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

№ 11 (листопад)

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. – №11 (листопад) . – 104 с.

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

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

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

ЗМІСТ

«…Чому Україна не має альтернативи діджитал-трансформації та чи варто цього боятись, …розповів фахівець з цифрової безпеки, інтелектуальних систем громадської безпеки у Dell Technologies Бернхард Отупал.

Про діджитал-трансформацію

Україна не має альтернативи діджиталізації. І мова йде не лише про трансформацію міст, але про зміни загалом: діджитал-суспільство, діджитал-місто, діджитал-країна тощо. Ми не можемо говорити лише про один напрямок. Це повинно бути комплексне рішення…

Але він вам необхідний. До прикладу, у Києві ви маєте міську адміністрацію, до якої входить електрика, вода, сміття, транспорт. Це різні сфери, але всі вони мають єдине адміністрування, спільний бюджет, спільну ІТ-систему тощо. Однак, ви маєте окремий департамент водопостачання, окремий департамент транспорту і так далі. При цьому запровадивши систему розумного міста, ви отримуєте кращу централізацію, економію коштів і вищий рівень захисту даних. Адже ви точно знаєте, хто шукав певну інформацію, коли він це робив і з якою метою.

Окрім того, можна запропонувати кращі рішення для потенційних проблем, тобто прогнозованих, таких, що можуть виникати. Дуже простий приклад: ми знаємо, що у такий-то час відбувається важливий футбольний матч, отже можна припустити, що під час перерви у матчі різко зросте використання електрики та води, адже глядачі побіжать до кухні чи вбиральні. Тож це навантаження можна запланувати наперед.

Або скажу на прикладі транспорту. Вранці трафік на дорогах значно вищий, ніж всередині дня. Тоді ж буде значно вищий рівень забруднення у повітрі. І всі ці речі можна спрогнозувати, знайти рішення і контролювати. Це стосується і безпеки. Якщо ви знаєте, що вранці на дорогах значно більше транспорту, шанс ДТП теж вищий, отже потрібно і більше поліції.

Про втручання у приватність

Багато людей справді бояться, що такий контроль може бути перевищенням повноважень влади. Хоча Китай (до досвіду якого часто апелюють скептики) – це негативний приклад такого прогресу. Адже ця країна значно відрізняється від більшості у світі. Люди там мають дещо інше мислення. А населення складає понад мільярд людей, тож підхід до контролю інший. У наших країнах таких проблем із контролем не виникає.

До речі, те, як вони використовують технології – цікавий приклад. Китайський громадянин має свій рейтинг. І якщо його поведінка задовільна, із точки зору влади, то він отримує бали. Але якщо він учинив якесь дрібне правопорушення, наприклад, викинув сміття із вікна чи перевищив швидкість, то він утрачає ці бали. В результаті, людина з поганим рейтингом не зможе отримати швидший інтернет або замовити кращий рівень послуг.

Наголошу: не варто боятися, що влада отримує доступ до ваших даних. Це не означає, що "інформація буде використана проти вас", її застосують аби захистити вас та покращити сервіс.

Скажімо, система справді відслідковує ваше пересування – щодня ви їздите з пункту А до пункту Б. Тож апарат може прорахувати і запропонувати вам кращий маршрут. Користувачеві вигідно, щоб цю інформацію знали й аналізували.

Про захист персональних даних

Насправді, дуже часто проблема із витоком персональних даних – це вина самих користувачів. Більшість просто не читає умови, а одразу погоджується, навіть не знаючи на що дає свою згоду. Останнім часом було дуже багато критики навколо збору даних Facebook. Але соцмережа збирає лише ті дані про користувачів, на які вони дають згоду.

З іншого боку, проблема таких угод в тому, що вони надто довгі і складні для розуміння, тому користувачі й не хочуть їх читати. Я думаю, їх потрібно зробити коротшими і зрозумілішими для широкого кола людей. В Євросоюзі існує регламент щодо захисту персональних даних усіх осіб (GDPR). Це важливий крок щодо регуляції захисту персональних даних.

Про уразливість до хакерських атак

Раніше аби викрасти гроші – йшли грабувати банк. Зараз це роблять через інтернет. Тобто, хакерство – це той же кримінал, тільки в іншому вигляді.

Але на мою думку, простіше захистити інформацію і дані від хакерів, аніж організувати, наприклад, фізичну систему захисту будівлі. Зараз важливо встановлювати надійний захист всередині, зокрема, програми захисту серверів, антивірусні програми тощо.

Про ознаки розумного міста

Якщо місто є "розумним", то громадяни помічають і відчувають це. Розумне місто – це не тільки набір характеристик, це комфорт для його громадянина. Це створення можливостей для людини, таких як відстеження руху транспорту, контроль за пересуванням ліфта, розумна вбиральня (щоб користувач був упевнений, що туалет дійсно очищений і стерильний – це теж може відбуватись автоматично).

Приклади розумних міст у Україні

Я знаю, що в Україні почали будувати розумні міста, але ще немає сформованої повноцінної системи. Власне, саме тому я тут. Загалом, це складний і тривалий процес. Ваша влада показує, що взяла курс на діджиталізацію держави – це хороший знак.

Про перші кроки для впровадження розумного міста

Спочатку потрібно зрозуміти, що місцеві люди справді хочуть цієї трансформації і чи готові до змін. Це маркетинг. Спочатку громадянам треба пояснити, що це не спроба посилити за ними стеження, а намагання покращити їхнє життя у місті.

Наступний крок – перевірка зв'язку та інтернету. Адже якщо ваше місто не має хорошого покриття інтернетом, то багато функцій системи не будуть доступними.

Також я рекомендую залучати до партнерства місцеві приватні компанії, які також мають допомогти із впровадженням системи розумного міста.

І останній важливий момент – кошти. Для провадження цієї системи потрібні гроші, тому потрібно залучати інвесторів.

Про розумні міста в майбутньому

Гадаю, через 20-30 років люди матимуть більше часу для себе. Наприклад, я вже зараз працюю віддалено, тому не витрачаю час на дорогу до офісу. І я переконаний, що незабаром так працюватиме більшість людей.

Хоча нам все рівно потрібна буде хороша інфраструктура. Ми ж не будемо витрачати весь свій вільний час на перегляд телевізора. З рештою, я сумніваюся, що в майбутньому люди в принципі будуть дивитись телевізор. Телебачення стане пережитком історії.

Думаю, що через 20 років ми матимемо кардинально іншу систему освіти. Сумніваюсь, що в нас буде релігійне навчання, при цьому дітей будуть вчити основам етики. Що стосується математики, то припускаю, що її теж не вивчатимуть – для цих функцій у нас будуть комп'ютери. Те ж саме стосується фізики.

Також зміняться і багато професій. Чимало функцій, що стосується рутинної роботи, виконуватиме робот. А от щодо мистецтва та речей, для виконання яких потрібно мислення, – цим продовжуватимуть займатися люди.

Що стосується фінансів, думаю, що через 20 років реальні гроші просто зникнуть. Їх замінять цифрові. Ми будемо розраховуватись за допомогою інтернету, наших гаджетів або кредитної картки.

Також вважаю, що майбутнє за безпілотним транспортом. В Ліоні, де я живу, вже починають впроваджувати експериментальні маршрути. Ми маємо систему, як Uber, але її автівки їздять без водіїв. Думаю, через 20 років ми вже будемо користуватись літальними машинами. Кілька тижнів тому в Штутгарті (Німеччина) вже випробували перше літальне таксі.

