруженному глазу коррупционные риски, – комментирует Владимир Стыран в своей публикации на Medium. – Этот документ невозможно выполнить, не остановив и не разрушив процессы в организации. Поэтому, если вам повезло, и вас внесли в перечень объектов критической инфраструктуры, готовьтесь. В ближайшее время у вас или исчезнет работа как таковая, или вам придется выполнять ее с грубыми нарушениями «общих требований» и под постоянной угрозой наказания.

Защита от атак «нулевого дня»

Особенно запоминается пункт 26 Перечня базовых требований по обеспечению киберзащиты объектов критической инфраструктуры, в котором указано, что «в случае невозможности физического разделения внешней сети и объекта критической информационной инфраструктуры объекта критической инфраструктуры на границе (периметре) между внешними сетями, другими информационно-телекоммуникационными системами, обслуживающими объект критической инфраструктуры, и объектом критической информационной инфраструктуры объекта критической инфраструктуры должны быть установлены средства сетевой защиты, выполняющих минимум следующие функции защиты: защита от атак "нулевого дня" (уязвимости программного обеспечения, которые еще неизвестны пользователям или разработчикам программного обеспечения и против которых еще не разработаны механизмы защиты), выявление злонамеренного кода и вредоносных программ».

Уязвимость нулевого дня, согласно определению — это неустраненная уязвимость, а также вредоносные программы, против которых еще не разработаны защитные механизмы. Этот термин означает, что у разработчиков было 0 дней на исправление дефекта: уязвимость или атака становится публично известна до момента выпуска исправлений производителем ПО (то есть потенциально уязвимость может эксплуатироваться на работающих копиях приложения без возможности защититься от нее). Одной из самых известных вредоносных программ, использующих 0day уязвимость, является червь Stuxnet, который был обнаружен летом 2010 года. Stuxnet использовал ранее неизвестную уязвимость ОС семейства Windows, связанную с алгоритмом обработки ярлыков.

"Как минимум, защитите все от zero-day". Это нонсенс по определению. Разве что, как метко заметили некоторые из коллег, это «заточка» под отдельные «решения безопасности», которые нагло хвастаются такими фичами в своих рекламных презентациях, – отмечает Владимир Стыран…

Если приведенный выше пример может свидетельствовать о желании Кабмина и ГСССЗИ защитится от неизвестных миру атак с помощью постановления, то другие нормы, прописанные в документе уже заставляют задуматься.

В частности, в пункте 2 Общих требований в определении критических бизнес/операционных процессов объекта критической инфраструктуры указано, что это процессы, реализация угроз на которые приведет, среди прочего, к причинению имущественного вреда.

Как я неоднократно подчеркивал, критическая инфраструктура это то, без чего мы умрем, и то, что может нас убить. Это высшая форма зависимости общества и государства. Поэтому говорить, что критическими мы считаем процессы, реализация угроз на которые может причинить нам имущественный вред, – это осуществить инфляцию слова «критический» во всех определениях вокруг понятия критической инфраструктуры. Таким образом, все становится критическим, а, следовательно, критическим не остается ничего. И это не ошибка, дальше в "требованиях" этот дух сохраняется до конца документа, – комментирует Владимир Стыран.

Кроме того, в документе почему-то упоминается и оценка рисков: «Техническое задание формируется по результатам оценки рисков, которые указываются в отчете по результатам оценки рисков на объекте критической информационной инфраструктуры объекта критической инфраструктуры. Методической основой для оценки рисков на объекте критической информационной инфраструктуры объекта критической инфраструктуры является стандарт ISO / IEC 27005».

В чем смысл слова «критический», если у объекта, который оно характеризует, остается пространство для дальнейшей оценки? Это вновь возвращает нас к мысли, что объекты критической инфраструктуры не так уж критичны. Скорее всего, в список запихнули все, что стоит защищать. Вместо того, чтобы провести оценку рисков и сформировать список, в котором только критические объекты, эту оценку рисков требуют от их владельцев пост фактум, – комментирует эксперт…

Также в утвержденных Кабмином Общих требованиях прописана обязанность владельца и / или руководителя объекта критической инфраструктуры организовать безотлагательное информирование правительственной команды реагирования на компьютерные чрезвычайные события Украины CERT-UA, а также Ситуационный центр обеспечения кибербезопасности СБУ о киберинцидентах и кибератаках, касающихся объекта критической информационной инфраструктуры объекта критической инфраструктуры. Тем не менее, наказания за сокрытие инцидентов не устанавливается.

В документе также прописано наличие на ОКИ подразделения или должностного лица, отвечающего за политику информационной безопасности, принятую на объекте критической инфраструктуры, и контроль за ее соблюдением. Однако, на что также указывали в телеком- сообществе, никакой, собственно, ответственности этого должностного лица и наказания, в случае инцидента, произошедшего по его вине, документ не предусматривает.

Более того, при назначении ответственного за кибербезопасность специальное образование, согласно «Перечню базовых требований», не является обязательным. В документе указано, что людям предпочтение должно отдаваться лицам, имеющим специальное образование и опыт работы в сфере технической защиты информации или информационной безопасности.

Идея это откровенно идиотская, в сетях такого рода пикнуть боятся, не то что пентесты делать. Способы и методы оценки защищенности таких сетей – это

отдельная дисциплина. Но это надо было сделать домашнюю работу и изучить вопрос. Авторы "требований" этого делать не стали, – комментирует Стыран…

Также в принятом Камином документе имеется требования подключать ОКИ к интернету только у провайдеров, построивших Комплексную систему защиты информации. Дело в том, что в пункте 37 Перечня базовых требований указано, что «к глобальным сетям передачи данных, в частности Интернету, объекты критической информационной инфраструктуры объекта критической инфраструктуры должны подключаться через тех операторов, провайдеров телекоммуникаций, у которых имеются защищенные узлы доступа к глобальным сетям передачи данных с созданными комплексными системами защиты информации с подтвержденным соответствием». Далее в этом же Перечне говорится, что «для обеспечения отказоустойчивости объекта критической информационной инфраструктуры объекта критической инфраструктуры» связь с Интернетом должна обеспечиваться с использованием двух и более каналов передачи данных, предоставляемых различными операторами сети передачи данных.

То есть, два провайдера с КСЗИ. Масштаб растет! – иронизирует Владимир Стыран…

«Ужасно, ничтожно и обидно. Пример обнаглевшей некомпетентности в государственных учреждениях», – именно так охарактеризовал документ организатор конференции по практической кибербезопасности NoNameCon.

– У авторов требований была одна задача: взять мануал по защите критической инфраструктуры от американского института NIST (Cyber Security Framework) (который, кстати, уже год доступен бесплатно в переводе на украинский, благодаря местному представительству компании Cisco) и развернуть его с использованием нормативки, которая авторам доступна: ISO 27000, NIST, Cobit или даже CIS. Но "в Украины свой путь", – резюмирует Владимир Стыран в комментарии нашему журналисту.

Эксперт объясняет: такие документы должны перед утверждением выноситься на суд общественности. В данной же ситуации общественности остается только читать принятое постановление и делать выводы.» ***(Владимир Кондрашов. Кабмин обязал объекты критической инфраструктуры отражать атаки «нулевого дня» // Internetua (https://internetua.com/kabmin-obyazal-ob-ekty-kriticseskoi-infrastruktury-otrajat-ataki-nulevogo-dnya). 24.06.2019).***

***

Кібервійна проти України

«Національний банк 18 червня перебував під зовнішньою DDoS атакою. Через це офіційний сайт Національного банку тимчасово працює у обмеженому режимі.

Про це повідомляє прес-служба НБУ.

«Критично важлива електронна інфраструктура Національного банку працює в звичайному режимі. У тому числі – система електронних платежів, якою

користуються банки; електронна пошта та внутрішня комп'ютерна мережа НБУ», – йдеться у повідомленні…» ***("Хакнули": Нацбанк зазнав кібератаки - сайт працює в обмеженому режимі // Голос Карпат (https://goloskarpat.info/business/5d09414465555/?utm_content). 18.06.2019).***

***

Боротьба з кіберзлочинністю в Україні

«Безработного украинца осудили на три года лишения свободы с испытательным сроком в один год за взлом и продажу ворованных аккаунтов в сервисе дистрибуции игр Steam…

Согласно материалам дела, безработный уроженец Черниговской области с июля по декабрь 2018 года, «путем преодоления систем логической защиты автоматизированной системы «Steam», используя данные для авторизации в качестве администратора аккаунта», получал доступ к панели администрирования аккаунтов в сервисе и менял у них идентификационные данные. Получив таким образом контроль над взломанным кабинетом пользователя в Steam, злоумышленник в дальнейшем продавал учетную запись на одном из «хакерских форумов».

Всего следствию удалось доказать четыре эпизода взлома и продажи злоумышленником чужих аккаунтов в Steam.

Кроме этого, полицейские обнаружили, что житель Чернигова, кроме продажи аккаунтов, занимался также распространением вредоносного программного обеспечения. Так, в конце декабря прошлого года мужчина с помощью мессенджера Telegram переслал другому пользователю вредоносную программу CLIPPER.exe. Её основная функция – подмена номеров электронных кошельков платежных систем Qiwi, Webmoney, а также целого ряда криптовалют (Bitcoin, Monero, zCash, DOGE, DASH, Etherium, Blackcoin и Litecoin) в буфере обмена операционной системы пораженного компьютера на номер электронного кошелька, который был указан лицом, его распространившим, в результате чего средства, которые перечисляются, попадают на счет последнего.

В судебном заседании обвиняемый ОСОБА_1 свою вину по предъявленному ему обвинению по ч.1 ст. 361, ч.2 ст. 361 («Несанкционированное вмешательство в работу ЭВМ»), ч. 1 ст. 361-1 («Распространение и сбыт вредоносного ПО») УК Украины признал полностью, подтвердив обстоятельства, изложенные в обвинительном акте и отметил, что в содеянном искренне раскаивается.

В результате, суд признал мужчину виновным в предъявленном ему обвинении и приговорил к наказанию в виде трех лет лишения свободы. Этим же решением суд освободил обвиняемого от отбывания наказания с испытательным сроком один год. Кроме этого, взломщик заплатит 5720 гривен за проведенные судебные экспертизы.» ***(Владимир Кондрашов. Украинец получил три года за продажу взломанных аккаунтов в Steam // Internetua (http://internetua.com/ukrainec-polucsil-tri-goda-za-prodaju-vzlomannyh-akkauntov-v-steam). 05.06.2019).***

***

«Хакери створювали віруси типу криптомайнер та «stealer», а двоє українців збували їх на закритих хакерських форумах, отримуючи за це відсоток від продажу. Для анонімізації платежів зловмисники використовували російські платіжні системи.

Працівники Причорноморського управління кіберполіції спільно зі слідчими поліції Одещини, за процесуального керівництва Одеської місцевої прокуратури №3, викрили мешканця Запоріжжя та Одеси у змові для поширення шкідливих програмних засобів.

Створені шкідливі програми використовувалися у середовищі операційних систем під управлінням Windows для майнінгу криптовалют. Крім того, користувачі цих шкідливих програм мали можливість втручатися в роботу комп'ютерів та копіювати персональну і білінгову інформацію власників вражених комп'ютерів. Серед таких даних – логіни, паролі, файли cookie, дані щодо гаманців криптовалют, доступи до онлайн банкінгу тощо.

За місцем мешкання учасників групи проведено санкціоновані обшуки, в ході яких вилучено комп'ютерну техніку, яка використовувалась для проведення злочинної діяльності. Під час попереднього огляду вилученої техніки, спеціалісти з кіберполіції виявили різноманітне шкідливе програмне забезпечення. Також виявлено листування зловмисників з користувачами хакерських форумів, через які вони продавали шкідливе програмне забезпечення.

Вирішується питання щодо оголошення підозри одному із учасників цієї злочинної групи. Його спільнику – мешканцю Одеси – вже повідомлено про підозру у вчиненні кримінального правопорушення, кваліфікованого за ст. 361-1 КК України (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут).Обвинувальний акт вже скеровано до суду. Спільникам загрожує до 5 років ув'язнення…» ***(Кіберполіція викрила злочинну групу у співпраці з російськими хакерами // Internetua (https://internetua.com/kiberpoliciya-vikrila-zlocsinnu-grupu-u-spivpraci-z-rosiiskimi-hakerami). 24.06.2019).***

***

«…Працівники Київського управління кіберполіції спільно зі слідчими поліції Київщини, за процесуального керівництва прокуратури Київщини, затримали 24 річного киянина у втручанні в роботу Державних реєстрів Міністерства юстиції України. Зловмисник маючи у користуванні ключі доступу до реєстрів, за гроші проводив незаконну перереєстрацію майна на підставних осіб.

Кіберполіція встановила: молодик зі своїм спільником, який наразі перебуває на тимчасово окупованій території, реєстрував без відома власників їх приміщення на підставних осіб. Серед таких об'єктів житлові та нежитлові приміщення, автозаправочні станції тощо. Так, нещодавно поліцейські зафіксували, що зловмисники перереєстрували на підконтрольні підприємства один зі столичних житлових комплексів. Тоді, сума збитків сягала більш як 16 мільйонів гривень.

Точна сума збитків та кількість потерпілих будуть встановлені після проведення всіх необхідних слідчих дій…

Киянину вже оголошено підозру за ст.361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України та ч.3 ст.206-2 (Протиправне заволодіння майном підприємства, установи, організації) КК України. Його арештовано з можливістю внесення застави у 778 тисяч гривень.

Крім того одному співучаснику, який перебуває на тимчасово окупованій території, вирішується питання про оголошення заочної підозри у вчиненні злочинів та оголошення його в розшук, а відносно інших осіб проводяться додаткові заходи спрямовані на їх затримання.

Спільникам загрожує до 10 років ув'язнення.» ***(Кіберполіція викрила «чорних» реєстраторів у втручанні в державні бази даних // Департамент кіберполіції України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-chornyx-reyestratoriv-u-vtruchanni-v-derzhavni-bazy-danyx-8847/). 27.06.2019).***

***

Міжнародне співробітництво у галузі кібербезпеки

«…Секретар Ради національної безпеки і оборони України Олександр Данилюк провів зустріч з тимчасово повіреним у справах США в Україні Крістіною Квін, під час якої сторони обговорили стан і перспективи реформування сектору безпеки і оборони України та питання розширення двостороннього співробітництва зі США, зокрема, і питання аудиту ДК "Укроборонпром"…

"Серед пріоритетів у роботі РНБО України секретар Ради назвав воєнну реформу, а також реформування ДК "Укроборонпром", постачання якісної зброї та техніки для української армії, енергетичну безпеку, кібербезпеку, реформу СБУ та розвідувальних органів", - вказали у прес-службі РНБО.

Торкаючись зовнішньополітичних викликів, які можуть загрожувати безпеці України, Данилюк заявив, що "РНБО України має стати майданчиком, що здатен оперативно реагувати на всі можливі проблеми"…» ***(Юлія Шрамко. Данилюк обговорив з тимчасово повіреною у справах США аудит "Укроборонпрому" // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1807113-danilyuk-obgovoriv-z-timchasovo-povirenoyu-u-spravakh-ssha-audit-ukroboronpromu). 14.06.2019).***

***

«Міжпарламентська асамблея Верховної Ради України, Сейму Литовської Республіки та Сейму і Сенату Республіки Польща (МПА) створила комітет з питань безпеки… про це голова Верховної Ради України Андрій Парубій заявив на брифінгу разом з головою Сеймасу Литви Вікторасом Пранцкєтісом та маршалком Сенату Польщі Станіславом Карчевським. Спільний

брифінг відбувся в рамках X сесії МПА «Безпека. Розвиток. Демократія. Сильні разом», яка проходить 7-8 червня 2019 року у Києві. Голова Верховної Ради повідомив, що на сесії МПА було оголошено про створення додаткового, четвертого, комітету у структурі Міжпарламентської асамблеї Литва-Польща-Україна – комітету з питань безпеки. «Ми узгодили, що координація наших дій з питань безпеки є важливою і актуальною, оскільки гібридні виклики, що стоять перед нашими країнами в обороні від російської агресії, є подібними і спільними: зокрема, це інформаційна безпека, це кібербезпека, енергетична безпека, гуманітарна безпека», — сказав він. Парубій підкреслив, що безпека у сьогоднішньому світі — це не тільки зброя і танки – це дуже широкий спектр питань…». ***(Міжпарламентська асамблея України, Литви та Польщі створила комітет з питань безпеки // EconomistUA (https://economistua.com/mizhparlamentska-asambleya-ukrayini-litvi-ta-polshhi-stvorila-komitet-z-pitan-bezpeki/). 09.06.2019).***

***

«Сьогодні успішна атака хакерів може не лише зашкодити онлайн-ресурсам, а й загрожувати національній безпеці та стабільності цілої країни. Інструменти кіберпростору постійно розвиваються, а кіберзахист вже давно став одним із пріоритетних напрямів діяльності НАТО…

Альянс активно розробляє шляхи, які допоможуть убезпечити та зміцнити не лише власну обороноздатність, а й партнерів. Для цього проводять інтерактивні заходи та навчання. Допомагають запровадити їх і в країнах, що є партнерами Альянсу.

Цілі НАТО: захистити національний інформаційний простір та підвищити обороноздатність армії, а також навчитися протидіяти атакам хакерів та знайти інноваційні шляхи розвитку збройних сил. НАТО постійно розвиває та реформує свої інформаційні системи, використовуючи при цьому різні концепції. Однією з таких є хакатон.

Що таке хакатон?Це змагання між групами фахівців з розробки програмного забезпечення. За обмежений час вони мають знайти інноваційне рішення у галузі безпеки та оборони. Після того вони презентують результати своєї роботи, а професійне журі їх оцінює…» ***(Фахівці НАТО вчать українців протистояти кіберзагрозам за допомогою змагань // Телеканал новин «24» (https://24tv.ua/fahivtsi_nato_vchat_ukrayintsiv_protistoyati_kiberzagrozam_za_dopomogoyu_zmagan_n1163199). 06.06.2019).***

***

«НАТО виділить понад 40 мільйонів євро на підтримку України, зокрема, у сфері кіберзахисту.

Про це заявив Генеральний секретар НАТО Єнс Столтенберг…

«Через десять трастових фондів союзники і партнери по НАТО зобов'язалися виділити понад 40 мільйонів євро на підтримку України. У таких областях, як командування та управління, кіберзахист і медична реабілітація», — сказав Генсек НАТО напередодні на прес-конференції з Президентом України Володимиром

Зеленським…» ***(НАТО виділить Україні 40 млн євро на кібербезпеку і медичну реабілітацію // Високий Замок Online (https://wz.lviv.ua/news/391735-nato-vydilyt-ukraini-40-mln-ievro-na-kiberbezpeku-i-medychnu-reabilitatsiiu). 05.06.2019).***

***

«Конгресмени представили у Палаті представників проект закону "Про надання підтримки Україні для захисту її незалежності, суверенітету і територіальної цілісності"…

Документ спрямований на посилення обороноздатності України шляхом передачі озброєнь, продажу летальних оборонних засобів, а також зміцнення спроможності України протистояти російським кібератакам.

Законопроект передбачає можливість надання Україні статусу головного союзника США поза НАТО до вступу до Північноатлантичного альянсу. Такий статус може бути використаний для спрощення процедури передачі Україні оборонних засобів…

Співавторами законопроекту виступили керівники комітету із закордонних справ, конгресмен-демократ Еліот Енгель та республіканець Майкл Маккол, а також голова та співголова підкомітету щодо Європи, Євразії, енергетики і довкілля даного комітету, демократ Віліам Кітінг та республіканець Адам Кінзінгер.» ***(Україна може отримати статус головного військово-політичного союзника США // Інформаційне агентство «1NEWS» (https://1news.com.ua/svit/ukrayina-mozhe-otrymaty-status-golovnogo-vijskovo-politychnogo-soyuznyka-ssha.html). 03.06.2019).***

***

«В понедельник Израиль заявил, что присоединился к Партнерству по цифровому развитию (DDP) Всемирного банка в целях содействия цифровизации и кибербезопасности в развивающихся странах.

Присоединившись к партнерству, Израиль впервые объединит усилия с мировым сообществом разработчиков из Японии, Великобритании, Финляндии, Дании и Норвегии и такими организациями, как GSMA (торговая организация, представляющая интересы операторов мобильных сетей по всему миру), с тем, чтобы оказывать техническую помощь странам Африки, Латинской Америки, Восточной Европы и Азии и повышать их устойчивость к кибербезопасности.

В рамках соглашения со Всемирным банком Израиль внесет один миллион долларов в многосторонний целевой фонд партнерства, чтобы получить доступ к общей информации и событиям. Параллельно Израиль будет предоставлять своим предпринимателям и ученым возможность давать советы и делиться своими знаниями с развивающимися странами.» ***(Израиль вступает в партнерство со Всемирным банком // ISRAland Online (http://www.isra.com/news/231256). 17.06.2019).***

***

«Компания Acronis анонсировала проведение своей первой международной конференции по киберзащите - Acronis Global Cyber Summit,

которая пройдет в отеле Fontainebleau в Майами, штат Флорида, с 13 по 16 октября. В конференции примут участие партнеры компании со всего мира, разработчики программного обеспечения и ученые для обсуждения проблем совершенствования защиты критически важных информационных активов и систем крупных компаний и малых предприятий.

На конференции будут представлены доклады ряда ведущих экспертов, включая Роберта Эрьявека, выдающегося специалиста в сфере кибербезопасности и ведущего телешоу Shark Tank, удостоенного премии Emmy, Эрика О'Нила, бывшего оперативного сотрудника FBI и автора ряда книг, а также Керен Элазари, всемирно признанного аналитика в области безопасности…

Современные компании сталкиваются с постоянно меняющимся и развивающимся комплексом угроз в отношении своих данных. С 2015 по 2018 год объемы данных, которыми должны управлять предприятия, увеличились с 1,45 до 9,70 петабайт. В то же самое время глобальные убытки от киберпреступности достигли 600 млрд долларов в год. При этом традиционные системы защиты данных и решения, направленные на обеспечение кибербезопасности, всё хуже справляются с задачей противостояния современным угрозам, что подвергает немалому риску множество организаций по всему миру.

Компания Acronis продвигает идею по интеграции технологий защиты данных и кибербезопасности с целью создания системы полной киберзащиты , обеспечивающей сохранность, доступность, конфиденциальность, подлинность и безопасность данных (SAPAS - Пять векторов киберзащиты). На конференции Acronis эта стратегическая концепция будет поставлена в центр внимания экспертов и лидеров индустрии, которые попытаются определить, каким образом можно обеспечить более эффективную киберзащиту всех данных, приложений и систем.

Для создания более крупной экосистемы, обеспечивающей киберзащиту на основе принципов SAPAS, компания Acronis недавно предоставила доступ сторонним разработчикам к платформе Acronis Cyber Platform. Доступ к этой платформе, который будет предоставлен всем участникам международной конференции по киберзащите Acronis Global Cyber Summit, обеспечивает расширенную поддержку решения для защиты данных и позволяет разрабатывать новые приложения таким образом, чтобы разработчики могли использовать функции и интегрировать своих приложения в масштабной экосистеме Acronis.

Помимо докладов экспертов мирового класса, руководителей и партнеров компании Acronis, на конференции также будут представлены эксклюзивные обучающие лекции для партнеров, уникальные возможности для встреч, направленные на налаживание и укрепление деловых связей, консультации для клиентов и партнеров, а также заседания, посвященные новейшим открытиям в сфере киберзащиты и решениям, предоставляемым компанией Acronis…» ***(Acronis проведет глобальный саммит по киберзащите // Компьютерное Обозрение (https://ko.com.ua/acronis_provedet_globalnyj_sammit_po_kiberzashhite_129087). 13.06.2019).***

***

«Українські офіцери-зв'язківці успішно відпрацювали понад 20 спільних тестів на досягнення взаємосумісності з системами кібернетичної безпеки членів НАТО та країн-партнерів в межах "CWIX-2019".

Про це повідомляє прес-центр Міноборони.

На спільних навчаннях у Польщі українці отримали цінний досвід використання сучасних технологій для підтримки кібербезпеки. Вони продемонстрували високий професіоналізм та організованість під час виконання спільних завдань.» ***(Українські зв'язківці беруть участь у навчаннях НАТО "CWIX-2019" // UATV (https://uatv.ua/ukrayinski-zv-yazkivtsi-berut-uchast-u-navchannya-nato-cwix-2019-foto/). 24.06.2019).***

***

Світові тенденції в галузі кібербезпеки

«Компания Foregenix проанализировала 9 миллионов интернет-магазинов по всему миру на степень уязвимости перед кибератаками. В результате исследования выяснилось, что в зоне повышенной опасности находятся более полумиллиона сайтов.

Около 200 тысяч проверенных ресурсов работают на базе CMS Magento. По результатам проверок около 87% из них были отнесены к категории высокого риска. На таких сайтах были обнаружены серьезные проблемы безопасности с оценкой 7 и более баллов по шкале CVSS 3.0. Также результаты исследования показывают, что с октября прошлого года доля уязвимых Magento-сайтов увеличилась почти на 7 п. п.

Исследователи выяснили, что злоумышленники успешно атаковали более 1700 торговых площадок и внедрили на них вредоносное ПО для сбора платежных данных. Большинство скомпрометированных сайтов работают на базе Magento, около 60% из них зарегистрированы в Северной Америке. Второй регион по количеству пострадавших онлайн-ресурсов — Европа.

Согласно данным исследования, на сайтах под управлением Magento чаще всего встречаются зловреды, которые крадут платежные данные. Часть из них внедряется с помощью Javascript-загрузчика, в других случаях скрипт напрямую внедряется на страницы сайта. Также преступники использовали ПО для сбора финансовой информации, которое маскируется при помощи полиморфного кода загрузчика, и вредоносные скрипты, создающие специальные фреймы. В некоторых случаях злоумышленники внедряли на сайт криптомайнер.

Помимо уязвимостей Magento, киберпреступники проявляют все больший интерес к атакам на цепочку поставок, которые могут затронуть в том числе и SaaS-платформы, такие как Shopify, BigCommerce и Magento Enterprise Cloud Edition…» ***(Dmitry Nazarov. Полмиллиона онлайн-магазинов уязвимы для кибератак // Threatpost (https://threatpost.ru/half-million-online-stores-are-vulnerable-to-cyberattacks/33045/). 12.06.2019).***

***

«Подавляющее большинство утечек корпоративных данных из облаков (около 90%) происходит из-за человеческих ошибок, спровоцированных с помощью социальной инженерии, а не из-за проблем, возникающих на стороне облачных провайдеров. Такой результат получила «Лаборатория Касперского» после проведения соответствующего опроса среди 6614 IT-специалистов из 29 стран по всему миру.

Использование облачной IT-инфраструктуры позволяет компаниям сделать бизнес-процессы более гибкими, сократить капитальные затраты и повысить скорость предоставления IT-услуг, но у организаций возникают опасения насчёт того, насколько безопасно хранить данные в облаках. Почти 33% из опрошенных глобально компаний выказывают беспокойство по поводу возможных киберинцидентов в IT-инфраструктуре, управляемой сторонним поставщиком: в случае утечки преимущества облачных сред померкнут на фоне коммерческого и репутационного ущерба для бизнеса.

Тем не менее, несмотря на то что компании обеспокоены целостностью и надёжностью внешних облачных платформ, киберинциденты в этих средах, как раз наоборот, чаще происходят из-за внутренних причин. Так, лишь каждая десятая (11%) утечка данных из облака стала возможной из-за тех или иных действий провайдера, в то время как треть всех киберинцидентов в облаке произошла из-за доверчивости сотрудников компании, попавшихся на приемы социальной инженерии.

Лишь около 47% респондентов внедрили специализированные решения для защиты облачной инфраструктуры. Возможно, руководители считают, что ответственность за защиту облачных сервисов лежит на поставщике, либо пребывают в ложном убеждении, что защитные решения для конечных устройств способны оградить от угроз также и облачные среды.

Важным шагом в принятии решения о переносе данных в публичное облако является понимание того, кто будет отвечать за безопасность хранящихся в нём корпоративных данных. Облачные провайдеры обычно принимают меры кибербезопасности, чтобы защитить платформы и клиентов, но они не могут нести ответственность за угрозы, возникающие на стороне клиента. Проведенный опрос показал, что компаниям нужно обратить пристальное внимание на вопросы повышения цифровой грамотности среди сотрудников и принять меры, которые позволят защитить облачную среду от возможных ошибок.

Минимальные требования для обеспечения безопасности данных, хранящихся в облаке из тех, что необходимы компаниям в первую очередь:

– обучать сотрудников основам информационной безопасности, например;

– определить процедуры покупки и использования облачной инфраструктуры для каждого департамента, чтобы минимизировать риск несанкционированного применения облачных платформ;

– после перехода на облако установить специализированное защитное решение для облачной инфраструктуры с унифицированным управлением безопасностью из единой консоли, которое позволяет без ущерба для производительности оградить рабочие нагрузки от самых сложных известных и неизвестных угроз и защищает всю облачную инфраструктуру — от платформ

виртуализации до публичных облаков.» ***(9 из 10 утечек данных из облаков происходит из-за человеческого фактора // Компьютерное Обозрение (https://ko.com.ua/9_iz_10_utechek_dannyh_iz_oblakov_proishodit_iz-za_chelovecheskogo_faktora_129034). 10.06.2019).***

***

«Наиболее уязвимыми для атак на информационную безопасность компьютерной системы являются крупные мировые производители программного обеспечения, такие как Microsoft, Apple, Google, Oracle.

Об этом в ходе круглого стола сообщил старший консультант отдела консультирования по управлению рисками KPMG в Украине Артем Кобец… Он также отметил, что с целью повышения информационной безопасности компаниям необходимо своевременно обновлять программное обеспечение… Старший консультант отдела консультирования по управлению рисками KPMG в Украине также сообщил, что KPMG провела исследование последних тенденций цифрового мошенничества в банковском секторе Америки, Европы и Азии, которые оказались во многом похожи. "Тенденции говорят о том, что цифровые риски, с которыми сталкиваются банки во всех этих трех регионах, в целом похожи. Среди основных рисков - утечка данных, социальная инженерия, стремительное развитие новых цифровых каналов и быстрых платежей", - отметил Кобец. По словам эксперта, каждый из этих рисков должен рассматриваться индивидуально, поскольку единого рецепта для защиты от этих угроз не существует, а банкам необходимо способствовать повышению осведомленности своих клиентов. В свою очередь, присутствующий на мероприятии начальник управления информационной безопасности "Укргазбанка" Сергей Недзельский отметил, что в этом году наиболее популярным видом мошенничества в Украине в банковском секторе является социальная инженерия, когда злоумышленники выманивают у клиентов данные логина и пароля, реквизиты банковских карт с целью завладения финансовыми средствами. Недзельский подчеркнул, что количество таких случаев возросло за счет увеличения доли бесконтактной оплаты платежей…» ***(Эксперт назвал самые уязвимые цели для кибератак // UNIAN.NET (https://www.unian.net/economics/telecom/10573881-ekspert-nazval-samye-uyazvimye-celi-dlya-kiberatak.html). 04.06.2019).***

***

«…Бремтейн Моуджеб (Bremtane Moudjeb), спеціаліст з продажу продуктів Cisco в категорії Data Center & Virtualization, розказує, чому нам всім так важливо турбуватися про кібербезпеку…

У світі кіберзагроз атаки стають дедалі складнішими та краще організованими. Зловмисники активно користуються засобами штучного інтелекту та машинного навчання, щоб зробити кібернапади складнішими для виявлення та автоматизувати їх…

Ще кілька років тому була дуже популярна категорія ransomware — злошкідливих програм-шантажистів. Ця категорія і зараз є популярною, але, згідно з останніми тенденціями, хакери дедалі більше використовують так званий

криптоджекінг. Це означає, що на комп'ютер жертви встановлюється програма, яка здійснює у фоновому режимі майнінг криптовалют. Тобто зловмисники крадуть вже не інформацію, а обчислювальні ресурси. І це набагато ускладнює роботу по виявленню таких загроз, адже важко зрозуміти, що шукати.

Також слід відзначити атаки на ланцюги постачання, це можна побачити на прикладі зламу серверу програмної системи «Медок» та розповсюдження вірусу non-Petya. Те саме відбувається і в інших галузях — таким чином виконуються атаки на критично важливі об'єкти інфраструктури. Ще одна специфічна характеристика атак – все ширше використовуються прийоми соціального інжинірингу, де залучені відомі слабкості людини.

Що стосується ландшафту кібербезпеки на боці кінцевих клієнтів, то тут, по-перше, все частіше використовується штучний інтелект та машинне навчання – це потрібно для того, щоб протистояти складно організованим атакам. Другий тренд – це делегування захисту стороннім організаціям керування засобами безпеки, так званим SOC (Security Operation Center — Центр Забезпечення Безпеки). Такий підхід викликаний тим, що в організаціях, які захищаються, бракує ресурсів, перш за все — людських.

Разом з тим, слід зазначити, що споживачі дедалі більше використовують пристрої так званого Інтернету речей (IoT), а також переміщають свої дані до обчислювальної хмари. Це загальна тенденція і вона ускладнює захист…» ***(Про критичність кіберзахисту в сполученому світі // Blog Imena.UA (https://www.imena.ua/blog/cyber-defense-in-the-united-world/). 19.06.2019).***

***

Сполучені Штати Америки

«США усилили кибератаки на российскую энергосистему.

В публикации издания «The New York Times» сообщается, что за последний год спецслужбами Соединенных Штатов попыток взлома программного обеспечения российских энергосистем было предпринято гораздо больше, чем раньше.

Источники издания утверждают, что в Вашингтоне речь пошла уже о внедренных программах слежения, которые способны отключать отдельные элементы энергетических систем, в том числе и касающихся российских военных и стратегических объектов.

Собеседник газеты заявил буквально следующее:

«Мы делаем это в таких масштабах, о каких и не думали несколько лет назад».

Он также подчеркнул, что активность, усиленная американскими правительственными хакерами, имеет цель стать предупреждением «президенту России Владимиру Путину».

В ходе публичного слушания одиннадцатого июня советник президента США по национальной безопасности Джон Болтон сделал заявление. В нем сказано, что Соединенными Штатами, в настоящее время, электронные сервисы

государств широко рассматриваются в качестве потенциальных целей для атак. По словам Болтона, это является частью попытки объяснить «России или кому-либо еще, кто проводит кибероперации против нас: «Ты заплатишь цену».

В совместном отчете ФБР и Министерства внутренней безопасности, опубликованном правительством США в 2017 году, говорится о хакерских атаках в отношении энергетических компаний и промышленных предприятий США. Спецслужбы утверждают, что с мая хакерами проявляется повышенный интерес к объектам ядерной энергетики, авиации, водоснабжения, а также к ключевым производствам.» ***(Стало известно о кибератаках США на российские военные и стратегические объекты // Avia. Pro (http://avia.pro/news/stalo-izvestno-o-kiberatakah-ssha-na-rossiyskie-voennye-i-strategicheskie-obekty). 17.06.2019).***

***

«Американські ЗМІ оприлюднили інформацію про кібератаки Сполучених Штатів на комп'ютерні системи енергомереж Росії, президент США Дональд Трамп назвав журналістів «зрадниками» та «ворогами народу»…

У інтерв'ю за останні три місяці американські посадовці описали раніше невідоме розгортання американського комп'ютерного коду всередині російської енергомережі та інших цілей, які супроводжували більш обговорювану атаку на російські хакерські та дезинформації підрозділи.