І також зміни торкнуться мови. У майбутньому ми матимемо якусь універсальну мову. Вже зараз діти користуються набором універсальних слів, які використовують для твітів та інших повідомлень в соцмережах. Це ж стосується емодзі та смайлів.

Така моя думка. Вона суб'єктивна. Загалом, мій погляд на майбутнє дуже позитивний (усміхається).» ***(Ірина Полицька. Діджиталізація України: які переваги та загрози нам очікувати – прогноз експерта з кібербезпеки // Телеканал новин «24» (https://24tv.ua/techno/didzhitalizatsiya_ukrayini_kiberbezpeka_nebezpeka_hakeriv_n1233999). 16.11.2019).***

***

«У Держспецзв'язку вважають, що в Україні нагальним є перехід на сучасні стандарти, зокрема, на ризикорієнтовані стандарти захисту інформації, і будуть пропонувати це впроваджувати Кабінету міністрів. Про це заявив голова служби Валентин Петров…

Так, Петров провів засідання громадської ради при Адміністрації Держспецзв’язку. Під час засідання він окреслив основні завдання, проблемні чинники та місію, трансформаційні завдання вдосконалення Держспецзв’язку. Серед них – питання захисту об’єктів критичної інфраструктури, інформаційної та кібербезпеки, діяльності Концерну радіомовлення, радіозв’язку та телебачення, питання регулювання та переходу на нові стандарти галузі.

Петров повідомив представникам громадськості, що Державна служба має зосередитись насамперед на завданнях національної безпеки. "Найважливіше сьогодні – це дерегуляція. Тобто ми максимально маємо віддалитись від бізнесу. Наше завдання – захищати ті системи, де циркулюють державні секрети", - додав Петров.

Він пояснив, що сьогодні "важливим є поступовий відхід від КСЗІ (комплексна система захисту інформації), і нагальним є перехід на сучасні стандарти, зокрема, на ризикорієнтовані стандарти захисту інформації". "Ми будемо пропонувати це впроваджувати Кабінету міністрів, ми маємо в цьому повне порозуміння з Міністерством цифрового розвитку і трансформації України. Наша справа – це технічне забезпечення системи управління державою, національна безпека та системи кризового управління", - сказав голова Держспецзв'язку.

Петров підкреслив і щодо необхідності створення галузевих стандартів у сфері захисту інформації, які, зокрема, мають визначати відповідні галузеві регулятори. Також, як підкреслив Петров, оптимізація, а саме - позбавлення невластивих функцій і технічне переозброєння – сьогодні на порядку денному. Але в будь-якому разі, завдання забезпечення мобілізаційної готовності, за словами голови Держспецзв'язку, збереження керованості держави в особливий період в умовах надзвичайної ситуації не має постраждати.

Петров, відповідаючи на питання фахівців галузі щодо кібербезпеки, зазначив, що Держспецзв’язку насамперед є оператором національної захищеної мережі. "Ця мережа стане основою інформаційного обміну державних електронних інформаційних ресурсів, систем спеціального зв’язку тощо. Тобто ми маємо стати головним центром для держресурсів, надаючи необхідні послуги, в разі потреби найбільш вразливим об’єктам критичної інфраструктури", - сказав він.

Відповідаючи на питання щодо взаємодії з Генштабом та управлінням телекомунікаційною галуззю в особливий період, Петров зазначив, що управління телекомунікаціями і формування політики – це прерогатива Кабміну, але технічна інфраструктура для цього вже побудована і скоро буде введена в експлуатацію. "Це є наше питання і воно якраз належить до питань національної безпеки і оборони України, і ми як суб’єкт сектору безпеки і оборони відповідальні за це", - підкреслив голова Держспецзв’язку.

Він окреслив також і проблемні питання розвитку галузі. "Так, сьогодні є негативне ставлення в суспільстві до нашого відомства... Так, є обґрунтована критика, насамперед, щодо зарегульованості галузі, є обґрунтована критика з боку бізнесу та інших державних органів. Дуже часто це виникає через недокомунікування. Зокрема, через недостатню просвітницьку роботу про діяльність нашого відомства. І ми будемо змінювати це, зокрема, більше спілкуватися з громадськістю", - підкреслив Петров.

Крім того, керівник Держспецзв’язку пояснив, що сьогоднішні трансформаційні зусилля також пов’язані і з питанням фінансування галузі, зокрема, в зв’язку з ухваленим нещодавно бюджетом на 2020 рік, в якому фінансування Держспецзв’язку було скорочено за рахунок додаткового фінансування Міноборони. За його словами, Держспецзв’язку це збільшення бюджету мало спрямувати на підвищення зарплати працівникам, що дало би змогу

вирівняти зарплати між ЗСУ і Держспецзв'язку…» ***(Юлія Шрамко. У Держспецзв'язку виступили за перехід на нові стандарти захисту інформації // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1835081-u-derzhspetszvyazku-vistupili-za-perekhid-na-novi-standarti-zakhistu-informatsiyi). 11.11.2019).***

***

«В Одессе эксперты на заседании круглого стола обсудили актуальные проблемы кибербезопасности.

Ректор ОНАС им. Попова Петр Воробиенко отметил, что с помощью кибератак можно вывести из строя различное оборудование и заполучить любую информацию, в том числе и персональные данные, которыми могут воспользоваться в корыстных целях…

По словам специалистов, популярные сегодня смарт-устройства напрочь лишены защиты, поэтому они часто подвергаются кибератакам.

«Эти предметы имеют подключение к интернету, а вот какая-либо защита отсутствует напрочь. Согласно прогнозам, в 2020 году 25% кибератак придется именно на такие устройства. Это связано с тем, что интернет вещей развивается огромными темпами и злоумышленники видят в этом потенциальный инструмент для выполнения своих целей», – подчеркнула ассистент кафедры информационных технологий и кибербезопасности ОНАПТ Екатерина Смирнова.

В то же время открыт свободный доступ к системам, где обрабатываются персональные данные, что облегчает работу кибермошенникам…

Специалисты считают, что необходимо разрабатывать комплексную систему защиты информации…

Заместитель начальника службы информационных технологий ГП «Одесский порт» Андрей Тындюк добавил, что в рамках законодательства выполнить требования по защите информации достаточно сложно…

По данным международных рейтингов, которые оценивают уровень кибербезопасности, Украина находится в середине списка.

«У нас в плане киберзащиты не все так плохо, но, тем не менее, есть над чем работать. К тому же одесские вузы выпускают хороших специалистов, которые разбираются в этой отрасли. Поэтому процесс запущен», – сказал директор учебно-научного института радио, телевидения и информационной безопасности Евгений Василиу.» ***(Observan. Одесситам рассказали, как не стать жертвой кибермошенников // Одесский Наблюдатель (http://nabludatel.od.ua/society/odessitam-rasskazali-kak-ne-stat-jertvoi-kibermoshennikov/). 15.11.2019).***

***

«В Харьковском национальном университете радиоэлектроники открылась современная научно-учебная лаборатория сетевой безопасности и надёжности.

Новое программное обеспечение позволит студентам получить навыки защиты информации в сети на практике.

Диджитал-оператор lifecell оборудовал лабораторию сетевой безопасности на базе факультета инфокоммуникаций серверами и предоставил необходимое программное обеспечение, операционную систему среды виртуализации, программное обеспечение виртуализации и виртуальные машины для изучения уязвимостей. Эксперты lifecell также разработали методические указания для выполнения тематических лабораторных работ с использованием лабораторного комплекса…

После открытия лаборатории состоялась встреча со студентами.