Своєю чергою президент США Дональд Трамп на сторінці в Twitter спростував інформацію, назвавши її брехнею, а журналістів — зрадниками…» ***(Олександр Стебницький. США посилили кібератаки на енергомережі Росії — ЗМІ // Громадське Телебачення (https://hromadske.ua/posts/ssha-posilili-kiberataki-na-energomerezhi-rosiyi-zmi). 16.06.2019).***

***

«Самая влиятельная газета мира The New York Times не стала отмалчиваться после того как президент США Дональд Трамп обвинил редакцию в виртуальной измене. Речь идет о публикации материала о якобы участившихся кибератаках Вашингтона против энергосистем России. Свое заявление The New York Times опубликовала в официальном Twitter издания. "Обвинять прессу в госизмене опасно. Мы проинформировали представителей правительства о статье еще до публикации. Как говорится в нашей статье, сами подчиненные Трампа, занимающиеся вопросами национальной безопасности, сказали, что не испытывают какой-либо обеспокоенности", - отметили представители газеты. В статье The New York Times, опубликованной 15 июня, утверждается со ссылкой на источники, что Вашингтон в течение последнего года участил попытки внедрить в энергосистему России вредоносное программное обеспечение. С его помощью США якобы могут собирать информацию о российской энергосистеме, а также, предположительно, отключить какие-то ее элементы… В материале The New York Times констатировалось, что сотрудники Совета национальной безопасности (СНБ) Белого дома отказались от комментариев в связи с приведенными в материале утверждениями. Вместе с тем они якобы

сказали, что у них не вызывает обеспокоенности публикация информации об участившихся, по версии журналистов издания, кибератаках США в отношении энергосистемы РФ.» ***(Конфликт Трампа и The New York Times вокруг публикации о кибератаках Вашингтона против Москвы // Ведомости-Украина (https://vedomosti-ua.com/100399-konflikt-trampa-i-the-new-york-times-vokrug-publikacii-o-kiberatakah-vashingtona-protiv-moskvy.html). 17.06.2019).***

***

«Президент США Дональд Трамп зажадав у понеділок від газети The New York Times негайно розкрити джерело, який повідомив їй інформацію про те, що американські спецслужби протягом останнього року стали значно активніше намагатися впровадити шкідливе програмне забезпечення в енергосистему Росії…

"Матеріал в The New York Times про збільшення кількості атак США на російську енергосистему є брехливою новиною, і занепадаюча The New York Times це знає. Вони (газета) повинні негайно розкрити свої джерела, які, якщо вони взагалі існують, в чому я сумніваюся, є фальшивкою", — написав президент США.

Він заявив, що видання "має нести повну відповідальність" за опублікований матеріал…» ***(Ілля Нежигай. Трамп зажадав від NYT розкрити джерело інформації про кібератаки на РФ // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1807631-tramp-zazhadav-vid-nyt-rozkriti-dzherelo-informatsiyi-pro-kiberataki-na-rf). 18.06.2019).***

***

«По мнению большинства экспертов, принявших участие в опросе The Washington Post, решение администрации Трампа о блокировании поставок американских компонентов и программного обеспечения компании Huawei не сделает безопасность страны лучше.

Этот запрет был наложен Министерством торговли США в прошлом месяце как часть наказания Huawei за помощь китайскому правительству в шпионаже за американскими компаниями. Однако, эксперты кибербезопасности обеспокоены, что истинными жертвами запрета станут предприятия в США, а вовсе не китайский телекоммуникационный гигант. Кроме того, такая мера, по их словам, приведёт к росту технологической независимости Китая и, соответственно, к сокращению у США возможностей влияния на политику этой державы.

В целом 61% респондентов опроса, охватившего свыше сотни экспертов кибербезопасности из университетов, частных компаний и госсектора, придерживаются мнения, что запрет это неудачная идея.

Некоторые из критиков утверждают, что запрет не сможет оградить американские компании от шпионажа и краж интеллектуальной собственности, более того, только обострит ситуацию. Один из них – Тони Коул (Tony Cole), технический директор Attivo Networks, полагает, что в сочетании с торговыми диспутами администрации Трампа с Китаем, запрет станет дополнительным поводом для значительного роста кибератак на американские компании…» ***(Запрет на поставки для Huawei не улучшит безопасность США //***

Компьютерное Обозрение (https://ko.com.ua/zapret_na_postavki_dlya_huawei_ne_uluchshit_bezopasnost_ssha_128979). 06.06.2019).

***

Країни ЄС

«Дитячий омбудсмен хоче, щоби діти та підлітки вміли дбати про власну безпеку в Інтернеті…

Дитячий омбудсмен пропонує ввести у польських школах заняття з безепеки користування Інтернетом. Міколай Павляк опрацював цю пропозицію разом з польською молоддю. За його словами, на цих заняттях діти та підлітки будуть вчитися користуватися можливостями Інтернету…

Міколай Павляк додав, що тема безпеки в мережі могла би бути елементом вже існуючих занять або новим предметом в школі. Молодь, котра спільно з дитячим омбудсменом опрацювала теми таких занять, каже, що на уроках з інформатики не порушуються теми безпеки в мережі або захисту від хейту в соцмережах…

«Найбільша проблема – це несвідомість дітей та молоді. Вони часто не усвідомлюють, що мова ненависті їх оточує всюди. Вони навіть не вміють відрізнити мову ненависті від звичайних коментарів або висловлення думки, оцінки».

Пропозицію створення у польських школах занять з кібербезпеки буде представлено в Раді Європи Комісарові з прав людини.» ***(У польських школах пропонують ввести заняття з кібербезпеки // Агенція інформації та аналітики (https://galinfo.com.ua/news/u_polskyh_shkolah_proponuyut_vvesty_zanyattya_z_kiberbezpeky_318909.html). 18.06.2019).***

***

Китай

«Офіційний представник МЗС КНР Ген Шуан на брифінгу в четвер не став коментувати інформацію про те, що причиною збою в роботі Telegram є серія DDoS-атак на його сервери з території Китаю…

У середу Telegram попередив про потужну DDoS-атаку на свої сервери, через яку користувачі в деяких країнах могли зіткнутися з неполадками. За даними сервісу Downdetector, що відслідковує роботу популярних інтернет-ресурсів, про збої повідомляли жителі Китаю, Сінгапуру, Австралії, Північної та Південної Америки, проблеми відзначалися в Європі.

Творець Telegram Павло Дуров в четвер пов'язав кібератаку на месенджер з заворушеннями в Гонконзі…» ***(Олексій Супрун. Ми не маємо інформації про кібератаки на сервери Telegram з території країни - МЗС Китаю // Інформаційне агентство «Українські Національні Новини»***

(https://www.unn.com.ua/uk/news/1806869-mi-ne-mayemo-informatsiyi-pro-kiberataki-na-serveri-telegram-z-teritoriyi-krayini-mzs-kitayu). 13.06.2019).

***

Російська Федерація та країни ЄАЕС

«Call-центр прямої лінії з президентом Росії Володимиром Путіним зазнав масованої кібератаки з-за кордону…

Одночасно, за словами головного редактора RT Маргарити Сімоньян, атака була нібито "проведена з території України". "DDos-атака, яка поклала додаток „Москва — Путіну", була з України", — йдеться в повідомленні. Уточнюється, що в даний момент додаток працює в штатному режимі.

Представники компанії "Ростелеком" уточнили, що на call-центр були здійснені дві потужні атаки. Обидві вдалося відбити, і вони не вплинули на роботу прямої лінії…» ***(Олексій Супрун. Під час прямої лінії з Путіним сталася DDos-атака, у РФ заявили про "українських хакерів" // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1808282-pid-chas-pryamoyi-liniyi-z-putinim-stalasya-ddos-ataka-u-rf-zayavili-pro-ukrayinskikh-khakeriv). 20.06.2019).***

***

«Минкомсвязи намерено ввести административные штрафы для операторов связи за использование иностранных спутниковых сетей. Соответствующий законопроект опубликован на портале проектов нормативных актов, внимание на него обратил телеграм-канал "Эшер II".

Министерство хочет дополнить Кодекс об административных правонарушениях (КоАП) статьей 13.41 — «Нарушение правил использования на территории Российской Федерации спутниковых сетей связи, находящихся под юрисдикцией иностранных государств».

В ведомстве предлагают штрафовать тех, кто «нарушил правила использования» в России иностранных спутниковых сетей, в частности, не обеспечил формирование российского сегмента такой же системы.

Минкомсвязи хочет ввести штрафы по этой статье для должностных лиц — от 10 до 30 тысяч рублей, для предпринимателей без юридического лица — от 70 до 200 тысяч рублей, а также для юридических лиц — от 500 тысяч до 1 млн рублей…» ***(Минкомсвязи предложило штрафовать операторов за подключение к иностранным спутникам // МБХ Медиа (https://mbk-news.appspot.com/news/minkomebo/). 11.06.2019)***

***

«Швейцарские спецслужбы считают, что к кибератаке на Всемирное антидопинговое агентство в 2016 году причастен «российский шпион», пишет французская газета Le Monde со ссылкой на источники.

…речь якобы идет о гражданине России Сергее Желтикове, который в 2016 году занимал пост вице-консула в генконсульстве России в Марселе.

Сотрудники французской разведки вели слежку за Желтиковым и предоставили информацию швейцарским коллегам. Как уточняет газета, россиянин обвиняется швейцарскими судами в том, что он был частью передвижной группы ГРУ, а также поддерживал связь с арестованными в апреле 2018 года шпионами Евгением Серебряковым и Алексеем Моренцом. Эти двое якобы действовали под дипломатическим прикрытием, будучи членами подразделения 26165 ГРУ, которое издание называет плацдармом военного кибершпионажа.

По информации спецслужб Швейцарии, Желтиков должен был обеспечить безопасность Серебрякову и Моренцу в Лозанне во время кибератаки на Всемирное антидопинговое агентство, пишут «Ведомости».

В 2018 году Желтиков якобы организовал приезд двух агентов для еще одной операции против федеральной лаборатории в Шпице. По информации издания, сам организатор покинул Францию в октябре 2016 году, вскоре после завершения миссии в Швейцарии.

Отмечается, что информацию о том, кем якобы является Желтиков, швейцарской стороне передала французская контрразведка – главное управление внутренней безопасности Франции. В то же время в публикации говорится, что «МИД Франции не знал о его существовании».

Российское генконсульство в Марселе в комментарии РИА «Новости» назвало публикацию Le Monde «грязной инсинуацией»… ***(Алина Назарова. Во Франции сообщили о разоблачении «российского шпиона» // Деловая газета «Взгляд» (https://vz.ru/news/2019/6/7/981479.html). 07.06.2019).***

***

«Місія ЄС у Москві у 2017 році пережила кібератаку, за якою, ймовірно, стоять росіяни…

Інформацію про порушення кібербезпеки місії виданню підтвердили у Єврокомісії після того, як про це у середу повідомило видання BuzzFeed. Атака сталася ще в 2017 році, але відомо про це стало тільки у квітні цього року.

"Ми спостерігали потенційні ознаки зламу систем, пов'язаних з нашою несекретною мережею, в нашій московській делегації. Були вжиті заходи, розслідування триває - на цьому етапі ми більше не можемо надати більше коментарів", - зазначили у Єврокомісії.

Видання BuzzFeed повідомило, що отримало в розпорядження документ, у якому сказано, що два роки тому співробітники відділу кібербезпеки виявили діяльність, яка торкнулася щонайменше двох комп'ютерів у московській місії.

Співробітники дійшли до висновку, що з цих комп'ютерів було вкрадено інформацію. Вони вважають, що атаку скоїли складні хакерські групи, традиційно пов'язані з державними розвідувальними службами.

BuzzFeed також процитував неназване джерело, яке повідомило, що за зламом, найвірогідніше, стоять російські угруповання.» ***(Місію ЄС у Москві атакували хакери і, можливо, вкрали інформацію // Європейська правда (https://www.eurointegration.com.ua/news/2019/06/6/7097003/). 06.06.2019).***

***

«Кибервойна США и России "гипотетически возможна", заявил 17 июня журналистам пресс-секретарь президента России Владимира Путина Дмитрий Песков

Так спикер Кремля прокомментировал публикацию The New York Times от 15 июня, передает "ДС" со ссылкой на ТАСС.

Газета со ссылкой на источники в американском правительстве сообщила, что США намерены разместить вредоносное программное обеспечение в российских электросетях. Источники рассказали, что с 2012 года США проводят разведывательные действия в системе управления энергосистемой России, однако теперь американская стратегия стала более наступательной. По данным The New York Times, стратегия США является предупреждением РФ, при этом Штаты готовы в том числе к кибератакам в случае конфликта между Москвой и Вашингтоном.

Песков подчеркнул, что президент США Дональд Трамп опроверг информацию The New York Times. При этом, по словам спикера Кремля, "если допустить, что какие-то государственные ведомства занимаются этим, не информируя об этом главу государства, то, безусловно, эта информация свидетельствует о гипотетической возможности, скажем так, всех признаков кибервойны и кибервоенных действий в отношении РФ".» ***(В Кремле заявили, что кибервойна США и РФ "гипотетически возможна" // DsNews (http://www.dsnews.ua/world/v-kremle-zayavili-chto-kibervoyna-ssha-i-rf-gipoteticheski-17062019135800). 17.06.2019).***

***

«…Чтобы противостоять вражеским кибератакам, в киберпространстве также предлагают придерживаться тактики сдерживания. Как это должно работать?

В начале 2019 года американские официальные лица впервые признали, что с помощью наступательных кибероперацийСША удалось остановить срыв выборов в Конгресс в 2018 году, который осуществлялся российскими хакерами. Такие операции редко обсуждаются, но в этот раз речь шла о новой доктрине «постоянного киберсдерживания» потенциальных противников…

Применять «сдерживание» означает остановить некие действия противника, заставив его поверить, что затраты для него превысят ожидаемую выгоду.

Понятие«сдерживания» в киберпространстве не идентично «ядерному сдерживанию». В случае с ядерным оружием цель сдерживания – полное

предотвращение его применения. Сдерживание в киберпространстве больше похоже на профилактику преступлений: правительства могут только частично предотвратить их…

Существует четыре основных механизма предотвращения преступного поведения в киберпространстве: угроза наказания, предотвращение защитой, изоляция и нормативные табу. Ни один из четырех способов не идеален, но все вместе они помогают снизить вероятность негативных последствий.

Эти подходы могут дополнять друг друга. Успех сдерживания зависит не только от того, как это происходит, но и от того, кто именно и что пытается сделать. Как ни странно, но удержать недружественное государство от кибератак на электросети другой страны, например, может быть легче, чем удержать хакера-одиночку от более мелких преступлений…

Ответ на кибератаку одного государства на другое не будет ограничиваться действиями в киберпространстве. Согласно оборонной доктрине США, Пентагон может ответить на вражеское кибервторжение любым оружием по своему усмотрению, пропорционально нанесенному ущербу. Это могут быть экономические санкции, международная изоляция или кинетическое оружие.

США и другие страны утверждают, что законы вооруженных конфликтов применяются в киберпространстве. Будет ли вражеская кибероперация рассматриваться как вооруженная атака, зависит от ее последствий, а не от используемых инструментов. Поэтому сдерживать нападения, которые не достигают эквивалентности вооруженного нападения, гораздо сложнее. Гибридная война России в Украине и ее вмешательство в президентскую кампанию в США оказались в такой «серой зоне»…

Средства предотвращения киберугроз вряд ли помешают спецслужбам вражеских государств – рано или поздно они взломают любую защиту. Но сочетание угрозы наказания и эффективной защиты может повлиять на их расчеты затрат и выгод. Цель тактики «киберсдерживания» – не только пресечь нападения, но и усилить защиту, увеличив расходы противника…

Эффективность сдерживания в киберпространстве предсказать сложно, потому что технологические новшества тут появляются быстрее, чем в ядерной сфере. Чем более совершенны средства атаки, тем дороже государству обойдется оборона от них. Расчеты рентабельности использования кибервойн постоянно меняются. Не все кибератаки имеют одинаковое значение, не все можно отклонить, и не все атаки поднимаются до уровня угрозы национальной безопасности.

Поэтому кибервойска будут сосредоточены на наиболее важных атаках и отклонять их будут, исходя из контекста и размера возможного урона для государства. Игнорировать такую форму агрессии, как кибератака, для современных государств было бы крайне опасно.» ***(Гарченко. Что такое «принцип сдерживания» в киберпространстве? Как он будет работать? // ETCETERA.MEDIA (https://etcetera.media/chto-takoe-printsip-sderzhivaniya-v-kiberprostranstve-kak-on-budet-rabotat.html). 23.06.2019).***

***

«…Израиль обвинил Россию в осуществлении атак на системы GPS в аэропорту имени Давида Бен-Гуриона. Как сообщило армейское радио «Гелей ЦАХАЛ», сбои в системах навигации были зафиксированы также в городе Ларнака на Кипре.

По данным израильского издания Haaretz, за последний месяц пилоты неоднократно сообщали о потере сигнала GPS во время полета. Репортеры газеты считают, что ответственность за сбои лежит на Москве, пытавшейся таким образом обезопасить свои самолеты в северо-западной Сирии. Инциденты фиксировались только в светлое время суток и не представляли угрозу безопасности пилотов или пассажиров.

Согласно сообщению Управления аэропортов Израиля, сбой затронул исключительно бортовые навигационные системы, а наземные работали в обычном режиме.

Пилоты в Израиле используют системы GPS для взлета и приземления. Кроме того, у них есть альтернативные системы для взлета, не зависимые от GPS.

Посол России в Израиле Анатолий Викторов заявил в эфире армейского радио, что сообщения СМИ о российских атаках на системы GPS являются «фейком» и не должны приниматься всерьез…» ***(Израильские СМИ обвинили РФ в атаках на системы GPS самолетов // SecurityLab.ru (https://www.securitylab.ru/news/499661.php). 28.06.2019).***

***

«…Хакеры, работающие на Министерство государственной безопасности КНР, проникли в сети восьми крупнейших технологических сервис-провайдеров с целью похищения коммерческих тайн их клиентов. Продолжавшаяся в течение нескольких лет кибершпионская операция получила название Cloud Hopper…

В декабре прошлого года Министерство юстиции США предъявило обвинения двум гражданам КНР в похищении интеллектуальной собственности западных компаний в интересах китайской экономики. Тогда сообщалось, что жертвами кибершпионов стали Hewlett Packard Enterprise и IBM. Теперь же Reuters смогло называть еще шесть организаций, чья интеллектуальная собственность утекла в Китай.

Помимо Hewlett Packard Enterprise и IBM, жертвами кибершпионов стали Fujitsu, Tata Consultancy Services, NTT Data, Dimension Data, Computer Sciences Corporation и DXC Technology (принадлежит Hewlett Packard Enterprise). От действий злоумышленников также пострадали более десяти клиентов вышеперечисленных компаний, в том числе шведская телекоммуникационная компания Ericsson, американская оборонная кораблестроительная компания Huntington Ingalls Industries и сервис бронирования билетов Sabre…» ***(Китайские кибершпионы проникли в сети восьми западных IT-компаний // SecurityLab.ru (https://www.securitylab.ru/news/499644.php). 27.06.2019).***

***

«Фінляндія, яка 1 липня бере на себе головування в ЄС, анонсувала проведення «військових ігор» для підготовки політиків країн-членів ЄС до протидії кібератакам з боку РФ і Китаю.

…спеціальні заняття, на яких чиновники будуть відпрацьовувати сценарії захисту, пройдуть в Гельсінкі в липні і вересні з міністрами внутрішніх справ і фінансів країн ЄС.

«Ми хочемо, щоб ЄС і держави-члени зміцнювали свої можливості для запобігання та реагування. Військові та цивільні органи влади можуть у кризовий момент зробити тільки те, до чого вони були підготовлені », – заявив глава МЗС Фінляндії Пекка Хаавісто, пояснюючи необхідність проведення навчань…» ***(В ЄС готуються відбивати російські кібератаки за допомогою «військових ігор» // UA.NEWS (https://ua.news/ua/v-yes-gotuyutsya-vidbyvaty-rosijski-kiberataky-za-dopomogoyu-vijskovyh-igor/). 28.06.2019).***

***

Створення та функціонування кібервійськ

«Президент США Дональд Трамп схвалив проведення кібератаки на комп'ютерні системи Ірану з управління запуском ракет після того, як Тегеран збив американський безпілотник…

За словами джерел, кібератака була здійснена в ніч на 21 червня, вона порушила роботу іранських систем. Удар по Корпусу вартових ісламської революції координувався Центральним командуванням США.

Операція завдала шкоди військовим системам командування і управління Ірану і не привела до загибелі людей або жертв серед цивільного населення, що могло б статися в разі нанесення звичайного удару, який, як заявив сам Трамп, був ним скасований.

Білий дім і військові відмовилися коментувати кібератаку по Ірану.

"Ця операція збільшує вартість постійної іранської кіберзагрози, але також служить для захисту військово-морського флоту Сполучених Штатів і морських операцій в Ормузькій протоці", – сказав колишній високопоставлений чиновник Білого дому з кібербезпеки в адміністрації Трампа Томас Боссерт.» ***(США провели кібератаку на сервери ракетних систем Ірану // Інформаційне агентство «1NEWS» (https://1news.com.ua/svit/ssha-provely-kiberataku-na-servery-raketnyh-system-iranu.html). 24.06.2019).***

***

Захист персональних даних

«…Служба таможенного и пограничного контроля США (US Customs and Border Protection, CBP) заявила об утечке данных, в результате которой

злоумышленники получили доступ к фотографиям путешественников и номерных знаков…

Утечка произошла в результате взлома сети субподрядчика ведомства, куда были загружены данные. Согласно заявлению СВР, инцидент затронул данные менее 100 тыс. человек. Речь идет о фотографиях машин, пересекающих границу США, но не фото из аэропортов. Другая персонально идентифицируемая информация не пострадала.

В СВР отметили, что подрядчик нарушил условия контракта, без ведома погранслужбы загрузив фотографии в свою сеть.

Как подчеркнули в ведомстве, в настоящее время свидетельств утечки данных в интернет или даркнет не обнаружено. В погранслужбе не сообщили, кто стоит за кибератакой. Название компании-подрядчика также не раскрывается.» ***(Погранслужба США сообщила об утечке фотографий путешественников // SecurityLab.ru (https://www.securitylab.ru/news/499422.php). 11.06.2019).***

***

«Дані 900 тис. клієнтів Альфа-банку, ОТП Банку і ХКФ Банку опинилися у відкритому доступі. Мова йде про імена, номери телефонів і паспортних даних. Про це заявили експерти з кібербезпеки…

Витік стався наприкінці травня - в базу потрапили дані про клієнтів банків, які збиралися протягом кількох років. При цьому аналітикам не вдалося виявити базу цілком - вони знайшли відомості про 55 тис. клієнтів, зібраних з 2014-2015 роки, а також 504 записи, зроблені з 2018 по 2019 роки. У будь-якому випадку, це величезна цифра. Якщо у Facebook можна додати неправильну або неповну інформацію, то в банку всі дані є справжніми, і можуть завдати непоправної шкоди користувачам.

Крім фізичних і юридичних осіб, у базі містяться дані про 500 співробітників МВС і 40 співробітників ФСБ, відзначають аналітики. У ХКФ-банк і Альфа-банку повідомили, що проведуть перевірку, в ОТП-банку витік інформації спростували.» ***(Дані мільйона клієнтів банків злили у відкритий доступ: про вас знають все // znaj.ua (https://techno.znaj.ua/238737-dani-milyona-kliyentiv-bankiv-zlili-u-vidkritiy-dostup-pro-vas-znayut-vse). 10.06.2019).***

***

«Роскомнадзор внес сервис знакомств Tinder в реестр организаторов распространения информации. Попадание в реестр накладывает на компанию обязанность делиться информацией о пользователях с ФСБ.

На попадание Tinder в реестр организаторов распространения информации обратила внимание организация Роскомсвобода. В реестре отмечено, что компания, владеющая сервисом, включена туда 31 мая. В самой компании попадание в реестр пока не прокомментировали.

"Компания внесена в реестр после того, как в ответ на требование Роскомнадзора предоставила необходимые сведения", - сообщили РБК в пресс-службе Роскомнадзора.

Организаторы распространения информации (ОРИ), включенные в реестр Роскомнадзора, должны хранить на территории России информацию о действиях пользователей (метаданные), а также переписку, аудио-, видео- и другие материалы пользователей и предоставлять их по требованию уполномоченным органам - например в ФСБ.

В реестр входят многие популярные в России сайты и интернет-сервисы: "Яндекс", "Мамба", "ВКонтакте", Mail.ru и другие.

В 2018 году у Tinder насчитывалось 57 млн пользователей а 190 странах. В российском App Store приложение занимает седьмую строчку по популярности в разделе "Образ жизни"…

На сайте Tinder указано, что приложение использует пользовательскую информацию ради "предоставления и улучшения сервисов". "Кроме того, мы используем вашу информацию в целях обеспечения вашей безопасности и предоставления рекламы, которая может вас заинтересовать", - сказано на сайте сервиса.

Там же говорится, что компания может раскрывать пользовательскую информацию, если это необходимо для исполнения судебного решения либо предупреждения или выявления преступления, а также для защиты безопасности пользователя…» ***(Tinder включили в реестр Роскомнадзора. Он должен делиться информацией со спецслужбами // BBC News. Русская служба (https://www.bbc.com/russian/news-48496137). 03.06.2019)***

***

«ФСБ запросила ключи шифрования «Яндекс.Почта» и «Яндекс.Диск», но компания отказывается их передать: ключи могут дать доступ к паролям пользователей всей экосистемы «Яндекса». За аналогичный отказ ранее был заблокирован Telegram.

Несколько месяцев назад ФСБ направила в «Яндекс» требование предоставить ключи для дешифровки данных пользователей сервисов «Яндекс.Почта» и «Яндекс.Диск», рассказали РБК источник на ИТ-рынке и собеседник, близкий к «Яндексу». Оба собеседника РБК утверждают, что за прошедшее время «Яндекс» так и не предоставил в спецслужбу ключи, хотя по закону на это отводится не более десяти дней…

«Яндекс.Почта» и «Яндекс.Диск» находятся в реестре организаторов распространения информации (ОРИ), то есть интернет-площадок, на которых пользователи могут обмениваться сообщениями. Согласно так называемому закону Яровой, с 20 июля 2016 года Центр оперативно-технических мероприятий ФСБ может потребовать от любого сервиса из реестра ОРИ передать ему «информацию, необходимую для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений пользователей сети интернет»…

По словам источника РБК на ИТ-рынке, в «Яндексе» считают, что ФСБ слишком широко трактует норму «закона Яровой». «Спецслужба требует от компании предоставить сессионные ключи, которые, по сути, дают доступ не только, например, к сообщениям в почте, но и позволяют анализировать весь трафик от пользователей к находящимся в реестре ОРИ сервисам «Яндекса». Не

говоря уже о том, что дешифровка всего трафика в рамках пользовательской сессии несет значительные риски в плане безопасности», — говорит он. Информацию про то, что ФСБ требует от компании именно сессионные ключи, подтвердил и второй собеседник РБК, близкий к интернет-холдингу.

Сессионный ключ — это ключ шифрования, который используется только для одного соединения между пользователем и сервером, то есть одной сессии, пояснил бывший разработчик The Tor Project Леонид Евдокимов. «В случае с «Яндекс.Почта» он вырабатывается, когда пользователь только заходит на страницу mail.yandex.ru, а прекращает свое действие в зависимости от настроек через какое-то время, после того как пользователь либо закроет вкладку «Яндекс.Почта», либо полностью закроет браузер, либо выключит компьютер», — говорит он. Таким ключом шифруются не только сообщения пользователя, но и все метаданные (когда, кто, с какого IP-адреса заходил в аккаунт и т.д.), а также логин и пароль, которые пользователь отправляет на серверы «Яндекса» в процессе авторизации. «Поэтому передача сессионного ключа какого-либо пользователя спецслужбам может позволить им завладеть логином и паролем от почтового ящика этого пользователя», — утверждает Евдокимов…

Консультант по информационной безопасности Cisco Systems Алексей Лукацкий подтверждает, что «сессионный ключ в любом случае шифрует логин и пароль, которые пользователь передает на сервер в процессе авторизации, так что передача такого ключа ФСБ может дать доступ к аутентификационным данным пользователя». Он указал, что «Яндекс» использует систему Single Sign-On, при которой, авторизовавшись в «Яндекс.Почта», можно без повторной аутентификации перейти в «Яндекс.Музыка», «Яндекс.Диск» и любой другой сервис. «Ключ шифрования при переходе в разные сервисы должен быть свой, но если это не так, то это архитектурная проблема, которая может открыть доступ к данным в разных сервисах «Яндекса». Тогда передавать сессионный ключ, конечно, небезопасно», — рассуждает Лукацкий.

Леонид Евдокимов считает, что сессионные ключи позволяют получить не только доступ к данным, но и анализировать само поведение пользователей. Например, в «Яндекс.Диск», завладев сессионным ключом, можно смотреть, кто и какие данные скачивал, отметил он.

По словам собеседника РБК, близкого к «Яндексу», компания обеспокоена тем, что сотрудничество с ФСБ может привести к оттоку пользователей, потере доли на рынке и, как следствие, существенным денежным потерям. «Иностранные компании, например Google, ФСБ не принуждает к такому сотрудничеству, поэтому «Яндекс» тут видит угрозу своему конкурентному положению», — говорит он…» ***(ФСБ потребовала ключи шифрования переписки пользователей у «Яндекса» // РБК (https://www.rbc.ru/technology_and_media/04/06/2019/5cf50e139a79474f8ab5494b). 04.06.2019)***

***

«Аэрокосмическая компания ASCO приостановила производство в четырех странах из-за кибератаки.

Один из крупнейших мировых производителей запчастей для авиационной техники бельгийская компания ASCO была вынуждена приостановить работу заводов в четырех странах из-за атаки с использованием вымогательского ПО.

…программа вывела из строя IT-системы ASCO, в результате компания отправила большую часть своих сотрудников в отпуск за свой счет на целую неделю.

Согласно имеющейся информации, инцидент произошел в минувшую пятницу, 7 июня. Изначально атаке подвергся завод в компании в Бельгии, однако ASCO также приостановила производство в Германии, Канаде и США. На данный момент неясно, связано ли данное решение с распространением заражения, или же является просто мерой предосторожности. Офисы компании во Франции и Бразилии не пострадали.

Компания сообщила об инциденте в правоохранительные органы. В настоящее время ведется расследование…» ***(Вымогательское ПО парализовало работу заводов ASCO // SecurityLab.ru (https://www.securitylab.ru/news/499456.php). 13.06.2019).***

***

«…В среду, 12 июня, популярный мессенджер Telegram на короткое время стал недоступен для сотен тысяч пользователей по всему миру. Причиной послужила мощная DDoS-атака на его серверы.

По словам основателя Telegram Павла Дурова, большинство IP-адресов, с которых осуществлялась атака, были китайскими, что указывает на возможную причастность к ней правительства КНР. В пользу этой теории говорят сразу несколько фактов, отметил Дуров. Во-первых, инцидент совпал с протестами в Гонконге. Во-вторых, как правило, мощность финансируемых китайским правительством DDoS-атак на Telegram составляет 200-400 Гб/с, и нынешний случай не стал исключением.

Начиная с прошлой недели, в Гонконге проходят массовые акции протеста против поправок в закон об экстрадиции, разрешающих экстрадировать арестованных в Гонконге граждан на материковый Китай и другие страны. Многие видят в поправках угрозу гражданским свободам и верховенству закона в Гонконге.

С помощью зашифрованного мессенджера Telegram протестующие координировали свои действия и обменивались информацией о происходящем, не боясь перехвата сообщений…» ***(DDoS-атака лишила сотни тысяч пользователей доступа к Telegram // SecurityLab.ru (https://www.securitylab.ru/news/499455.php). 13.06.2019).***

***

«…Из-за кибератаки британская музыкальная группа Radiohead была вынуждена выложить в открытый доступ 18 часов записанного аудиоматериала.

Как сообщает участник группы Джонни Гринвуд, неизвестные взломали и похитили у лидера Radiohead Тома Йорка архив с аудиоматериалами времен альбома «OK Computer» (вышел в 1997 году) и потребовали выкуп в размере $150 тыс., пригрозив в противном случае опубликовать его. Записи не предназначались для публикации, хотя некоторые отрывки все же вошли в переиздание «OK Computer».

«Вместо того чтобы жаловаться или игнорировать, мы публикуем все 18 часов записи на Bandcamp в пользу Extinction Rebellion. Только на 18 дней. За 18 фунтов вы сможете сами оценить, стоит ли нам платить выкуп», - сообщил Гринвуд в Twitter.

Любой желающий может бесплатно прослушать сборник записей «Minidiscs [Hacked]» в сервисе Bandcamp. Скачать этот импровизированный альбом можно за 18 фунтов стерлингов. Все полученные средства будут переданы экологическому движению Extinction Rebellion.» ***(Группа Radiohead опубликовала 18 часов неизданных записей из-за кибератаки // SecurityLab.ru (https://www.securitylab.ru/news/499446.php). 13.06.2019).***

***

«…Компания Microsoft предупредила о текущей спам-кампании, в рамках которой злоумышленники распространяют электронные письма с целью заражения систем вредоносным ПО. Судя по всему, кампания в основном направлена на жителей европейских стран, поскольку сообщения оформлены на различных языках, используемых в Евросоюзе.

В ходе атак организаторы кампании эксплуатируют уязвимость CVE-2017-11882, затрагивающую редактор формул (Equation Editor) в MS Office. Исправление для данной проблемы было выпущено еще в ноябре 2017 года, а в январе 2018 года Microsoft и вовсе удалила этот компонент из своих офисных программ, заменив его альтернативной функциональностью. Тем не менее, как показывает практика, действующий эксплоит для данной уязвимости все еще эффективен, учитывая его лидирующие позиции в рейтингах популярности среди организаторов атак.

В ходе текущей спам-кампании злоумышленники распространяют вредоносный документ RTF, который достаточно просто открыть, чтобы запустить загрузку и выполнение различных скриптов (VBScript, PowerShell, PHP). По словам специалистов Microsoft, на компьютер загружается троян Trojan:MSIL/Cretasker - бэкдор, который после запуска пытается установить связь с C&C-сервером. В настоящее время домен, к которому обращается троян, заблокирован, но злоумышленники могут в любой момент, используя ту же тактику, организовать новую кампанию, предупреждают эксперты.» ***(Спамеры активно эксплуатируют уязвимость в MS Office для распространения бэкдора // SecurityLab.ru (https://www.securitylab.ru/news/499409.php). 10.06.2019).***

***

«Новое исследование показало, что в реальных атаках используется только порядка 5,5% уязвимостей, раскрываемых публично, притом в половине случаев атакующие пишут эксплойт с нуля.