Начальник департамента информационной безопасности lifecell Анатолий Покоса провёл лекцию о безопасности данных и устроил онлайн конкурс с призами через портал Kahoot…» ***(Новая лаборатория в ХНУРЭ. Кибербезопасность для студентов на практике // Стрічка новин Харкова (http://uanews.kharkiv.ua/society/2019/11/08/278418.html). 08.11.2019).***

***

«Группа компаний «Бакотек» сообщает об успешном завершении сертификации «Государственной службой специальной связи и защиты информации Украины» (Госспецсвязь) линейки решений Palo Alto Networks.

Результаты экспертизы подтверждают, что системы сетевой безопасности от Palo Alto Networks отвечают нормативным документам, регламентирующим требования к средствам технической защиты информации, установленные законодательством Украины.

Перечень сертифицированных Госспецсвязью решений:

Межсетевые экраны PA-220, PA-820, PA-850, PA-3020, PA-3050, PA-3060, PA-3220, PA-3250, PA-3260, PA-5220, PA-5250, PA-5260, PA-5280, PA-7050, PA-7080

Программное обеспечение на виртуальные машины VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, VM-1000HV

Система защиты конечных точек от вредоносного ПО Traps Advanced Endpoint Protection.

Полученные сертификаты подтверждают возможность использования решений Palo Alto Networks в учреждениях, где необходимы сертифицированные программные продукты (в государственных, финансовых, международных и других организациях).» ***(Госспецсвязи сертифицировала решения кибербезопасности от Palo Alto Networks // Компьютерное Обозрение (https://ko.com.ua/gocspecsvyazi_sertificirovala_resheniya_kiberbezopasnosti_ot_palo_alto_networks_130829). 11.11.2019).***

***

«Столична влада заявляє про стандарт захисту ІТ-інфраструктури Києва

Київ посилив свій інформаційних захист.

Про це повідомив директор Департаменту інформаційно-комунікаційних технологій Київської міської держадміністрації Юрій Назаров на своїй сторінці у Facebook.

Він поінформував, що Спеціалізоване комунальне підприємство «Київтелесервіс» отримало атестат відповідності Комплексної системи захисту інформації.

«Звучить складно і загрозливо. І це насправді так для кіберзлочинців та потенційних атак на міську мережеву сервісну інфраструктуру. Атестат підтверджує високий стандарт захисту ІТ-інфраструктури Києва. Це означає, що 1200 кілометрів мережі захищені від посягань будь-якої складності. А це безперебійна робота міських підприємств та служб, а значить - і якісні сервіси для киян», - зазначив Назаров.

Він підкреслив, що «безпека - це не тільки правоохоронці, смарт-рішення в сфері захисту на кшталт камер відеоспостереження чи кнопок виклику допомоги, в сучасному світі це ще й кібербезпека»…» ***(Київ посилив свій захист від хакерів // Українські медійні системи (https://glavcom.ua/kyiv/news/kijiv-posiliv-sviy-zahist-vid-hakeriv-642704.html). 27.11.2019).***

***

«Петро Порошенко двічі зустрічався з адвокатом Дональда Трампа Руді Джуліані. Той обіцяв п'ятому президентові України, що допоможе підняти рівень співпраці між США та Україною.

Порошенко сказав, що Джуліані не порушував питання "Бурісми" чи Байденів. Про це він розповів на Форумі з міжнародної безпеки у Канаді…

"Пан Джуліані обіцяв мені допомогти підняти рівень нашої (США та України) співпраці у кібербезпеці", – сказав Порошенко.

На запитання, чи просив щось Джуліані за такі послуги, Порошенко спочатку відповів ухильно.

Дивіться, я – президент України, величної європейської нації, великої європейської країни, найбільшої за територією в Європі. І, звичайно, я не можу уявити такого типу розмов зі мною як із президентом України, – згодом відповів президент…» ***(Порошенко розповів, що йому обіцяв Джуліані на зустрічі // Телеканал новин «24» (https://24tv.ua/poroshenko_rozpoviv_shho_yomu_obitsyav_dzhuliani_na_zustrichi_n1238880). 25.11.2019).***

***

«Семінар «Цифрова безпека «розумного міста» відбувся… 20 листопада, для працівників Харківської міської ради.

Як повідомив заступник керуючого справами виконавчого комітету Харківської міської ради Сергій Захаревич, останнім часом у Харкові активно впроваджуються інноваційні технології, і разом із цифровізацією усіх сфер життєдіяльності міста з'являються певні загрози.

«За останні роки в місті впроваджено багато цифрових технологій і програм для активної інтеграції Харкова у глобальний інформаційний простір. Однак, разом із перевагами сучасного кіберпростору, впровадження концепції «розумного міста» супроводжується кіберзагрозами щодо функціонування міських інформаційних ресурсів. Саме з метою їх запобігання, а також для підвищення компетентності з

цього питання співробітників міськради ми проводимо цей семінар», - зазначив Сергій Захаревич.

Під час заходу професор кафедри інформаційних технологій та кібербезпеки Національного університету внутрішніх справ Віталій Носов зазначив, що за останні роки кількість шкідливих програм у кіберпросторі збільшилася у 70 разів. Тому спочатку на етапі проектування «розумного міста» необхідно створити систему його захисту.

«Це не просто окремі заходи, а постійні процеси. Наприклад, у Євросоюзі правоохоронні органи створили систему, або протокол, реагування на кібератаки. Вона є багатостороннім процесом і складається з семи стадій: раннє виявлення, класифікація загрози, термінова координація реагування, повідомлення та раннє попередження, дії правоохоронних органів, розслідування та закриття цього протоколу реагування на надзвичайну подію», - зазначив Віталій Носов.

Він додав, що створювати систему захисту «розумного міста» можна кількома шляхами - або законодавчо, і в цьому випадку Кабінет міністрів своїми підзаконними актами регулюватиме цю роботу, або ж за стандартами, рекомендаціями і міжнародними процедурами. Віталій Носов підкреслив, що це питання треба вирішити в першу чергу.

Також, за словами професора, необхідно створити окремий орган, який контролюватиме цю роботу - службу або підрозділ інформаційної безпеки «розумного міста».» ***(У міськраді розповіли про кібербезпеку «розумного міста» // Харьковские Известия (http://izvestia.kharkov.ua/on-line/gorod/1297288.html). 21.11.2019).***

***

"…Три тижні поспіль Джокер у своєму Телеграм-каналі публікує листування, які він веде від імені одних високопосадовців з іншими.

Три тижні нардепи і урядовці продовжують наступати на ті самі граблі та "вестися" на пранки, з легкістю розповідаючи речі, якими б навряд чи стали хвалитися публічно. Дехто з "жертв", наприклад, Михайло Радуцький, підтверджують спілкування з Джокером. Інші – відмовчуються.

…Як захиститись від Джокера

1. Захист від папараці – антишпигунська плівка

Є декілька варіантів отримання доступу до вашої переписки. Примітивний варіант – це коли ви щось пишите, а вам дивляться в екран телефону, не обов'язково фотографують, а підглядають.

Для захисту від цього можна скористатися захисними плівками: коли ви дивитесь прямо на екран, ви бачите інформацію. Але під іншими кутами – збоку, знизу, згори – ви не бачите, що на екрані.

2. Захист сім-картки – паспорт

Краще, щоб сім-картка була або контрактного підключення, або прив'язана до паспорту.

Так ніхто з вулиці не зможе прийти і відновити цю картку і отримати доступ до неї. Але навіть так будь-хто не зможе переписуватись від вашого імені, лише отримає доступ до вашої переписки.

Переписка зберігається у цифрових хмарах (віртуальне місце для зберігання інформації), особливо, у тому ж Telegram. І якщо підключити на будь-якому пристрої аккаунт Telegram з тим самим номером, ви отримаєте доступ до всіх переписок, які були до цього.

У WhatsApp, Viber із цим трохи краще: отримати переписку можна тільки на авторизованому пристрої.

Саме через це сім-картка має бути обов'язково прив'язана до паспорту, так буде набагато складніше її відновити.

3. Захист листування – паролі

Рекомендується ставити на сам месенджер додаткову двофакторну аутентифікацію (двоетапне підтвердження особистості).

Тоді, щоб зайти з нового гаджету, потрібно вводити додатковий пароль, який знаєте тільки ви. Навіть якщо хтось перехопив смс-підтвердження, відновив сім-картку і її включать на новому пристрої, телефон запитує додаткову аутентифікацію. І тільки після цього на ньому почне працювати месенджер.

Як може працювати Джокер

Спосіб перший. Хакерський. Складний

Можна отримати сім-карту з потрібним номером телефону. Прийти в сервісний центр, сказати: "Я втратив свою картку, хочу її відновити".

Вам скажуть – назвіть останні 3 набрані номери, дату поповнення. Це можна легко зорганізувати: купити 3 сім-картки, зателефонувати і одразу покласти слухавку. Людина, скоріш за все, перетелефонує. Таким чином ви можете отримати три останні набрані номери. Також при бажанні можна поповнити рахунок людини і отримати останню дату поповнення рахунку.

У сервісному центрі ви називаєте 3 номери, дату поповнення, і вам відновлюють картку, якщо вона не контрактна, а анонімна, тобто передплаченого сервісу.

Але якщо ви вставили цю картку в новий телефон, або хочете використовувати WhatsApp на комп'ютері, то на телефоні, де вперше була встановлена програма, здійсниться вихід з акаунту. Або програма покаже, що хтось використовує її на іншому гаджеті.

Якщо клонувати сім-картку і переприв'язати до неї WhatsApp, то людина одразу це побачить. Тому що WhatsApp не можна використовувати паралельно на двох телефонах, він відключається на одному із них.

У минулому на WhatsApp була діра безпеки. Можна було відправити спеціальне відео і отримати доступ до переписки. Але це доступ до переписки, але не доступ до акаунту.

Можна перехопити смс-повідомлення, яке підтверджує підключення Telegram до окремого номеру, перехопити, встановити собі на пристрій і користуватися.

Telegram можна використовувати на невеликій кількості пристроїв паралельно.

Але тут подібна ситуація з отриманням оповіщень. Дуже-дуже важко зробити так, щоб людина не побачила, що відправляються та надходять повідомлення.

Спосіб другий. Нехакерський. Легкий

Неможливо використовувати відновлену сім-карту так, щоб цього не помітив хазяїн першої картки. І давайте уявимо, що, наприклад, хтось отримав віддалений доступ до телефону, і з нього відправляв повідомлення. Людина, чий телефон зламали, ці повідомлення побачила би.

Тому ці переписки – або фотошоп, або все було набагато примітивніше.

У WhatsApp або іншому месенджері можна написати ім'я користувача. І людина підписувала себе, наприклад, прізвищем генерального прокурора.

Але в цьому випадку це був не злам, а соціальна інженерія, обман людей. І ця людина, з якою спілкувалися, бачила, що це ім'я не з телефонної книжки, а просто ім'я користувача.

Якщо брати за основу переписку Джокера з політиками, то схоже на те, що він просто писав ім'я користувача, а неуважні люди на це куплялися.

УП теж спробувала нехакерський спосіб на собі, змінивши ім'я користувача у популярних месенджерах WhatsApp (ліворуч) і Telergam (праворуч). Цей спосіб працює, якщо номер пранкера не записаний у контактах жертви…

Що робити жертві хакерів?

Необхідно звернутися до кіберполіції, писати заяву. Це їхня зона відповідальності.

Вони мають всі необхідні доступи і можливості, для того, щоб викрити, як це було, і допомогти з'ясувати, це був злам чи шахрайство.

Приватні компанії до цих інструментів доступу не мають. Приватні компанії не можуть звернутися до WhatsApp, Facebook або Telegram і запросити інформацію про те, звідки і коли заходили в акаунт.

Ці компанії зберігають інформацію і співпрацюють з нашими правоохоронними органами. Вони будуть надавати факти за запитом і судовим ордером.

Якщо відбувся злочин, то кіберполіція має можливість його розслідувати і надати інформацію, чи це дійсно злам, і ким він був потенційно здійснений.

Тут потрібно розуміти, чи людина постраждала через неуважність або була введена в оману. Якщо був злам, відновили сім-картку або зламали телефон, це вже інша стаття. І вона більш сувора.

Чи знаходять таких "джокерів"? Така практика є, просто вона не афішується.

Що робити жертвам пранку? Порада юристки

Прокуратура може відкривати провадження через факти, які стали відомі зі ЗМІ. Але пранкер Джокер не є медіа чи офіційним джерелом інформації.

Зараз у спілкуванні поширений тролінг, технічні можливості дозволяють підробляти фото і відео. Правоохоронці не зобов'язані сприймати інформацію з пранків за правду і перевіряти її.

Але люди, які вважають, що оприлюднена інформація може зашкодити їхнім або взагалі державним інтересам, мають підстави звернутись до правоохоронних органів, щоб вони перевірили правдивість фактів.

Особи, які стали жертвами розіграшу, можуть звернутися до суду, щоб відновити репутацію та відшкодувати моральну шкоду, бо іноді ці пранки схожі на психологічне насильство.

У цивільному праві діють такі інструменти: вибачитися перед потерпілим, спростувати інформацію, призначити грошове відшкодування за моральну шкоду. Але зазвичай гроші виплачуються, тільки якщо було завдано шкоду здоров'ю або стались якісь непоправні наслідки.

Питання у тому, щоб фізично знайти людину чи групу людей, які є Джокером. Позиватися треба до когось.

Саркастична, але найдієвіша порада, як не стати жертвою пранку:

Чесно виконуйте свою роботу, не беріть участі у сірих схемах, не підставляйте колег, не пліткуйте і не претендуйте на чужі місця. Тоді ваша переписка просто нікого не зацікавить. ***(Соня Лукашова, Катерина Рещук. Захиститись від Джокерів. Як пранкери зливають листування // Українська правда (https://www.pravda.com.ua/articles/2019/11/20/7232553/). 20.11.2019).***

***

Національна система кібербезпеки

«Міністерство цифрової трансформації має намір запустити Офіс реформ у сфері кібербезпеки

За словами першого заступника міністра цифрової трансформації Олексія Вискуба, зараз йде робота над створенням відомства… Вискуб нагадав, що в положенні про Мінцифру є пункт про те, що відомство бере участь у формуванні політики сфери кібербезпеки.

«Цей пункт поки в положенні тимчасового, адже, згідно із законодавством, ця функція закріплена за Держспецзв'язком та до зміни закону ми можемо тільки брати участь у формуванні політики в сфері кібербезпеки. Але в цілому ми готуємося до досить масштабної реформу в цій сфері», — розповів чиновник. За його словами, міністерство звернулося до USAID (агентство США з міжнародного розвитку) з проханням про створення при міністерстві Офісу реформ в сфері кібербезпеки.

«У досить короткий термін Офіс повинен напрацювати дорожню карту реформи. У нашому зверненні в USAID були викладені конкретні запити і завдання, які повинні бути досягнуті в короткостроковій і довгостроковій перспективах. У короткостроковій перспективі — це питання проведення функціонального аудиту», — сказав Вискуб.