Эти результаты группа исследователей из аналитической компании Cyentia, НКО RAND Corporation и Политехнического университета Виргинии получила на основе анализа данных, собранных различными организациями в период с 2009 года по 2018-й.

Так, сведения об уязвимостях команда почерпнула из базы данных NVD (National Vulnerability Database), которую ведет Национальный институт по стандартизации и технологии США. Информацию об эксплойтах, используемых в кибератаках, исследователям предоставили компании Fortinet, Secureworks, AlienVault, ReversingLabs, а также Центр SANS по сетевым угрозам. Список обнародованных PoC-кодов был составлен на основе коллекций Exploit DB, Contagio, Secureworks, ReversingLabs и каталогов модулей, создаваемых для специализированных фреймворков (Metasploit, D2 Elliot Web Exploitation Framework, Canvas).

Как оказалось, за 10 лет было выявлено около 76 тыс. уязвимостей; из них злоумышленники использовали немногим более 4 тыс. Примечательно, что почти в половине случаев они отдали предпочтение критическим багам, с оценкой 9 баллов и выше по шкале CVSS v2.

Против ожидания, исследователи не смогли установить взаимосвязь между публикацией PoC и началом атак через уязвимость. Совокупно за 10 лет было обнародовано свыше 9,7 тыс. PoC-кодов; из них злоумышленники позаимствовали лишь 2,1 тыс., а в остальных случаях (в том же объеме) создали эксплойт самостоятельно.

Результаты масштабного исследования были представлены на очередной конференции «Финансовые аспекты информационной безопасности», прошедшей в Бостоне в начале этой недели. Авторы работы надеются, что полученные данные помогут компаниям, полагающимся на CVSS-рейтинг, лучше оценивать риски и расставлять приоритеты при установке патчей.» ***(Maxim Zaitsev. Отсутствие PoC не смущает злоумышленников // Threatpost (https://threatpost.ru/lack-of-public-poc-does-not-stop-attackers-from-exploiting-vulnerabilities/32980/). 07.06.2019).***

***

«Фишинговые атаки, необновленное ПО и неразрешеные облачные приложения создают постоянные риски и требуют постоянного внимания специалистов по информационной безопасности. Автономные функции мониторинга угроз и применения исправлений для устранения уязвимостей программного обеспечения зачастую являются лучшим — и все чаще единственным эффективным — способом решения этих проблем.

Это один из ключевых выводов совместного исследования Oracle и KPMG. В «Отчете Oracle и KPMG об угрозах для облаков в 2019 году» (Oracle and KPMG Cloud Threat Report 2019) анализируются многочисленные угрозы, с которыми сталкиваются предприятия. Основные выводы исследования Oracle и KPMG:

23% респондентов утверждают, что их организации не располагают ресурсами для обновления всех своих систем вручную. Это свидетельствует о необходимости автономных вычислений при развертывании патчей и исправлений безопасности.

50% отмечают, что использование облачных приложений без разрешения привело к несанкционированному доступу к данным; 48% говорят, что несанкционированный доступ повлек за собой заражение вредоносным ПО, а 47% сообщают о потере данных. Это указывает на необходимость внедрения политик для ограничения несанкционированного использования облачных приложений — и, возможно, применения автономных функций обнаружения или блокирования такого использования.

92% опрошенных обеспокоены тем, что отдельные лица, отделы или направления бизнеса в организации нарушают политики безопасности, когда речь идет об использовании облачных приложений. Это может выражаться в применении неразрешенных облачных приложений или непредусмотренном использовании разрешенных облачных приложений.

69% организаций знают о том, что сотрудниками используется умеренное или значительное количество неразрешенных облачных приложений. Еще 15% заявили, что им известно по крайней мере о нескольких таких приложениях. Привлекательность облачных приложений огромна, и сотрудники часто не колеблясь используют их, не взирая на принятые политики безопасности или процедуры утверждения.

Общий вывод таков: сегодня как никогда важно использовать автономные вычисления для защиты бизнеса в дополнение к аналитике событий безопасности. Исследование также показало, что для CISO важно больше знать об использовании облачных вычислений в своих организациях и что всем заинтересованным сторонам, включая ИТ-отделы, необходимо лучше понимать модель совместной ответственности за безопасность облачных вычислений…

Количество тревожных сообщений и инцидентов, с которыми приходится иметь дело корпоративному отделу информационной безопасности, и без того слишком велико. Если к ним добавить еще и предупреждения об аномальном поведении конечного пользователя (как это и должно быть), проблема, скорее всего, быстро усугубится. Типичное крупное предприятие имеет дело с 3,3 млрд событий в месяц, «однако только 31 из них на самом деле являются реальными событиями безопасности или несут в себе угрозы, — говорит Брайан Дженсен из KPMG. — Это как искать иголку в стоге сена – или даже хуже».

Предприятия не видят выход из этого хаоса, ведь невозможно найти, нанять, обучить и удержать такое количество аналитиков по безопасности. «Данная задача не может быть решена только путем наращивания кадрового состава, для этого необходимы интеллектуальная автоматизация и обученный квалифицированный персонал. Они нужны для разработки масштабируемого решения, которое учитывает уникальные риски использования облачных сервисов», — говорит Брайан Йенсен из KPMG.

Еще одна угроза исходит от систем с необновленным программным обеспечением. При обнаружении уязвимостей в операционных системах,

приложениях или прошивке устройства (например, в реализациях Интернета вещей) ИТ-персоналу совместно с отделом информационной безопасности может потребоваться слишком много времени для установки и тестирования необходимых исправлений или изменений конфигурации.

Решение состоит в том, чтобы позволить программному обеспечению самостоятельно выполнять утомительную, повторяющуюся тяжелую работу, чтобы аналитики в области ИТ и безопасности могли сфокусироваться на устранении более сложных проблем. Обновление уязвимого оборудования или программного обеспечения — одна из наиболее важных мер, которые может предпринять отдел кибербезопасности. Согласно отчету, автоматизированное обновление (установку патчей) используют 43% организаций, причем среди крупных организаций (1000 сотрудников или более) этот показатель составляет 50%. Еще 46% всех организаций планируют внедрить автоматическое обновление в течение следующих 12-24 месяцев.

Исследование показывает четкое стратегическое намерение использовать автономные вычисления для патчинга базы данных. Около четверти респондентов (24%) полностью или в основном автоматизировали обновление ПО своих серверов баз данных, а еще 18% частично автоматизировали патчинг своих баз данных. Тем не менее, отчет выявил четкие различия в средствах автоматизации, которые использовались на протяжении многих лет, и показал, какие формы автономных вычислений действительно эффективны…

Отчет об угрозах в 2019 году содержит дополнительные данные исследования, а также рекомендации для решения этих и других проблем безопасности предприятия при переносе критически важной нагрузки в облачную среду. Данные получены от 450 специалистов по кибербезопасности и ИТ из коммерческих и государственных организаций США, Канады, Великобритании, Австралии и Сингапура.» ***(46% компаний рассматривают автономные вычисления для предотвращения угроз безопасности в облаке // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5592953-46-kompanij-rassmatrivayut-avtonomn.html). 13.06.2019).***

***

«Специалисты Netskope обнаружили спам-кампанию, в рамках которой злоумышленники распространяют ISO-образы с троянами LokiBot и NanoCore. Эксперты сообщают о десяти разновидностях рассылок, в которых используются разные файлы и письма.

Сообщения с вредоносными вложениями под видом счетов-фактур мошенники отправляют случайным жертвам. Обнаружить кампанию специалисты смогли благодаря нестандартному размеру вложений — размер ISO-файлов не превышал 1–2 МБ, что несвойственно образам дисков. Вероятно, этот формат для распространения троянов злоумышленники выбрали, чтобы обойти фильтры большинства почтовых сервисов. Эксперты отмечают, что жертве достаточно кликнуть по вложению, чтобы ОС смонтировала вредоносный образ.

Одним из видов полезной нагрузки выступал LokiBot. Этот штамм трояна умеет распознавать запуск внутри отладчика или виртуальной машины, но в

остальном мало отличается от прошлых версий. Сразу после запуска программа проверяет наличие в системе распространенных инструментов удаленного администрирования — SSH, VNC и RDP, а также 25 различных веб-браузеров и 15 почтовых клиентов, из которых LokiBot крадет учетные данные.

В других случаях ISO-образы содержали модульный троян NanoCore, позволяющий получить полный контроль над компьютером, чтобы красть информацию и шпионить за жертвой через веб-камеру. В феврале прошлого года разработчик программы Тейлор Хадлстон (Taylor Huddleston) получил 2 года и 9 месяцев тюрьмы за создание вредоносного ПО. Несмотря на то что NanoCore доступен в Интернете с 2013 года, зловред до сих пор актуален как угроза и продолжает развиваться. Обнаруженный вариант трояна может перехватывать нажатия клавиш, собирать информацию о сохраненных документах и данные из буфера обмена, а также использовать протокол FTP для вывода украденных данных…» ***(Dmitry Nazarov. Спамеры рассылают письма с вредоносными ISO-файлами // Threatpost (https://threatpost.ru/spammers-sending-emails-with-malicious-iso/33286/). 27.06.2019).***

***

Діяльність хакерів та хакерські угруповування

«…По меньшей мере две хакерские группировки активно атакуют почтовые серверы с установленным агентом Exim в целях эксплуатации недавно обнаруженной в ПО уязвимости.

По состоянию на июнь 2019 года Exim было установлено на 57% (507 389) от всех видимых через интернет почтовых серверов (по некоторым данным, в действительности число установок Exim превышает данную цифру в десять раз и составляет 5,4 млн).

Речь идет об уязвимости CVE-2019-10149, также известной как «Return of the WIZard», которая затрагивает версии Exim от 4.87 до 4.91. Уязвимость позволяет удаленному/локальному злоумышленнику запускать на почтовом сервере команды с привилегиями суперпользователя.

По данным специалиста Фредди Лимана (Freddie Leeman), первая волна атак началась 9 июня. В ходе кампании некая хакерская группа начала атаковать почтовые серверы с расположенного в интернете C&C-сервера, а в последующие дни принялась экспериментировать с методами эксплуатации, меняя тип вредоносного ПО и скриптов, загружаемых на зараженные серверы.

Примерно в то же время была зафиксирована еще одна волна атак, организованная уже другой группировкой. По словам ИБ-экспертов, данная кампания более сложная по сравнению с вышеописанной и продолжает развиваться. В ходе атак злоумышленники создают бэкдор на почтовых серверах путем загрузки шелл-скрипта, добавляющего SSH ключ к учетной записи суперпользователя. Сам скрипт располагается на сервере в сети Tor, благодаря чему его происхождение практически невозможно выяснить. В основном хакеры атакуют системы на базе ОС Red Hat Enterprise Linux (RHEL), Debian, openSUSE и

Alpine Linux, рассказал ZDNet эксперт из компании Cyren Магни Сигурдсон (Magni R. Sigurdsson).

По данным ИБ-специалистов, во второй кампании также используется червь для распространения заражения на другие почтовые серверы. Кроме того, помимо бэкдора, атакующие загружают на скомпрометированные серверы программы для добычи криптовалюты.

Для защиты от атак владельцам уязвимых серверов рекомендуется обновиться до новой версии Exim - 4.92.» ***(Миллионы почтовых серверов Exim находятся под активными атаками // SecurityLab.ru (https://www.securitylab.ru/news/499465.php). 14.06.2019).***

***

«Группировка Achilles предположительно имеет иранское происхождение и пользуется хорошей репутацией у хакеров.

Некто под псевдонимом Achilles продает на киберпреступных форумах доступ к внутренним сетям целого ряда организаций, в том числе ЮНИСЕФ, Symantec и Comodo. В зависимости от организации стоимость доступа составляет от двух до пяти тысяч долларов.

Ранее SecurityLab сообщал о киберпреступнике или группе киберпреступников под псевдонимом Fxmsp, продающей исходные коды и другие данные троих американских производителей антивирусных решений. Однако если Fxmsp является русскоязычной группировкой, то участники Achilles используют английский язык и могут быть иранцами.

По данным специалистов компании Advanced Intelligence (AdvIntel), группировка Achilles пользуется успехом у киберпреступного сообщества и может похвастаться хорошими отзывами на хакерских форумах.

В разговоре с потенциальным покупателем группировка сообщила о наличии у нее доступа к внутренним сетям организации ЮНИСЕФ, ИБ-компаний Symantec и Comodo, производителя ПО для 3D Hash Inc и канадской турфирмы Transat. По словам продавцов, доступ к сетям Symantec и Hash Inc возможен через удаленное подключение к рабочему столу.

На запрос журналистов BleepingComputer пресс-служба Symantec предоставила следующий ответ: «В настоящее время Symantec не фиксировала никаких свидетельств вторжения в сеть. Мы также считаем, что у наших клиентов нет никаких причин для беспокойства».

Никаких доказательств того, что у нее действительно есть доступ к внутренним сетям Transat, Symantec и Comodo, группировка не представила. Тем не менее, доступ к документам ЮНИСЕФ у нее, похоже, все-таки есть. За четыре тысячи долларов Achilles предлагает покупателям непосредственный доступ к сети организации, позволяющий похитить 3,6 ТБ принадлежащих ей данных. В качестве доказательства наличия у них доступа к ЮНИСЕФ киберпреступники представили соответствующие скриншоты.» ***(Киберпреступники выставили на продажу доступ к сетям Symantec и Comodo // SecurityLab.ru (https://www.securitylab.ru/news/499387.php). 07.06.2019).***

***

«…В рамках получившей кодовое название Soft Cell операции, которая длится с 2012 г. (а вероятно, и дольше) хакеры из группировки APT10, предположительно аффилированные с китайским правительством, атаковали десяток телекоммуникационных компаний в тридцати с лишним странах.

Получение доступа к этим компаниям, чьи названия не приводятся, проводилось в несколько этапов. Реализация первого этапа, как сообщила 25 июня в своем докладе американо-израильская компания Cybereason Nocturnus, работающая в сфере безопасности, началась в 2017 г. В течение уже 2018 г. киберпреступники получили полный доступ к сетям компаний с целью получения персональных данных интересующих Пекин лиц. А привлекали внимание китайцев прежде всего представители иностранных правительств и силовых органов, а также политики.

По данным Cybereason, хакеры заполучили доступ к паролю каждого пользователя, что в свою очередь открыло путь к счетам, сведениям о телефонных разговорах и переписке, почте, геолокации и т. д. В общем, ко всему, что имеет значение в наш цифровой век.

По словам гендиректора Cybereason Лиора Дива, за семь лет операции Soft Cell проникновение хакеров в компьютерные сети стало полномасштабным - на всех уровнях… По его мнению, высокий уровень сложности проводимых атак свидетельствует о том, что кибернападения не были делом рук каких-нибудь криминальных группировок, а могли проводиться лишь в тесной координации с любым правительством. И речь о правительстве Китая.

Что указывает на Китай? В Cybereason, изучив анатомию атак, пришли к выводу, что применяемые инструменты и методы, или TTP (tactics, techniques and procedures) идентичны тем, которые использует группировка APT10 (известная также, как Menupass, Red Apollo, Stone Panda, CVNX), которую правительство США связывает с Министерством государственной безопасности КНР.

Для получения доступа к сетям телекоммуникационных компаний использовалась модифицированная версия веб-оболочки China Chopper. Эту веб-оболочку, которая "весит" лишь 4 килобайта, впервые обнаружили еще в 2012 г. Ее применяют по большей части китайские хакеры для удаленного управления веб-серверами. Сам взлом сетей тех 10 компаний производился через процесс ОС Windows - w3wp.exe, запускающий веб-приложения и отвечающий за обработку запросов, отправленных на веб-сервер…

Вызывает вопрос, собственно, время, выбранное для публикации данного доклада. Если операция длится с 2012 г., а атаки на телекоммуникационные компании хакеры начали готовить еще в 2017-м, то почему деятельность китайской группировки попала на страницы данного отчета в середине 2019-го?

Нет ли связи между этим докладом и продолжением торговой войны между Вашингтоном и Пекином, которая выразилась сперва в введении Дональдом Трампом ограничений в отношении компании Huawei по подозрении в шпионаже? И буквально накануне - 21 июня - Минторговли США в черный список внесло также еще пять IT-компаний из Поднебесной: Higon, Sugon, THATIC, Chengdu Haiguang Integrated Circuit и Chengdu Haiguang Microelectronics Technology. Как

пишет Bloomberg, эти компании являются лидерами по разработкам в области сверхбыстрых компьютерных вычислений. И теперь им запрещено покупать американские товары и услуги.

И примечательно, что 25 июня, когда появился доклад Cybereason, CNN со ссылкой на свои источники сообщил о проведении американскими военными в ответ на сбитый беспилотник масштабной кибератаки на шиитскую группировку "Катаиб Хезболла", которая действует на территории Ирака, а также Сирии, где воюет плечом к плечу с силами режима Башара Асада. Она также активно участвовала в боях против Международной коалиции во главе с Штатами в Ираке. По данным Госдепартамента США, группировка финансируется спецподразделением иранского КСИР "Кудс".

Казалось бы, при чем здесь Китай? Но на сегодняшний день Китай и Иран в списке Белого дома внешних угроз для США занимают верхние строчки, по понятной причине подвинув Россию (личная аллергия Трампа на "российское дело").

Вышеупомянутый доклад Cybereason в совокупности с просочившимися в СМИ данными о кибератаке на иранские прокси-силы вполне может быть еще одним элементом информационной войны. Наряду с введением санкций в отношении китайских цифровых и технокомпаний. Таким образом в медиа прочно укрепляется аргументация для предстоящей или предстоящих кибероперацій наступательного характера против и Китая, и Ирана…» ***(Владислав ГИРМАН . Операция Soft Cell. Как китайские хакеры помогли Трампу // DsNews (http://www.dsnews.ua/world/operatsiya-soft-cell-kakoy-otvet-kitayu-gotovyat-amerikanskie-26062019220000). 26.06.2019).***

***

«Хакер зумів обійти систему безпеки NASA і пробратися в мережу Лабораторії реактивного руху (JPL) Агентства, вибравши в якості "зброї" мікрокомп'ютер під назвою Raspberry Pi.