Ці завдання Офіс повинен вирішити за три місяці. Як зазначив Вискуб, з лютого 2020 року готуватися пакет допомоги Україні від USAID, який повинен допомогти в реалізації цієї реформи…» ***(В Україні відкриють Офіс реформ у сфері кібербезпеки // UA.NEWS (https://ua.news/ua/v-ukrayne-otkroyut-ofys-reform-v-sfere-kyberbezopasnosty/). 26.11.2019).***

***

«План мероприятий на 2019 год по реализации Стратегии кибербезопасности Украины до сих пор не утвержден Кабинетом Министров Украины и, вероятнее всего, в виде отдельного документа больше не появится. Взамен в Госспецсвязи решили «убить двух зайцев сразу» и подготовили проект постановления КМУ об утверждении такого плана сразу на 2 года – на этот и на следующий…

На заседании сегодня, 19 ноября, Национальная комиссия, осуществляющая государственное регулирование в сфере связи и информатизации, согласовала без замечаний проект постановления КМУ «Об утверждении плана мероприятий на 2019-2020 годы по реализации Стратегии кибербезопасности Украины».

Стратегия кибербезопасности Украины была утверждена Советом национальной безопасности и обороны 27 января 2016-го года и введена в действие Указом Президента от 15 марта того же года. Целью Стратегии кибербезопасности Украины является создание условий для безопасного функционирования киберпространства, его использования в интересах личности, общества и государства.

Ежегодно Кабмин своим распоряжением утверждает план мероприятий на год по реализации Стратегии. В 2017-м году соответствующий план мероприятий на текущий год был утвержден 10 марта, в прошлом году план мероприятий на 2018 год по реализации Стратегии кибербезопасности Украины был утвержден 11 июля. Предложения в план мероприятий по реализации Стратегии на 2019-ый год принимались, согласно распоряжению Кабмина, до первого сентября 2018-го. Однако соответствующего распоряжения Кабмина так и не появилось: месяц назад, 22 октября, НКРСИ без замечаний согласовала проект распоряжения Кабинета Министров Украины «Об утверждении плана мероприятий на 2019 по реализации Стратегии кибербезопасности Украины», направленный письмом Государственной службы специальной связи и защиты информации Украины. Однако, похоже, в ГСССЗИ осознали, что утверждать план мероприятий на 2019-ый за полтора месяца до нового 2020-го года глупо, и разработали новый документ – план сразу на два года, который сегодня и был согласован Нацкомиссией. Когда документ попадет на рассмотрение Кабмина – пока неизвестно.» ***(Владимир Кондрашов. В Госспецсвязи придумали "отмазку" от стратегии кибербезопасности на уходящий год // Internetua (https://internetua.com/v-gosspecsvyazi-pridumali-otmazku-ot-strategii-kiberbezopasnosti-na-uhodyasxii-god). 19.11.2019).***

***

Кібервійна проти України

«Псевдомінування в Україні останнім часом стали мало не звичним явищем. Уже навіть немало людей не хвилюються, почувши повідомлення про замінування того чи іншого об’єкта. А таких повідомлень стає все більше: «мінують» торгові центри і офіси, вокзали і аеропорти, державні установи і навіть

лікарні. «За останній тиждень подібні повідомлення по кілька разів отримували в Києві, Львові, Харкові та інших містах», повідомляє ресурс belsat, зауважуючи, що 15 тисяч – таку рекордну кількість неправдивих повідомлень про замінування перевірили українські правоохоронці за місяць.

І хоч це зазвичай «фейкові» повідомлення, але рятувальники, правоохоронці, інші відповідні служби перевіряють кожен виклик з передбаченою інструкцією ретельністю. Адже тут розслаблятись не можна: де гарантія, що чергове повідомлення – не сигнал про справжній теракт?

«Масові псевдомінування відбуваються в Україні майже щодня, а виїзд спецслужб на кожен такий виклик обходиться бюджету близько 2 тисяч доларів в еквіваленті…»…

Поліція уточнює, що такі сигнали все частіше надприходять не від фізичних осіб, а від спеціальних програм і ботів. Це стало частиною гібридної війни. За словами– директора департаменту інформації МВС України Артема Шевченка, це е-мейли, це і роботизовані програми, автодозвон, айпі-телефонія та інші-інші сучасні засоби комунікації. «Слід цих повідомлень тягнеться або за кордон, або на території, тимчасово не контрольовані урядом України, це окуповані території Донецької області і окуповані території автономної республіки Крим. Також тягнеться з території сусіда – Росії».

Психологи зауважують, що такий кібертероризм спрямований на породження страху і панічних настроїв в суспільстві, підрив довіри до влади і формування відчуття нестабільності…» ***(Косянчук Інна. Мінування України як елемент «гібридної війни»: все більше сигналів надходить від ботів // ІА «Погляд» (https://www.poglyad.tv/minuvannya-ukrayiny-yak-element-gibrydnoyi-vijny-vse-bilshe-sygnaliv-nadhodyt-vid-botiv/). 14.11.2019).***

***

«Сенатор-республіканець Джон Кеннеді заявив, що був неправий, що казав, що не знає, хто насправді - Україна чи Росія - стоїть за кібератакою 2016 року на сервер Демократичної партії…

Кеннеді заявив, що "неправильно зрозумів" запитання ведучого Fox News Кріса Уоллеса, і визнав, що докази вказують на втручання з боку Москви.

"Кріс правий. Я був неправий. Єдиний доказ, який я маю, і, гадаю, він переважає, це те, що Росія намагалась зламати комп'ютер Національного комітету Демократичної партії. Я не бачив свідчень того, що це прагнула зробити Україна", - сказав сенатор.

Минулого тижня колишня чиновниця Білого дому Фіона Гілл на слуханнях в Конгресі в рамках розслідування імпічменту президента Дональда Трампа заявила, що подібні заяви щодо України "створюють і поширюють" російські спецслужби.

Президент США Дональд Трамп висловився на користь дискредитованої теорії змови, відомої як "Crowdstrike", яка звинувачує Україну, а не Росію у втручанні у президентські вибори в США в 2016 році.» ***("Я був неправий": сенатор США визнав, що Україна не втручалася в американські вибори // Європейська правда (https://www.eurointegration.com.ua/news/2019/11/27/7103539/0. 27.11.2019).***

***

«Украина постоянно становится целью информационных и кибернетических атак, заявил министр обороны Андрей Загороднюк в канадском Галифаксе на международном форуме, посвященном безопасности…

“Загороднюк отметил, что на сегодня Украина является страной, которая не только противостоит вооруженной агрессии, а фактически стала „полем битвы“ и постоянно отражает атаки – как в информационном, так и в кибернетическом пространстве», – говорится в сообщении.

Министр отметил, что украинцы «уже научились отражать такие атаки, но пространство постоянно развивается», побуждая действовать гораздо активнее.

«Сегодня многие страны инвестируют в развитие кибернетического направления, но, к сожалению, мы никогда не будем действовать быстрее тех, кто целенаправленно разрабатывает новые формы ведения информационных и кибернетических войн. Поэтому единственным возможным фактором сопротивления являются общие усилия стран, а также людей, которые в них проживают, противостоять таким вызовам», – подчеркнул Загороднюк.

Он считает, что «это должно преподаваться в школах, чтобы с детства обучать население, как отличать правду от лжи, как проверять информацию и соблюдать «цифровую гигиену»…» ***(Украина постоянно отражает атаки в информационном и киберпространстве – Загороднюк // Одесский Наблюдатель (http://nabludatel.od.ua/odessa/ykraina-postoianno-otrajaet-ataki-v-informacionnom-i-kiberprostranstve-zagorodnuk/). 25.11.2019).***

***

Боротьба з кіберзлочинністю в Україні

«…Використовуючи вірус, 20-річний житель Дніпропетровщини отримував доступ до користувацьких даних та комп’ютерної інформації. Фігурант викрадав конфіденційну інформацію користувачів. Крім цього, збував за грошову винагороду шкідливі програмні засоби…

Працівники кіберполіції Дніпропетровщини встановили, що зловмисник збував за грошову винагороду шкідливий програмний засіб та за допомогою якого викрадав дані для доступу до облікових записів користувачів мережі Інтернет.

…Під час попереднього огляду… працівники кіберполіції виявили шкідливе програмне забезпечення та скомпрометовану конфіденційну інформацію понад 100 облікових записів користувачів з України та понад 3500 громадян інших країн. Така інформація містила дані щодо електронних платіжних систем, паролів від електронних поштових скриньок, ключів від електронних гаманців криптовалют.

Досудове розслідування триває, зловмисник підозрюється у скоєнні кримінального правопорушення за ч. 1 ст. 361-1 (створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) Кримінального кодексу України. Фігурантові загрожує до двох років позбавлення волі…» ***(Кіберполіція викрила зловмисника у***

поширенні шкідливого програмного забезпечення // Лица (http://www.litsa.com.ua/show/a/47929). 15.11.2019).

***

«По ходатайству прокуратуры города Киева постановлением следственного судьи Шевченковского районного суда города Киева от 11.11.2019 применен экстрадиционный арест сроком на 2 месяца до гражданина Литовской Республики, находившийся в международном розыске и был задержан в Киеве.

Об этом сообщает пресс-служба прокуратуры города Киева.

В сообщении говорится, что расследование преступной деятельности 32-летнего иностранца началось еще в 2010 году сотрудниками Федерального бюро расследования и Службы расследования финансовых преступлений США.

Мужчина был объявлен в розыск для привлечения к уголовной ответственности за совершение ряда уголовных преступлений в сфере незаконного доступа к банковским счетам. Среди прочего его подозревают в похищении 6 000 000 долларов США со счетов американских финансовых учреждений, завладении персональными данными и легализации доходов, полученных преступным путем.

Задержание иностранца произошло в одном из столичных отелей, где он временно проживал.

Осознавая невозможность избежать экстрадиции в Соединенные Штаты Америки, иностранец дал согласие на упрощенный порядок его выдачи. В настоящее время прокуратурой города Киева начато в отношении него экстрадиционную проверку…» ***(В Киеве на 2 месяца арестовали киберпреступника, который скрывался от ФБР // ГолосUA (https://golos.ua/i/716706). 12.11.2019).***

***

«Як повідомляє кіберполіція, підозрюваний нібито розсилав користувачам спам із вірусом, який викрадав логіни, паролі, дані банківських карт, електронних гаманців та іншу інформацію…

Зазначається, що у викраденні інформації підозрюють 33-річного мешканця Чернігівської області. Раніше він проходив службу у Збройних сил України на посаді інженера комп’ютерних мереж. Звільнившись з лав ЗСУ, чоловік начебто почав заробляти продажем баз даних.

За інформацією кіберполіції, підозрюваний продавав викрадену інформацію на спеціалізованих закритих форумах. Під час обшуку у нього на комп'ютері виявили більше 20 Гб текстових документів із конфіденційними даними. Поліцейські вилучили обладнання та направили на експертизу.

Наразі розпочато кримінальне провадження за ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) та ст. 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в комп'ютерах, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) КК України.

Чоловіку загрожує до двох років ув'язнення…» ***(Кіберполіція викрила хакера, який отримав конфіденційну інформацію 1 млн осіб // MediaSapiens (https://ms.detector.media/web/cybersecurity/na_chernigivschini_kiberpolitsiya_zatrimala_khakera_yakiy_vikrav_konfidentsiynu_informatsiyu_1_mln_osib/). 11.11.2019).***

***

«Залещицкий районный суд Тернопольской области (Украина) приговорил к штрафу в размере 8,5 тыс. грн. (примерно 22 тыс. рублей) кладовщика магазина, продавшего учетные данные 386 для входа в аккаунты online-сервиса цифрового распространения компьютерных игр Steam. Злоумышленнику предъявлены обвинения по ст. 361-2 ч.1 УК Украины (несанкционированный сбыт информации с ограниченным доступом, хранящейся в автоматизированных системах, компьютерных сетях, созданной и защищенной в соответствии с действующим законодательством).

Как сообщается в приговоре, в период с 29 марта 2018 года по 10 июня того же года обвиняемый продал неизвестным лицам логины и пароли 386 учетных записей в Steam, заработав на этом 53 944 рубля, которые поступали на электронный кошелек QIWI.

В августе нынешнего года обвиняемый заключил сделку со следствием и признал свою вину. Он также обязался добровольно возместить затраты на услуги экспертов в сумме 5024 грн. (примерно 13 тыс. рублей).

Следствию не удалось найти пострадавших или узнать, каким образом в распоряжении обвиняемого оказались учетные данные.» ***(Украинца оштрафовали за продажу учетных данных 386 аккаунтов в Steam // SecurityLab.ru (https://www.securitylab.ru/news/502395.php). 08.11.2019).***

***

«В конце сентября неизвестные злоумышленники получили доступ к серверу главного бухгалтера ювелирной сети «Рубин», в результате чего все файлы были закодированы, а за раскодирование хакеры требовали 1,3 биткоина. Полицейские больше месяца «футболили» заявление пострадавших…

Как стало известно, 26 сентября представитель ООО «Ювелирная сеть «Рубин» обратился с письменным заявлением в Криворожский отдел полиции ГУНП в Днепропетровской области с заявлением о совершении уголовного преступления. Адвокат заявил о несанкционированном вмешательстве в работу электронно-вычислительных машин, автоматизированных систем, компьютерных сетей, а именно в сервер главного бухгалтера компании, после чего все файлы были закодированы, а за раскодирование предлагалось перечислить 1,3 биткоина на соответствующий биткоин-кошелек. Не смотря на то, что полицейские получили заявление в тот же день, никакой реакции от правоохранителей не было.

Спустя две недели адвокат обратился в Криворожский ОП ГУНП в Днепропетровской области с целью получения информации о судьбе поданного заявления. Там ему сообщили, что его заявление передали в Приднепровское управление киберполиции. 16 октября сотрудники Приднепровского управления киберполиции сообщили адвокату, что у них в штате нет следователей, а поэтому

они не имеют возможности вносить сведения в Единый государственный реестр досудебных расследований и отправили его заявление назад в Криворожский отдел полиции. 18 октября представитель ювелирной компании направил адвокатский запрос, в котором просил сообщить, были ли внесены сведения по его заявлению в ЕГРДР. Однако ответа он так и не получил.

29 октября Следственный судья Центрально-Городского районного суда города Кривого Рога Днепропетровской области рассмотрел в открытом судебном заседании жалобу адвоката на невнесение сведений об уголовном правонарушении в Единый реестр досудебных расследований и обязал Криворожский отдел полиции внести соответствующие сведения в реестр, начать расследование и через 24 часа с момента внесения таких сведений предоставить заявителю выписку из Единого реестра досудебных расследований.