Вторгнення було здійснено ще в 2018 році, але відомо про це стало лише зараз у звіті за 18 червня. В ньому NASA розповідає про "неавторизований" Raspberry Pi, що створив портал, який давав невідомому зловмиснику доступ до мережі протягом декількох місяців, поки він не був в кінцевому підсумку виявлений та виправлений…

"Секрет" хакера в тому, що міні-комп'ютер не був призначений для підключення до мережі і міг отримати доступ до мережі без ідентифікації. Саме цим недоліком і скористався зловмисник.

Про те, чи зашкодило це "вторгнення" системі безпеки NASA поки невідомо, але, однозначно, це дуже тривожний дзвіночок, адже неперевірений пристрій, підключений до мережі однієї з найбільш секретних організацій, залишався там протягом декількох місяців і вихопив чимало даних, перш ніж його виявили.

…Raspberry Pi - це мікрокомп'ютер вартістю 35 доларів, який популярний серед шкільних наукових проектів та через його випадкову появу в хакерських фільмах або телешоу. Його розмір і ціна роблять його привабливим елементом обладнання для безлічі майстрів. І хоча він дешевий і крихітний, у нього мало

обмежень в тому, що він може робити, якщо ним користуються умілі руки. Хакер, який використовував зовнішній обліковий запис користувача, непомітно переміщався по мережі НАСА протягом приблизно 10 місяців, згідно з червневим звітом з кібербезпеки. Перебуваючи там, він шукав 23 файли, два з яких містили інформацію про поточну місію на Марс. У цілому, згідно зі звітом, хакер отримав дані приблизно на 500 мегабайт.» ***(Хакер обдурив систему безпеки NASA: хотів полетіти на Марс // znaj.ua (https://techno.znaj.ua/242497-haker-obduriv-sistemu-bezpeki-nasa-hotiv-poletiti-na-mars). 26.06.2019).***

***

Вірусне та інше шкідливе програмне забезпечення

«…Считавшееся исчезнувшим вредоносное ПО ICEFOG (другое название Fucobha) снова появилось в арсенале киберпреступников.

Изначально ICEFOG использовался одноименной китайской APT-группой, деятельность которой специалисты «Лаборатории Касперского» описали еще в 2013 году. После публикации отчета ЛК группировка свернула свои операции, и ICEFOG исчез с киберпреступной арены. Однако, как оказалось, работа над вредоносом не прекращалась.

На конференции по ИБ, состоявшейся в Польше на прошлой неделе, исследовательница компании FireEye Чи-Энь Шэнь сообщила об обнаружении обновленных версий ICEFOG. Главные из них, ICEFOG-P и ICEFOG-M, использовались в атаках с 2014-го и 2018-го года соответственно. Обе версии являются прямыми «потомками» оригинального ICEFOG, а значит, на самом деле работа над вредоносом не прекращалась. Более того, Шэнь обнаружила ранее неизвестную версию ICEFOG для Mac.

Примечательно, что группировки, использующие новые версии ICEFOG, никак не связаны с одноименной APT-группой. Вредонос был обнаружен во множествах операций, проводимых разными группировками…

Каким образом вредонос оказался в арсенале множества группировок, Шэнь затрудняется сказать. Тем не менее, ранее ИБ-эксперты уже сталкивались с использованием одних и тех же инструментов разными китайскими группировками.

Новые варианты ICEFOG были обнаружены в атаках на европейскую сельско-хозяйственную компанию, правительственные и финансовые организации, а также СМИ в России и Монголии (операция TOPNEWS), правительственные учреждения пост-советских стран (Roaming Tiger), казахских должностных лиц (APPER) и пр. В 2018-2019 годах вредонос использовался в атаках на турецкие и казахские организации (операция SKYLINE).» ***(Древнее вредоносное ПО ICEFOG снова вернулось в строй // SecurityLab.ru (https://www.securitylab.ru/news/499410.php). 10.06.2019).***

***

«Специалисты Федерального управления по информационной безопасности Германии (BSI) сообщили о вредоносных программах, обнаруженных в прошивке четырех моделей смартфонов, продаваемых в стране. Это Android-устройства Doogee BL7000, M-Horse Pure 1, Keecoo P11 и VKworld Mix Plus.

Прошивка телефонов содержит троянский бэкдор Andr/Xgen2-CY. Программа запускается при включении телефона, собирает сведения о зараженном устройстве, соединяется с центром управления и ожидает дальнейших инструкций.

Представители BSI заявили, что удалить вредоносный компонент вручную невозможно, поскольку он привязан к внутренней области прошивки. Чтобы избавиться от трояна, нужно установить новую прошивку, но безопасные обновления доступны только для одной из четырех моделей — Keecoo P11.

По данным Sophos, Andr/Xgen2-CY собирает следующие данные:

номер телефона;

информация о местоположении;

идентификатор IMEI и идентификатор Android;

разрешение экрана;

производитель, модель, марка, версия ОС;

информация о процессоре;

тип сети;

MAC-адрес;

объем оперативной и постоянной памяти;

объем SD-карты;

используемый язык;

оператор мобильной связи.

После того как данные попадут на C&C-сервер, злоумышленники присвоят устройству уникальный профиль и смогут:

скачивать, устанавливать и удалять приложения;

выполнять команды оболочки;

открывать страницы в браузере.

Эксперты предполагают, что многие владельцы все еще пользуются зараженными телефонами. Ежедневно более 20 тысяч немецких IP-адресов обращаются к командным серверам Andr/Xgen2-CY.4874…» ***(Dmitry Nazarov. В четырех бюджетных смартфонах в Германии обнаружен бэкдор // Threatpost (https://threatpost.ru/backdoor-found-in-four-budget-smartphone-models-in-germany/32999/). 07.06.2019).***

***

«Эксплойт-пак RIG начал распространять ранее неизвестный вариант вымогателя Vega. Шифровальщик Buran кодирует пользовательские файлы и предлагает жертве связаться с киберпреступниками по электронной почте для восстановления данных. ИБ-аналитики пока не смогли создать декриптор для нового зловреда и рекомендуют пострадавшим на всякий случай скопировать документы с требованием выкупа, а также записи реестра, созданные вредоносной программой.

Новую полезную нагрузку вредоносного комплекта RIG обнаружила команда исследователей nao_sec, специализирующаяся на отслеживании эксплойт-паков. Как выяснили ИБ-специалисты, для доставки на целевые устройства шифровальщика RIG использует уязвимости в браузере Internet Explorer. Оказавшись на машине, Buran копирует себя в папку с адресом %APPDATA%\microsoft\windows\ctfmon.exe, после чего приступает к кодированию информации жертвы.

По данным аналитиков, новый зловред не удаляет теневые копии томов, не отключает механизм автоматического восстановления Windows и не чистит журналы событий. Вымогатель кодирует все файлы на диске, за исключением объектов, включенных в его стоп-лист. Шифрование не затрагивает файлы с расширениями COM, EXE, DLL, SYS, а также некоторые другие форматы. Кроме того, зловред пропускает около сорока папок, содержимое которых может нарушить работоспособность устройства.

Для зараженного компьютера создается уникальный идентификатор компьютера, который Buran также использует в качестве расширения измененных файлов. Послание жертве содержится в текстовом документе с именем !!! your files are encrypted !!!.txt. Злоумышленники предлагают пострадавшему связаться с ними по электронной почте, чтобы получить декриптор, и предостерегают его от попыток восстановить данные самостоятельно.

Исследователи отмечают, что вредоносная программа создает в реестре HKEY_CURRENT_USER\Software\Buran записи, похожие на публичный и секретный ключ шифрования, однако неизвестно, можно ли с их помощью восстановить закодированную информацию.

RIG в настоящее время является одним из наиболее активных эксплойт-паков. Он пришел на смену наборам Angler, Nuclear и Neutrino в 2016 году. Операторы RIG зачастую подряжаются распространять вымогательское ПО и в разное время доставляли с его помощью шифровальщиков Matrix, Locky, CryptoShield и GandCrab. Несмотря на общее снижение доли готовых наборов, RIG регулярно появляется в поле зрения ИБ-специалистов. Так, летом прошлого года он был замечен в кампании по распространению руткита CEIDPageLock.» ***(Dmitry Nazarov. Набор эксплойтов RIG теперь доставляет шифровальщик Buran // Threatpost (https://threatpost.ru/rig-toolkit-distributes-buran-ransomware/32982/). 07.06.2019).***

***

«Необычный зловред для macOS нашли ИБ-специалисты. Программа устанавливает в систему собственный прокси-сервер и прослушивает трафик, передаваемый браузером Safari. Единственным видимым последствием взлома является подмена поисковой выдачи Google на аналогичные результаты Bing, однако теоретически киберпреступники способны изменять любые данные из HTTP/HTTPS-запросов жертвы.

По мнению аналитиков, заражение происходит через спам или drive-by-загрузки. Установщик маскируется под обновление Adobe Flash Player, однако на деле доставляет на компьютер два вредоносных скрипта. Первый изменяет

настройки интернет-соединения так, чтобы весь трафик проходил через порт 8003, прослушиваемый злоумышленниками, а второй добавляет в связку ключей корневой сертификат безопасности.

Помимо этого, в инфицированную систему устанавливается локальный прокси-сервер Titanium Web Proxy — кроссплатформенная утилита с открытым исходным кодом, которая запускается на macOS, используя платформу MONO. С момента установки программы весь трафик, передаваемый браузером Safari, перехватывается и, при необходимости, изменяется.

Благодаря наличию действительного корневого сертификата прокси-сервер имеет возможность на лету генерировать сертификаты SSL/TLS для запрашиваемых сайтов. Это позволяет зловреду прослушивать не только HTTP-трафик, но также защищенные соединения.

Реализовав таким образом классическую схему атаки «человек посередине», операторы вредоноса пока лишь изменяют результаты поисковых запросов пользователя. ИБ-специалисты считают, что таким образом они монетизируют свою разработку, внедряя в выдачу рекламные объявления, которыми изобилует Bing. Тем не менее, этим же методом можно модифицировать трафик для любых сайтов, а также перехватывать конфиденциальные данные жертвы.

Скорее всего, появление вредоносной программы стало ответом злоумышленников на изменение политики безопасности Safari, где после выхода macOS Mojave были запрещены сторонние плагины и выполнение сценариев AppleScript…» ***(Maxim Zaitsev. macOS-зловред подменяет выдачу Google на результаты Bing // Threatpost (https://threatpost.ru/macos-malware-intercepts-google-traffic-to-inject-bing-results/32973/). 06.06.2019).***

***

«Всплеск атак ботнета Hakai зафиксировали ИБ-специалисты Netscout. Нападающие эксплуатируют уязвимость SDK Realtek, найденную еще в 2014 году. Основной целью киберпреступников являются роутеры, расположенные в Южной Африке — на долю этой страны приходится более 80% попыток взлома в рамках данной кампании.

Резкий рост атак на маршрутизаторы, использующие SDK Realtek, начался в конце апреля этого года. На пике кампании ловушки исследователей фиксировали более 600 нападений в сутки. Большая часть атак исходила из Египта и была направлена на роутеры, расположенные в Южной Африке. Также чуть более 8% целей находилось в Европе и около 3,5% — в азиатских и тихоокеанских странах.

Злоумышленники эксплуатируют уязвимость CVE-2014-8361 в пакете разработчика для чипов Realtek. Эти микросхемы используются в коммуникационном оборудовании различных марок, например маршрутизаторах D-Link и TRENDnet. Проблема связана с работой сервиса miniigd SOAP. Она позволяет нападающему повысить свои привилегии, а также удаленно выполнить код на устройстве.

В рамках зафиксированных исследователями инцидентов на уязвимые роутеры доставляется клиент ботнета Hakai, предназначенный для организации DDoS-атак. Злоумышленники устанавливают на устройство скрипт,

ориентированный на работу в среде MIPS-процессоров, однако исследователи отмечают, что нашли на командном сервере варианты полезной нагрузки и для чипов других архитектур.

В атаках на южноафриканские IoT-устройства применяется оригинальная сборка Hakai, которая помимо стандартных для этого семейства зловредов функций обладает возможностью проводить DDoS-атаки против игровых серверов. Аналогичной возможностью располагает ботнет Mirai.

Hakai впервые попал на глаза ИБ-специалистам летом прошлого года. Зловред разработан на основе слитого в сеть кода QBot, однако впоследствии он получил несколько дополнений, расширяющих его возможности. Первоначально зомби-сеть строилась на уязвимых маршрутизаторах Huawei HG352. Позже она стала атаковать также роутеры D-Link при помощи нескольких разных эксплойтов.» ***(Julia Glazova. Ботнет Hakai атакует южноафриканские роутеры // Threatpost (https://threatpost.ru/hakai-botnet-attacks-south-african-routers/32917/). 03.06.2019).***

***

«Аналитики «Лаборатории Касперского» изучили Android-троян Riltok, который охотится за платежными данными пользователей в России, Франции и других европейских странах. Зловред перехватывает информацию через веб-инжекты, скрывает уведомления от банковских приложений и блокирует антивирусные процессы.

Эксперты объединяют в семейство Riltok трояны, в составе которых есть библиотека librealtalk-jni.so. Она обеспечивает обмен данными с управляющим сервером, обновление вредоносных функций и взаимодействие с зараженным устройством.

Как правило, операторы Riltok маскируют свой троян под приложения сервисов онлайн-объявлений, распространяя ссылки на него через SMS. Исследователи также находили кампании, в которых зловред притворялся сервисом для поиска авиабилетов и некого магазина Android-приложений.

Попав на мобильное устройство, Riltok запрашивает доступ к службе специальных возможностей AccessibilityService — якобы из-за ошибки при установке. Всплывающее окно появляется раз за разом, пока жертва не даст разрешение. Далее Riltok перехватывает контроль над SMS и уходит в скрытый режим.

Доступ к AccessibilityService позволяет трояну открывать поддельные окна для кражи персональных данных. Такие формы могут выглядеть как уведомления от Google Play или банковских приложений — их список вшит в библиотеку librealtalk-jni.so. Последние поколения зловреда сразу открывают в браузере фишинговую страницу.

Помимо перехвата SMS, Riltok способен скрывать уведомления от легитимных приложений и сворачивать антивирусные программы. Полученные платежные данные троян проверяет на отсутствие ошибок по контрольной сумме номера и длине CVC. У зловреда также есть черный список номеров, с которым он сверяется в ходе работы…» ***(Egor Nashilov. Троян Riltok расширил географию***

атак на Европу // Threatpost (https://threatpost.ru/easy-easy-riltok/33261/). 26.06.2019).

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«В понедельник суд Олд-Бейли приговорил к четырем годам тюремного заключения 22-летнего Дэниэла Келли (Daniel Kelley). Он был причастен к крупной хакерской атаке на TalkTalk, одну из четырех крупнейших телекоммуникационных компаний в Великобритании.

Нападение было совершено в 2015 году и привело к утечке адресов электронной почты и банковских реквизитов более 150 тыс. пользователей. Всего в скомпрометированной базе хранилась информация о более чем полутора миллионах человек. Общий ущерб от последующих кибератак составил 77 млн фунтов стерлингов.

Келли также признал себя виновным еще в 10 атаках. Они затронули несколько организаций, в числе которых был валлийский Колледж Сэр Гар, где учился будущий киберпреступник.

Келли, в то время 16-летний подросток, не смог набрать достаточно баллов, чтобы попасть на компьютерные курсы желаемого уровня. По мнению прокурора Питера Рэтлиффа (Peter Ratliff), эта неудача подтолкнула его к первому нападению: Келли провел DDoS-атаку на сайт своего колледжа, парализовав его работу. Серия организованных им в период с сентября 2013 года по апрель 2014 года кибератак стоила учебному заведению сотен часов учебного времени. Некоторые студенты покинули колледж из-за сорванных экзаменов.

Эта серия атак также имела более широкие и опасные последствия. Сеть колледжа была связана с сетью валлийского правительства (PBSA), таким образом, нападения затронули больницы, аварийные службы и учебные заведения.

В частности, был нарушен уход за тяжелобольными пациентами в больнице принца Филиппа в Лланелли и госпиталя Витибуш в Хаверфордуэсте. Медики потеряли доступ к диагностическим изображениям, что привело к «серьезному клиническому риску катастрофического исхода». Устранение последствий атаки стоило почти 400 000 фунтов стерлингов.

2 июля 2015 года валлийское подразделение по борьбе с киберпреступностью арестовало Келли в его доме в Лланелли и конфисковало все цифровые устройства. Однако после освобождения под залог он продолжил свою преступную деятельность — уже с корыстными целями.

Как выяснилось позже, Келли вошел в состав группировки, которая организовала нападение на TalkTalk, еще находясь под следствием за атаку на колледж.

Серия организованных им кибератак с вымогательством криптовалюты затронула такие компании, как RC hobbies, For the Record и JJ Fox Ltd. Во всех

нападениях Келли использовал схожую схему — компрометировал персональные данные пользователей, затем связывался с руководством компаний и требовал средства в биткойнах в качестве выкупа за непричинение вреда. Если жертва отказывалась платить, он выставлял скомпрометированные данные на продажу в даркнете.