К слову, в письменных возражениях Криворожского отдела полиции, предоставленных суду, было сказано, что указанное заявление адвоката было зарегистрировано в ЖЕО за №21542, рассмотрено руководством следственного отдела КОП и, в связи с отсутствием в соответствии со ст. 11 УК Украины обязательных признаков субъективной и объективной стороны уголовного преступления, данное заявление не подлежало согласно ст..214 КПК Украины внесению в ЕРДР. Суд такие аргументы полиции не устроили.» ***(Владимир Кондрашов. Хакеры закодировали данные на сервере сети «Рубин» и потребовали выкуп // Internetua (https://internetua.com/hakery-zakodirovali-dannye-na-servere-seti-rubin-i-potrebovali-vykup). 06.11.2019).***

***

«К двум годам лишения свободы условно с испытательным сроком в один год приговорен одинокий отец, который с помощью нехитрых комбинаций получил доступ к чужим социальным сетям и мессенджерам…

Согласно приговору Рубежанского городского суда Луганской области, слесарь одного из предприятий в декабре 2018-го года приобрел стартовый пакет Vodafone и, позвонив на горячую линию оператора заявил, что потерял сим-карту с абонентским номером, которым пользовалась потерпевшая. Мужчине удалось убедить оператора и он переоформил сим-карту жертвы на свой новый стартовый пакет. После этого он, используя чужую сим-карту, зашел в мобильное приложение «My Vodafone» и в аккаунте потерпевшей в качестве дополнительного номера отметил свой мобильный абонентский номер, в результате чего информация, которая должна была поступать на мобильный телефон потерпевшей, стала доступной в случае использования абонентского номера обвиняемым.

– Таким образом, был нарушен установленный порядок маршрутизации информации из сетей электросвязи, – говорится в приговоре.

Получив полный контроль над номером телефона жертвы, мужчина осуществил вход в почтовый сервиса «gmail. com », а также в учетные записи потерпевшей в соцсети «Instagram », сервисах «Viber » и «WhatsApp», путем восстановления и изменения паролей.

– Таким образом, обвиняемый совершил уголовное преступление, предусмотренное ч.1 ст. 361 УК Украины, то есть несанкционированное вмешательство в работу компьютерных сетей и сетей электросвязи, что привело к

утечке, блокированию информации и нарушение установленного порядка ее маршрутизации, – говорится в приговоре.

11 апреля между на тот момент подозреваемым и потерпевшей было заключено соглашение о примирении, согласно которому подозреваемый в полном объеме признал свою виновность в совершении уголовного преступления, предусмотренного ч.1 ст. 361 УК Украины, а стороны соглашаются на назначение ему наказания в виде лишения свободы сроком на 2 года, с освобождением от отбывания наказания с испытательным сроком в один год.

Только в конце октября суд соглашение утвердил. Кроме заранее оговоренного наказания, украинца также суд обязал оплатить 4004 гривны затрат на привлечение экспертов.» ***(Владимир Кондрашов. Украинцу дали два года за несанкционированный доступ к чужим аккаунтам в соцсетях // Internetua (https://internetua.com/ukraincu-dali-dva-goda-za-nesankcionirovannyi-dostup-k-csujim-akkauntam-v-socsetyah). 01.11.2019).***

***

«Киберпреступники нашли новый метод добраться к деньгам украинцев. Теперь целью мошенников - мобильные телефоны украинцев, через которые они входят в личный кабинет банковских счетов. Киберполиция предупреждает о новой волне вирусов, которые блокируют телефоны. Тем временем мошенники получают доступ к вашим данным…

На данный момент, на крючок мошенников попали школьники. Вирус замаскирован под рекламу или раздачу бесплатных "бонусов". При переходе по ссылке телефон блокируется. Выведя из строя гаджет, - нужно всего лишь кликнуть на ссылку, которая пришла в мессенджере, аферисты получают доступ к деньгам на телефоне.

Если даже ваш телефон не привязан к финансовым данным, то ремонт процессора может вылиться в кругленькую сумму около 2-х тысяч гривен.

Эксперт техбезопасности рассказал, что вирус сначала похищает данные кредиток. Чтобы пострадавший не смог отключить платежные карты от телефона выводит из строя сам телефон…

Если телефон заблокирован, то ждите сообщение, с предложением заплатить за разблокировку.

Александр Карпов, специалис по кибербезопасности уверен, что на такой шантаж идти не стоит. А вот обратиться на сайт Европола можно:

"Если приложение заблокировало ваш смартфон, и у вас начинают вымогать деньги за разблокировку, не тратьте деньги. Переводите устройство в заводские настройки или идите на сайт европола"…» ***(На "халяву" вестись не стоит: как не пустить "троянского коня" в свой смартфон – касается каждого // Ukrainianwall.com (https://ukrainianwall.com/society/18762-na-halyavu-vestis-ne-stoit-kak-ne-pustit-troyanskogo-konya-v-svoy-smartfon-kasaetsya-kazhdogo). 23.11.2019).***

***

«Секретар Ради національної безпеки і оборони України Олексій Данілов провів зустріч із заступником міністра оборони, Державним секретарем Міністерства оборони Королівства Норвегія пані Туне Скуген. Під час зустрічі сторони обговорили двостороннє співробітництво, а також поточну безпекову ситуацію…

Данілов вважає важливим питання безпеки у кіберсфері, тож висловив сподівання на співпрацю у цій сфері з Норвегією…

У свою чергу, Скуген наголосила на необхідності розвивати системну міжнародну співпрацю у сфері кібербезпеки, відзначивши прогрес України у напрямку реформування сектору безпеки і оборони, боротьби з корупцією та реформи системи державних закупівель.

Заступник міністра запевнила у незмінності підтримки України у її боротьбі за відновлення територіальної цілісності, і висловила готовність і надалі поглиблювати двосторонню співпрацю…» ***(Наталія Рябцева. Секретар РНБО обговорив з представницею Норвегії питання кібербезпеки // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1835771-sekretar-rnbo-obgovoriv-z-predstavnitseyu-norvegiyi-pitannya-kiberbezpeki). 14.11.2019).***

***

«31 жовтня 2019 року відбулася конференція «Дезінформація та кібербезпека під час виборів в Україні: уроки 2019 року та майбутні перспективи», яка стала заключним етапом проекту «Протидія кіберзагрозам та дезінформаційним кампаніям в Україні», що реалізується Естонським центром Східного партнерства (ECEAP) у співпраці з CybExer Technologies та за підтримки Європейського Союзу.

Проект був частиною зусиль Європейського Союзу щодо підтримки стійкості України до кіберзагроз та дезінформації шляхом розбудови спроможності структур України, відповідальних за запобігання та управління кіберзагрозами та зміцнення навичок представників місцевих ЗМІ для виявлення та інформування громадськості про дезінформацію в кіберпросторі.

Голова Держспецзв'язку Валентин Петров, Начальник Державного центру кіберзахисту Держспецзв'язку Микола Худинцев та начальник Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ Микола Кулешов взяли участь у панельній дискусії на тему "Цифрова трансформація та кіберпотенціал".

Дискусія була присвячена майбутньому нарощуванню кіберспроможності в Україні: сучасним тенденціям та очікуваним викликам.

Під час дискусії Валентин Петров розповів про напрями реформування Держспецзв'язку, основні задачі та виклики, які постають перед службою.

"Державна служба спеціального зв'язку і захисту інформації. Місія цього органу зашита у його назву. Але я з подивом дізнався, що цей потужний орган має 94 функції, серед яких є навіть доставка кореспонденції. Тож перше, що ми хочемо

зробити - це провести аудит бізнес-процесів і позбавитися невластивих функцій. Процес походить від статусу організації. Якщо вона є військовою і я, як військова людина, керую цією організацією, я не можу займатись цивільним зв'язком. Ще цікава ситуація. У нашій структурі ще зашита адміністрація зв'язку, як центральний орган виконавчої влади в сфері телекомунікацій, і ми є центральним органом виконавчої влади, який скеровується через Міністерство цифрової трансформації віце-прем'єра, тобто ЦОВ у ЦОВі у ЦОВі, як матрьошка", - зазначив Валентин Петров.