При аресте в ноябре 2015 года на компьютере Келли были найдены файлы, содержащие тысячи записей кредитных карт. Стоимость этих данных на черном рынке составляет около 105 000 фунтов стерлингов…» ***(Dmitry Nazarov. Взломщик клиентской базы TalkTalk приговорен к 4 годам тюрьмы // Threatpost (https://threatpost.ru/talktalk-hacker-sentenced-to-4-years-in-prison/33067/). 13.06.2019).***

***

«В федеральном суде округа Колумбия оглашены обвинения, выдвинутые против администраторов и участников форума Darkode. На сайте в течение нескольких лет осуществлялась купля-продажа вредоносного ПО — в частности, Bfbot, на основе которого был построен многомиллионный ботнет Mariposa.

Криминальная площадка Darkode была создана в 2008 году и просуществовала вплоть до лета 2015-го, когда ее удалось ликвидировать совместными усилиями правоохранительных органов разных стран. В пору своего расцвета закрытое англоязычное сообщество насчитывало около 300 участников, среди которых также числился Gribodemon — создатель банковского трояна SpyEye.

Расследование деятельности Darkode было запущено после того, как выявилась его связь с операторами Mariposa — крупнейшей бот-сети, охватившей 190 стран и составленной из 12,7 млн зараженных Windows-устройств. Ботнет был построен на основе p2p-червя Bfbot, он же Palevo, Rimecud и Butterfly Flooder. Этот зловред-полиморфик открывает на машине бэкдор и по команде загружает другое вредоносное ПО — кейлоггеры, банковские трояны, модули для проведения DDoS-атак.

Лица, предположительно причастные к созданию и распространению Bfbot, были с подачи ФБР задержаны в Испании и Словении в 2010 году. В ходе судебного разбирательства вина автора Bfbot была доказана; житель Словении Матьяж Шкорьянц (Matjaž Škorjanc), известный в Сети как iserdo, получил на родине 4 года и 10 месяцев заключения. В настоящее время он уже на свободе…

На прошлой неделе суд округа Колумбия заслушал обвинительный акт в новой редакции. В деле прибавился еще один ответчик, житель штата Вашингтон Томас Мак-Кормик (Thomas McCormick), а текст документа был дополнен свидетельствами преступлений, подпадающих под статьи RICO (Racketeer Influenced and Corrupt Organizations Act) — американского закона об организованной преступности.

Всем фигурантам дела теперь также инкриминируется связь с преступным сообществом (Darkode). По версии следствия, создателем криминального форума, а

также его первым администратором являлся Шкорьянц, а последним — Мак-Кормик. За работу с клиентами отвечали Руис и Леники.

Все они также получали прибыль от торговли на Darkode. Шкорьянц продвигал Bfbot, создавая с помощью Руиса кастомные версии. Руис также занимался распространением зловреда, формировал базы краденых данных и продавал доступ к зараженным машинам в рамках схем pay-per-install, позволяющих загружать на ботнет другие вредоносные программы с оплатой каждой удачной установки.

Леники тоже приобрел Bfbot, создал собственный ботнет и продавал к нему доступ другим участникам форума. Мак-Кормик, купив модификацию Bfbot, занимался ее перепродажей на правах партнера. Кроме того, он выставлял на продажу копии мощного банкера ZeuS и похитителя информации ngrBot, созданного им со сторонней помощью.

В случае вынесения обвинительного приговора у ответчиков может быть конфисковано все имущество и денежные средства, нажитые противоправными методами.» ***(Maxim Zaitsev. Власти США внесли коррективы в дело о Mariposa // Threatpost (https://threatpost.ru/us-case-against-mariposa-creators-corrected-to-include-new-charges-forth-suspect/33032/). 11.06.2019).***

***

Технічні аспекти кібербезпеки

«…Команда исследователей из США, Австралии и Австрии разработала новый вариант атаки Rowhammer. В отличие от предыдущих версий новая атака под названием RAMBleed позволяет не только модифицировать данные и повышать привилегии, но и похищать хранящиеся на устройстве данные.

Rowhammer – это класс эксплоитов для аппаратной уязвимости (CVE-2019-0174) в современных картах памяти. По умолчанию данные в картах памяти хранятся в ячейках, расположенных на кремниевом чипе в рядах, образующих сетку. В 2014 году ученые обнаружили, что многократное чтение данных, хранящихся в одном ряду, приводит к возникновению электрического заряда, способного влиять на данные в соседних рядах. Атака получила название Rowhammer, и с ее помощью ученые могли либо повреждать данные, либо использовать их в вредоносных целях.

С 2014 года исследователи существенно расширили возможности оригинальной атаки, однако изъять из памяти и похитить данные с ее помощью удалось только сейчас.

Для того чтобы RAMBleed стала возможной, ученым удалось заставить распределитель памяти Linux (buddy allocator) выделить большой блок памяти последовательных физических адресов, позволивший им оркестровать атаку. Исследователи создали новый механизм «Frame Feng Shui» для размещения страниц программы жертвы в нужном месте физической памяти. Кроме того, они разработали новый метод управления данными в памяти и повторяющего их чтения (так называемый row hammering) для определения, какие данные находятся в

соседних ячейках памяти.» ***(Новый вариант Rowhammer теперь позволяет похищать данные // SecurityLab.ru (https://www.securitylab.ru/news/499451.php). 12.06.2019).***

***

«…Группа исследователей из Технического университета Граца (Австрия) разработала автоматизированную систему для создания профилей браузеров с помощью двух новых атак по сторонним каналам, позволяющих получить информацию об используемом программном и аппаратном обеспечении и более эффективно отследить браузер в интернете.

Результаты исследования специалисты представили в работе под названием «JavaScript Template Attacks: Automatically Inferring Host Information for Targeted Exploits». По их словам, новый метод облегчает отслеживание браузеров, помогает обойти ряд противодействующих слежке техник и демонстрирует, что обеспечивающие конфиденциальность браузерные расширения «допускают утечку большего объема информации, чем могут замаскировать».

Получение цифрового отпечатка браузера предполагает сбор данных о браузере пользователя, таких как связанное с ним ПО и аппаратное обеспечение, тип браузера, используемая операционная система, различные заголовки, cookie-файлы, расширения, разрешение экрана и пр. Данные сведения могут быть собраны с помощью JavaScript.

Разработанный учеными метод достаточно прост: на первом этапе создается профиль браузера на основе списка свойств, доступных из объектов JavaScript. На втором этапе проводится повторный сбор данных из другой среды (альтернативный браузер или ОС). Далее два профиля сводятся в единый шаблон, который затем используется для поиска вариаций. Эти вариации позволяют узнать связанные со средой свойства в Chrome, Edge, Firefox и мобильной версии Tor, с помощью которых можно получить представление об ОС, процессоре, установленных плагинах для обеспечения конфиденциальности и версии браузера.

Исследование ученых лишний раз показывает, что обеспечить полную анонимность в Сети достаточно сложно, даже в случае браузера Tor, разработанного с учетом защиты от слежки. Как пояснили эксперты, реализованные в Tor меры, призванные замаскировать цифровой след, могут оказаться неэффективными, если принимать во внимание дополнительные данные.» ***(Ученые изобрели новый метод отслеживания браузеров // SecurityLab.ru (https://www.securitylab.ru/news/499426.php). 11.06.2019).***

***

«Экспертам удалось обмануть системы верификации, узнающие пользователя по нажатиям клавиш.

Определить, является ли пользователь киберпреступником, можно по тому, как он работает с клавиатурой. Однако, как показывают последние исследования, подобные системы верификации вполне реально обмануть.

Киберпреступники непрерывно совершенствуют свои техники, и для обеспечения безопасности пользователей одних лишь антивирусных решений,

основывающихся на цифровых подписях, теперь уже недостаточно. В связи с этим ИБ-эксперты работают над новыми способами идентификации пользователей, в том числе по нажатиям клавиш на клавиатуре и движениям мыши. Тем не менее, специалисты Университета имени Бен-Гуриона в Негеве (Израиль) доказали, что подобные методы верификации также не являются на сто процентов надежными.

Исследователи представили атаку под названием Malboard, с помощью которой им удалось обмануть решения безопасности, проверяющие подлинность личности пользователя на основании характеристик его взаимодействий с клавиатурой.

Подобные системы верификации базируются не только на том, с какой скоростью пользователь набирает текст. Реакция на опечатки, привычные орфографические ошибки и другие элементы поведения также могут использоваться для подтверждения личности пользователя.

Специалисты Университета имени Бен-Гуриона в Негеве продемонстрировали, как злоумышленник может использовать скомпрометированную клавиатуру для имитации нажатий клавиш жертвой. Для исследования они взяли клавиатуры от Microsoft, Lenovo и Dell и с их помощью попытались обойти системы верификации пользователей по нажатиям клавиш KeyTrac, TypingDNA и DuckHunt.

Работая над Malboard, исследователи использовали данные о поведении 30 добровольцев, прошедших три разных теста по работе с клавиатурой. Зараженная Malboard клавиатура могла автоматически генерировать строки в стиле того или иного добровольца. С помощью нового метода исследователям удалось обмануть системы верификации в 83% случаев.» ***(Атака Malboard позволяет генерировать нажатия клавиш на клавиатуре в стиле жертвы // SecurityLab.ru (https://www.securitylab.ru/news/499373.php). 06.06.2019).***

***

«Японские исследователи из токийского Университета Васэда обнаружили способ скрытно подключаться к Android-смартфонам и манипулировать ими. Технология построена на уязвимостях NFC-соединения и особенностях работы емкостных экранов.

Для PoC-атаки, получившей название Tap’n Ghost («тапающий призрак»), используется целый комплект оборудования, включая небольшой компьютер, высоковольтный трансформатор и медный коврик, через который взломщик отправляет запросы об NFC-подключении. Эксперты указывают, что несмотря на количество приборов, их все же можно вмонтировать в стол или другую поверхность.

Особенность Android-устройств в том, что они постоянно сканируют эфир в поисках доступных соединений. Если жертва разместит свой смартфон в непосредственной близости от вредоносного объекта, подключение произойдет автоматически.

После этого зловредное устройство может заставить смартфон перейти по ссылке, принять сопряжение от стороннего Bluetooth-агента или подключиться к небезопасной WiFi-сети. Две последние операции требуют подтверждения со

стороны пользователя, для чего исследователи научились эмулировать прикосновения к экрану. Это становится возможным благодаря отправке электрических импульсов через медный передатчик — емкостный экран воспринимает их как контакт с пальцем.

Эксперты протестировали прием на семи смартфонах и добились успеха в пяти случаях. Эту же технологию можно использовать для атак на любые NFC-устройства с емкостным экраном, вплоть до банкоматов и машин для голосования. Правда, в каждом случае злоумышленнику потребуется подобрать нужные параметры, поскольку техника разных производителей может работать по-разному.

В настоящий момент исследователи призывают разработчиков Android повысить безопасность NFC-подключений на своих аппаратах. Для этого можно, например, добавить дополнительное подтверждение перед установкой соединения. От нежелательных манипуляций с емкостными экранами также можно защититься внедрением дополнительной защиты…» ***(Egor Nashilov. Ученые взломали Android-смартфоны через модуль NFC // Threatpost (https://threatpost.ru/poc-allows-taps-on-android-smartphones-with-copper-pad/32950/). 05.06.2019).***

***

«Хакерам не обов'язково проводити масивні кібератаки, щоб захопити контроль над девайсом. Вони можуть просто «підслухати» пароль до нього під час введення користувачем, кажуть науковці Університету Кембриджа та Університету Лінчепінга. Вони експериментально показали, що PIN-код можна визначити за звуковими хвилями, які генерують пальці під час торкання сенсорного екрана.

Для шпигування за паролем вистачить додатка, який використовуватиме мікрофон та розшифровуватиме запис. Така атака не лише здатна розпізнавати PIN-коди, а й визначає літери та слова.

Такий шкідливий додаток може легко проникнути в телефон. Відомі випадки мільйонної аудиторії у заражених програм в Google Play, а також поширення шкідливих програм із заводу виробника смартфона. При цьому, кажуть дослідники, запити ОС про дозвіл на користування своїми елементами юзери часто ігнорують і сліпо дозволяють усі запити.

В експерименті науковці використали нейромережу, яка визначала вібрації від окремих натиснень на екран. Експеримент проводили на двох смартфонах LG Nexus 5 та планшеті Nexus 9. Учасники дослідження вводили паролі в трьох різних місцях на території університету, де були різні рівні шуму: загальна аудиторія з кавовим автоматом, читальний зал з комп'ютерами та бібліотека.

Серед тестової групи у 45 осіб протягом кількох тестів система правильно розпізнавала паролі 7 із 27 разів, використовуючи на це 10 спроб. На планшетах результати були значно кращими – із 19 з 27 разів протягом 10 спроб.

Дослідники кажуть, що захистом від такого типу атаки може бути вимикач для мікрофона, який контролює користувач. Також можна оснастити мікрофон індикатором активності. Це може бути як спеціальний світлодіод, що спалахує при записі звука, так і іконка на екрані.» ***(Євген Корольов. Зловмисники можуть «підслухати» PIN-код, який ви друкуєте на екрані // Tech Today***

(https://techtoday.in.ua/news/zlovmysnyky-mozhut-pidsluhaty-pin-kod-shho-vy-drukuyete-na-ekrani-115791.html). 11.06.2019).

***

«Технический директор РосКомСвободы Станислав Шакиров прокомментировал «сердечный приступ интернета», произошедший из-за ошибки американского провайдера Verizon, который затронул работу таких глобальных сервисов, как Cloudflare, Amazon, Reddit и Twitch

Недавно работе многих крупных интернет-сервисов произошел сбой, он затронул, в частности, облачный сервис Amazon, сайт Reddit, стриминговую платформу Twitch, мессенджер Discord и сервис Downdetector, который сам отслеживает сбои в интернете. Сбой произошел около двух часов дня по московскому времени (в семь утра на востоке США) и продлился примерно два часа.

Проблему изначально связали с крупным сервисом доставки контента Cloudflare, услугами которого пользуются миллионы сайтов. Компания заявила, что потеряла около 15% своего мирового трафика, однако ее собственные системы работали нормально: трафик не доходил до нее из-за чужих ошибок — в том числе, компании Verizon, одной из крупнейших телекоммуникационных компаний в США. Cloudflare опубликовала в своем блоге большой пост про причины сбоя (и с жесткой критикой Verizon), в котором описала случившееся словами «у интернета произошел небольшой сердечный приступ». Интернет-провайдер из Пенсильвании DQE Communications некорректно сконфигурировал маршрутизацию порядка 2% мирового интернета через свою сеть и сеть клиента — металлургической компании Allegheny Technologies. Источник ошибки был в настройке оптимизатора BGP — основного протокола динамической маршрутизации современного интернета.

Неверную конфигурацию почему-то принял и передал всему миру владелец шлюза DQE в магистральный интернет — компания Verizon. Allegheny тоже клиент Verizon, и, возможно, это спровоцировало ошибку. Трафик, предназначенный для гигантов интернета, пошел через маломощную сеть. Это вызвало каскадные отказы в обслуживании, больше всего от которых пострадали клиенты Cloudflare — защищенного облачного хостинга, «держащего» в том числе приложение для подкастов Overcast и мессенджер Discord. Многие сайты на хостинге были недоступны несколько часов, на пике хостинг лишился 10% трафика.

Руководитель Cloudflare Мэтью Принс заявил: «Сотрудникам Verizon и Noction [разработчик оптимизатора BGP] должно быть очень стыдно за то, что их небрежность затронула Cloudflare и значительную часть интернета. То, что BGP настолько неустойчив, — абсурд. Еще абсурднее то, что Verizon принимает маршрутизацию без простейших фильтров».

Инцидент показал, что интернет-протокол, о котором и не подозревают большинство пользователей, способен прямо повлиять на их жизнь — и что использовать BGP в подрывных целях очень легко. Похожая ошибка маршрутизации стала причиной беспрецедентного сбоя WhatsApp, Instagram и Facebook в марте, а сбой Google в ноябре 2018 года вызвал один небольшой

нигерийский провайдер…». ***(Глобальный обвал Сети продемонстрировал возможные риски «суверенного» интернета // РосКомСвобода (https://roskomsvoboda.org/47830/). 26.06.2019).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«…Компания Cisco исправила в пользовательском web-интерфейсе своего продукта IOS XE опасную уязвимость, позволяющую посторонним проникать во внутренние сети без авторизации. Уязвимость межсайтовой подделки запросов (CSRF) получила идентификатор CVE-2019-1904.

Cisco IOS XE – это сетевая операционная система на базе ядра Linux, использующаяся на различных маршрутизаторах корпоративного уровня и коммутаторах Cisco Catalyst. Версии IOS, IOS XR и NX-OS уязвимости не подвержены.

Причиной проблемы является недостаточная защита web-интерфейса от CSRF. Злоумышленник может воспользоваться ею, заставив пользователя пройти по вредоносной ссылке (к примеру, эксплоит можно спрятать в вредоносной рекламе). Поскольку уязвимость можно проэксплуатировать совершенно незаметно, она является весьма привлекательным инструментом для киберпреступников.

Успешная эксплуатация уязвимости позволяет злоумышленнику выполнять любые действия с теми же правами, что есть у атакуемого пользователя. «Если у пользователя есть права администратора, атакующий может менять конфигурацию, выполнять команды или перезагружать затронутое устройство», – пояснили специалисты Cisco.

Единственный способ исправить уязвимость – установить последние обновления (доступны только для пользователей с действительной лицензией). PoC-эксплоит для уязвимости уже существует, однако никаких свидетельств ее эксплуатации в реальных атаках обнаружено не было.» ***(Уязвимость в Cisco IOS XE позволяет проникнуть в сети через вредоносную рекламу // SecurityLab.ru (https://www.securitylab.ru/news/499461.php). 14.06.2019).***

***

«Компания Adobe выпустила обновления для Flash Player и платформы ColdFusion, в которых объявились программные ошибки, грозящие исполнением произвольного кода.

Совокупно разработчик устранил 11 уязвимостей в трех продуктах, включая маркетинговое решение Adobe Campaign. В итоге новый набор плановых патчей оказался гораздо скромнее предыдущего — в мае Adobe суммарно залатала 87 брешей.

Из новых уязвимостей наиболее опасны те, что были обнаружены в коммерческой платформе Adobe ColdFusion, предназначенной для ускорения разработки веб-приложений. «Adobe выпустила обновления для системы безопасности ColdFusion 2018, 2016 и 11, — сказано в бюллетене. — Эти апдейты устраняют три критические уязвимости, которые могут повлечь исполнение произвольного кода».

Баги классифицируются как обход черного списка файловых расширений (CVE-2019-7838), возможность внедрения команд (CVE-2019-7839) и десериализация недоверенных данных (CVE-2019-7840). Патчи включены в состав обновлений ColdFusion 2018 Update 4, ColdFusion 2016 Update 11 и ColdFusion 11 Update 19. Разработчик рекомендует их установить в течение месяца, так как продукт относится к группе повышенного риска.

В равной степени опасна возможность использования высвобожденной памяти в Adobe Flash (CVE-2019-7845), которую выявил участник проекта Zero Day Initiative (ZDI), пожелавший остаться неизвестным. «Уязвимость use-after-free проявляется при обработке объектов LocalConnection, — пояснил для Threatpost представитель ZDI Дастин Чайлдс (Dustin Childs). — Выполняя действия в ActionScript, злоумышленник может спровоцировать повторное использование указателя после его освобождения. Уязвимость позволяет выполнить любой код в контексте текущего процесса».

Проблема актуальна для десктопных и браузерных Flash Player всех прежних выпусков; пользователям настоятельно рекомендуется установить обновление 32.0.0.207.

Остальные уязвимости были найдены в пакете Adobe Campaign, призванном облегчить создание многоканальных и персонализированных сообщений, а также управление ими. Это критический баг внедрения команд (CVE-2019-7850), пять ошибок, чреватых раскрытием информации (две оценены как существенные, три — как умеренно опасные), а также возможность XML-инъекций, позволяющая получить доступ на чтение к произвольному объекту файловой системы.

Уязвимостям подвержены Adobe Campaign Classic 18.10.5-8984 и более ранние сборки, установленные на Windows и Linux. Проблемы решает установка обновления 19.1.1-9026.

Ботнет GoldBrute атакует хосты с открытым RDP-доступом и угрожает более чем 1,5 млн устройств. К такому выводу пришли ИБ-специалисты, которым удалось изучить код вредоносной программы и результаты сканирования потенциально уязвимых портов, а также список логинов и паролей для брутфорс-нападения. Наибольшее количество целей находится в странах Юго-Восточной Азии, США и Европе.

Как утверждают исследователи, ботнет сканирует Интернет в поиске открытых RDP-портов и пытается подобрать учетные данные администратора при помощи credential stuffing или же перебором из собственной базы слабых паролей. Получив доступ к уязвимой машине, GoldBrute устанавливает WebSocket-соединение с командным сервером через порт 8333. Адрес хоста жестко задан в коде клиента, а сообщения шифруются ключом AES.

Зловред загружает на целевое устройство архив размером около 80 Мб с основным скриптом GoldBrute и Java-оболочкой для его исполнения. После распаковки вредоносная программа получает имя bitcoin.dll, хотя на самом деле является JAR-объектом. Далее бот приступает к поиску новых целей и передает на командный сервер адреса потенциально уязвимых компьютеров.

Как только клиент находит 80 машин с открытыми RDP-портами, центр управления объединяет их в пул целей для проведения атаки. Для обхода систем безопасности проверка одной пары «логин + пароль» для каждого IP проводится с уникального адреса, принадлежащего зараженному устройству.

Исследователи не сообщают об иных деструктивных действиях, которые выполняет зловред. Ботнет находится в стадии роста — по информации ИБ-специалистов, в его базе сейчас находится более 1,5 млн доступных для атаки хостов. Не исключено, что зараженные машины в дальнейшем будут использованы для новых вредоносных кампаний…» ***(Dmitry Nazarov. В списке целей ботнета GoldBrute более 1,5 млн хостов // Threatpost (https://threatpost.ru/goldbrute-botnet-holds-1-5m-computers-at-gunpoint/33010/). 10.06.2019).***

***

«Фахівці в області кібербезпеки виявили небезпечну вразливість Windows, яка дозволяє зловмисникам обійти блокування екрану. Дані про проломи опубліковані на сторінці Інституту Програмної Інженерії американського Університету Карнегі Меллон. Схоже, компанія так і не змогла за 90 днів вирішити цю проблему, так що експерти опублікували принцип злому. Схоже, тепер мільйони користувачів під загрозою злому, а хакери вже потирають руки.

Уразливість дозволяє обійти двофакторну аутентифікацію. Вона зачіпає протокол RDP (Remote Desktop Protocol - віддаленого робочого столу) і пов'язана з перевіркою на рівні мережі: при відновленні перерваного підключення з екрану автоматично знімається блокування. Саме тут Microsoft зробила помилку, за яку поплатяться мільйони користувачів Windows 10. Практично щотижня в ОС Windows виявляють нову уразливість, яку не змогла передбачити Microsoft.

За допомогою нової уразливості, хакеру навіть не потрібно встановлювати фізично доступ до ПК - злом відбувається віддалено.

Під загрозу потрапили деякі версії Windows 10. Експерти присвоїли уразливості код CVE-2019-9510.» ***(У Windows 10 виявили нову вразливість: хакери потирають руки // znaj.ua (https://techno.znaj.ua/237791-u-windows-10-viyavili-novu-vrazlivist-hakeri-potirayut-ruki). 06.06.2019).***

***

«Специалисты по кибербезопасности из Trend Micro сообщили, что уязвимость, обнаруженная в апреле в сервере Oracle WebLogic, используется для установки вирусов-майнеров.

Уязвимость CVE-2019-2725 в сервере Oracle WebLogic позволяет устанавливать сертификат, содержащий специальный файл, в котором зашифрована ссылка на вредоносный PowerShell-скрипт

Trojan.PS1.MALXMR.MPA. После скачивания данный скрипт, в свою очередь, скачивает и устанавливает майнер для добычи Monero (XMR).

«Идея использования сертификатов для сокрытия вредоносного кода уже не нова. Однако в данном случае, чтобы избежать обнаружения вируса, используется двойное шифрование. Тем более, что файл сертификата выглядит легитимным и скачивается через HTTPS-соединение», – сказали исследователи.

При этом остальные файлы скачиваются напрямую без каких-либо приемов для обмана антивирусного ПО, отметили специалисты по кибербезопасности. Они также подчеркнули, что компаниям, использующим в работе сервера Oracle WebLogic, необходимо установить последние обновления для программы.» ***(Сервер Oracle WebLogic заразили вирусами-майнерами // LetKnow OÜ (https://letknow.news/news/uyazvimost-v-oracle-weblogic-ispolzuetsya-dlya-ustanovki-virusov-maynerov-24582.html). 11.06.2019).***

***

«Користувачам операційної системи WINDOWS рекомендують встановити останні оновлення, аби не допустити чергової масової кібератаки. Рекомендації розмістив Департамент кіберполіції Національної поліції України.

Спеціалісти виявили вразливість операційних систем версій Windows 7, Windows Server 2003, Windows Server 2008 та більш старих версій Windows. Якщо не виконати їх оновлення, хакери зможуть скористатись цими вразливостями для віддаленого використання враженого комп'ютера та викрадення конфіденційної інформації.

Щоб не допустити чергової масової атаки, Кіберполіція радить користувачам операційної системи Windows (більш старих її версій) оновити систему до останньої версії для усунення вразливостей попередньої версії. Нехтування таких дій може призвести до витоку особистої інформації, яка міститься на персональному комп'ютері, а в бізнесі - до великих матеріальних втрат…» ***(Українцям радять оновити WINDOWS для захисту від кібератак // Інформаційне агенство "ЛІГА:ЗАКОН (https://buh.ligazakon.net/ua/news/187169_ukrantsyam-radyat-onoviti-windows-dlya-zakhistu-vd-kberatak).***

***

«…Уязвимость в инсулиновых помпах Medtronic MiniMed позволяет злоумышленникам менять настройки устройства и контролировать введение инсулина пациенту.

Проблема связана с механизмом беспроводной радиосвязи, использующимся помпами Medtronic для обмена данными с другим оборудованием (глюкометрами, сенсорами глюкозы и USB-устройствами CareLink). Уязвимость (CVE-2019-10964) существует из-за отсутствия надлежащей авторизации и аутентификации в протоколе радиосвязи. С ее помощью группе исследователей удалось перехватить передаваемые данные и внедрить подмененные. По шкале оценивания опасности CVSS v3 уязвимость получила 7,1 балл из максимальных 10.

Medtronic рекомендует пользователям уязвимых помп в США обсудить со своими лечащими врачами возможность их замены на новые, более защищенные модели. Пациенты за пределами США получат соответствующие уведомления с инструкциями, разработанными специально с учетом страны их проживания…» ***(Уязвимость в инсулиновых помпах Medtronic MiniMed ставит под угрозу здоровье пациентов // SecurityLab.ru (https://www.securitylab.ru/news/499680.php). 28.06.2019).***

***

«…В IIoT-платформе Advantech WebAccess/SCADA выявлен ряд опасных уязвимостей, в том числе критических, которые позволяют получить доступ к информации, удалить файлы или удаленно выполнить произвольный код. Проблемы затрагивают версию Advantech WebAccess/SCADA 8.3.5 и более ранние релизы.

К числу наиболее опасных относятся уязвимости CVE-2019-10993, CVE-2019-10987, CVE-2019-10989 и CVE-2019-10991. Все они позволяют удалено выполнить код. Проблемы CVE-2019-10987, CVE-2019-10989 и CVE-2019-10991 связаны с отсутствием корректной проверки пользовательских данных. Уровень опасности вышеперечисленных уязвимостей варьируется от 8,8 до 9,8 баллов по шкале CVSS v3.

Уязвимости CVE-2019-10985 и CVE-2019-10983 также связаны с отсутствием корректной проверки данных. Воспользовавшись первой, злоумышленник может удалить файлы под видом администратора, а с помощью второй - получить доступ к данным.

Производитель устранил вышеописанные проблемы с выпуском версии WebAccess/SCADA 8.4.1. Обновление доступно на сайте Advantech.

Advantech WebAccess - интегрированная панель, позволяющая контролировать промышленную IoT-инфраструктуру. Решение используется для диспетчерского управления производственными процессами и работы с человеко-машинными интерфейсами.» ***(В IIoT-платформе Advantech WebAccess обнаружен ряд опасных уязвимостей // SecurityLab.ru (https://www.securitylab.ru/news/499681.php). 28.06.2019).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«…На конференции IBM Security Summit в Варшаве компания IBM показала передвижной центр X-Force Command Cyber Tactical Operations Center (C-TOC), позиционируемый как первый в своем роде центр мониторинга и реагирования на инциденты в области информационной безопасности на колесах.

C-TOC представляет собой 23-тонный грузовик, полностью оснащенный всем необходимым оборудованием центра оперативного киберреагирования.

Центр может использоваться в качестве учебного киберполигона, для имитации внешних атак, проведения соревнований «захват флага» или наблюдения за специальными событиями безопасности, что позволит сотрудникам, вовлеченным в процесс оперативного реагирования (от специалистов SOC до руководства высшего звена), оценить готовность к реальным атакам и усовершенствовать стратегию кибербезопасности и реагирования на инциденты.

На протяжении 2019 года C-TOC проедет по городам Европы в целях мобильного обучения кибербезопасности. В первом квартале нынешнего года C-TOC побывал Великобритании, Ирландии, Нидерландах, Испании, Швейцарии и Франции.

Согласно статистике, приведенной IBM, компании, способные ответить на кибератаку в течение 30 дней, могут сэкономить более $1 млн. Однако скоординированный план реагирования на ИБ-инциденты имеют менее 25% опрошенных организаций и предприятий.» ***(В Польше представлен мобильный центр мониторинга и реагирования на киберинциденты // SecurityLab.ru (https://www.securitylab.ru/news/499411.php). 10.06.2019).***

***

«Компания Eset, ведущий европейский разработчик средств информационной безопасности, представила новое бизнес-решение Enterprise Inspector, предназначенное для предотвращения, обнаружения и реагирования на киберинциденты в корпоративной сети.

Согласно исследованию консалтинговой компании PricewaterhouseCoopers (PwC), 41% опрошенных инвесторов, аналитиков и владельцев компаний признают кибератаки самой серьезной угрозой для бизнеса. Компаниям необходима надежная система корпоративной защиты, чтобы новые киберугрозы, потенциально опасные действия сотрудников и нежелательные приложения не подвергали риску репутацию и финансовую стабильность организации.

Eset Enterprise Inspector – решение для многоуровневой защиты конечных точек, которое анализирует большие объемы информации в режиме реального времени, получая данные от каждого уровня защиты. Детектирование угроз осуществляется на основе репутации, поведения и ретроспективного анализа.

Гибкие настройки позволяют клиентам адаптировать решение к своим потребностям, а также обеспечивает обнаружение и своевременную реакцию на все типы киберугроз.

Продукт поддерживает не только проактивный поиск угроз, но и ретроспективный анализ. Достаточно настроить правила поведения, а затем «сканировать» базу данных событий. Поиск осуществляется не только по статическим IoC, но и на основе динамического анализа поведения с несколькими параметрами.

Продукт позволяет оперативно распознавать, анализировать и устранять любые угрозы безопасности в сети, в том числе обнаруживать APT-угрозы;

блокировать бесфайловые атаки; блокировать угрозы нулевого дня; защищать от программ-вымогателей; нейтрализовать state-sponsored кибератаки.

Сотрудники службы информационной безопасности могут завершать процессы, загружать файлы, вызвавшие срабатывание, удаленно выключить компьютер или перезапустить его прямо из консоли. Для более точной настройки решения можно легко редактировать правила с помощью XML, а также осуществить интеграцию с SIEM-системой.

Для выстраивания полноценной экосистемы безопасности Eset Enterprise Inspector используется вместе с другими продуктами Eset, что обеспечивает комплексную защиту конечных точек.» ***(Eset Enterprise Inspector поможет защитить корпоративную сеть // Компьютерное Обозрение (https://ko.com.ua/eset_enterprise_inspector_pomozhet_zashhitit_korporativnuyu_set_129016). 07.06.2019).***

***

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

Даник Ю. Г. Основи кібербезпеки та кібероборони: підручник / Даник Ю. Г., Воробієнко П. П., Чернега В. М. - Одеса : ОНАЗ ім. О. С. Попова, 2018. - 227 с.

Розглянуто роль і місце кібербезпеки у системі національної безпеки держави. Надано аналіз побудови системи кібербезпеки. Приділено увагу технологіям дій у кіберпросторі.

Шифр зберігання НБУВ: ВА831646

***

Кибербезопасность и качество электрической энергии в системах электроснабжения медицинских объектов : учеб. пособие. - Харьков, 2019. - 259 с.

Розглянуто загальні питання кібербезпеки та якості електричної енергії в системах електропостачання медичних об’єктів.

Шифр зберігання НБУВ: ВА832143

***

Концептуальні засади менеджменту та фінансів в умовах глобальної нестабільності = Conceptual foundations of management and finance in conditions of global instability : зб. матеріалів VI Міжнар. наук.-практ. інтерент-конф. «Актуальні проблеми менеджменту та фінансів в сучасних глобалізаційних процесах», 14 берез. 2019 р. - Ірпінь, 2019. - 497 с.

Зі змісту:

- Ковернінська Ю.В. Світовий досвід щодо страхування кіберризиків.

Шифр зберігання НБУВ: ВА831639

***

Чернишов Г.М. Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження / Г.М.Чернишов // Прикарпатський юридичний вісник. - 2018. - Вип. 3(24). - С. 158-162.

На підставі детального теоретичного аналізу розкрито сутність та надано кримінологічне визначення поняття «кіберзлочинність». Розкрито основні прояви кіберзлочинності, передбачені міжнародними документами та актами вітчизняного законодавства.

Шифр зберігання НБУВ: Ж74200

***

Шевченко А. С. Аналіз застосування штучних нейронних мереж у задачах виявлення кіберзагроз / А. С. Шевченко, І. В. Самойлов, О. А. Пономарьов, О. Г. Науменко // Збірник наукових праць [Військового інституту телекомунікацій та інформатизації]. - 2018. - Вип. 4. - С. 141-146.

Проананлізовано застосування штучних нейронних мереж у прикладних задачах забезпечення виявлення та класифікації кіберзагроз. Розглянуто структуру штучних нейронних мереж, математичні основи їх роботи, основні етапи обробки даних при використанні для вирішення задач виявлення кібернетичних загроз.

Шифр зберігання НБУВ: Ж71640

***

Шимченко Л. А. Кіберзагрози в Україні як проблема в умовах геополітичного суперництва / Л. А. Шимченко // Економічний вісник університету. - 2019. - Вип. 40. - С. 70-76.

Проведено дослідження проблематики геостратегічного суперництва, де основну увагу звернуто на кіберборотьбу. Встановлено, що кібербезпекова проблематика дедалі більше стає проблемою і національного рівня, що простежується в швидкості прийняття нормативно-правових рішень з узаконеними механізмами протидії кіберзагрозам, в створенні спеціальних кіберпідрозділів для забезпечення кіберпротистояння та ін. Акцентовано увагу на тих кіберзагрозах, що були найбільш резонансними в останні роки для українського суспільства і держави та звернуто увагу на застосовуваних владою механізмах протидії.

Шифр зберігання НБУВ: Ж73720

***