Тож необхідно реформувати всю структуру державного органу. Також серед першочергових задач стоїть формування стратегії кібербезпеки. До цього процесу буде залучена громадськість та бізнесмени.

Після цього необхідно змінити законодавство. У найближчих планах Держспецзв'язку змінити три базових закони, які створювалися ще у 1994 році і наразі не відповідають сучасній моделі кіберзагроз.

На цьому етапі варто зауважити, що нині процес зміни законів України вкрай довгий, складний і забюрократизований. Після формування всіх необхідних документів проекти законів подаються у Верховну Раду, і коли (або якщо) до цих законопроектів доходить черга, депутати вносять свої правки і тільки потім голосують, якщо погодять правки.

Водночас модель кібербезпеки, як і всі моделі у світі технологій, змінюються і оновлюються із шаленою швидкістю. Тож не складно передбачити, що на той час, коли почнуть діяти "нові" закони вони вже також будуть неактуальні. Держслужбовцям варто було б замислитися над створенням певної динамічної моделі і перезавантаженням всієї системи виконавчої влади в галузі інформаційної безпеки, проте для цього мають бути залучені кваліфіковані фахівці.

Цікавим моментом під час панельної дискусії була заява у сфері інформаційної безпеки СБУ Миколи Кулешова. У той час як роботодавці, без перебільшення, всіх сфер діяльності країни жаліються на кадровий голод, на відсутність працівників необхідної кваліфікації, відмічають шалену трудову міграцію, у Департаменті контррозвідувального захисту інтересів держави пишаються чергою серед бажаючих у них працювати.

…Працівник СБУ також підкреслив бездоганні результати у кіберзахисті під час цьогорічних виборів в Україні. Він запевнив, що негаразди у 2014 році були досвідом, завдяки якому вдалося посилити захист інформації та не допустити втручання РФ у президентські та парламентські вибори.

Микола Кулешов подякував естонським партнерам за реалізацію спільного проекту «Протидія кіберзагрозам та дезінформаційним кампаніям в Україні». Він також зауважив, що Україна власними зусиллями гідно рухається у цьому напрямку і досягає неабияких результатів…» ***(Єва МЕРЕЖКО. Виклики у протидії кіберзагрозам в Україні // Дніпроград (https://dniprograd.org/2019/11/13/vikliki-u-protidii-kiberzagrozam-v-ukraini_82035). 13.11.2019).***

***

«Сьогодні у Брюсселі відбулося п'яте засідання Комітету асоціації Україна – ЄС, де обговорювали питання щодо політичного, економічного та галузевого співробітництва.

Міністерство цифрової трансформації України на заході представила заступник Міністра з питань розвитку публічних послуг Людмила Рабчинська. У своїй доповіді особливу увагу вона приділила питанню кібербезпеки, адже від вересня цього року Мінцифри відповідає за криптографічний і технічний захист інформації – і це питання є доволі нагальним для України.

«Роками наша країна веде постійну гібридну, асиметричну та кібернетичну війну, в якій наш сусід-агресор регулярно здійснює кібератаки на критичну інфраструктуру України. Комунальні сектори, включаючи енергетику, дамби, водопровідні та каналізаційні системи, є особливою ціллю їхньої кіберагресії», – зазначила у своїй промові Людмила Рабчинська.

Для прикладу вона згадала напади на українські енергооб'єкти, які почалися 2014 року. За словами заступника Міністра, ці напади, паралельно з іншими нещодавніми атаками, становлять складні нові виклики, які вимагають від України швидкого реагування, розгортання ефективних контрзаходів та створення нових засобів захисту від майбутніх атак.

Незважаючи на наявність політичної волі для боротьби з цими нападами, Україна стикається з критичними проблемами кібербезпеки, а саме:

– відсутність зрілої моделі кібербезпеки в усіх галузях промисловості;

– дефіцит кваліфікованих фахівців із кібербезпеки;

– обмежені кошти та ресурси для вирішення структурних питань.

– Зважаючи на всі ці виклики, Україні найближчим часом украй необхідно:

– усунути вразливості у комунальних секторах;

– зміцнити наші законодавчі та регуляторні умови, що дозволяють забезпечити більш ефективний обмін досвідом та важливою інформацією в державному, приватному та освітньому секторах;

– створити безпечну та надійну платформу для обміну актуальною інформацією та забезпечити постійне впровадження інноваційних кібертехнологій, послуг та рішень;

– навчати спеціалістів та розкрити потенціал талановитих висококваліфікованих лідерів – фахівців із кібербезпеки – як для Уряду, так і для приватного сектору;

– знаходити та підтримувати українських підприємців у сфері кібербезпеки.

Реалізація цих заходів дозволить Україні стати більш стійкою до кібератак та більш впевнено захищати критичні об'єкти інфраструктури, а також швидко відновлюватися після здійснених кібератак.

Людмила Рабчинська вважає, що унікальний цінний досвід України у протистоянні найсучаснішим та цілеспрямованим атакам слід використовувати для створення інновацій у сфері кібербезпеки. І таким чином зробити Україну надійним джерелом рішень, послуг і талантів у світовій індустрії кібербезпеки, що швидко зростає. Прикладом у цьому випадку є Естонія, для якої кібербезпека вже давно є основою успішної цифрової трансформації.

«Тому ми дуже вдячні Європейському Союзу за підтримку України у сфері кібербезпеки та запуск нового проекту «Підтримка ЄС для електронного урядування та цифрової економіки в Україні», що відбудеться найближчим часом», – наголошує Людмила Рабчинська.

Також українська сторона має намір встановити регулярний двосторонній діалог між Україною та ЄС у сфері кібербезпеки.» ***(Досвід України у протистоянні найсучаснішим атакам слід використовувати для створення інновацій у сфері кібербезпеки // Рупор Житомира (http://ruporzt.com.ua/interestingness/134152-dosvd-ukrayini-u-protistoyann-naysuchasnshim-atakam-sld-vikoristovuvati-dlya-stvorennya-nnovacy-u-sfer-kberbezpeki.html). 05.11.2019).***

***

«Во вторник израильская компания венчурного капитала "Team8" по кибербезопасности заявила, что она сотрудничает с Корпорацией экономического развития Нью-Йорка (NYCEDC), чтобы помочь укрепить экосистему кибербезопасности в городе.

Фирма заявила, что присоединится к городской инициативе на 100 миллионов долларов, чтобы сделать Нью-Йорк мировым лидером в области кибер-инноваций и создать около 10 000 новых рабочих мест. По данным NYCEDC, в прошлом году израильские фирмы "SOSA" и фонд венчурного капитала "Jerusalem Venture Partners" были в числе организаций, выбранных для участия в этой инициативе.

Партнерство "Team8" с NYCEDC будет сосредоточено на трех направлениях: обучение и развитие талантов на местах в сфере кибербезопасности, рост экосистемы кибербезопасности города и помощь в выявлении прорывных идей в научных кругах.» **(Израиль поможет Нью-Йорку стать мировым лидером в области кибербезопасности // ISRAland (http://www.isra.com/news/237212). 05.11.2019).**

***

«Компания ABB присоединилась к новому альянсу операционных технологий и кибербезопасности (Operational Technology Cyber Security Alliance, OTCSA), который будет заниматься устранением пробелов в безопасности OT, объектов критически важной инфраструктуры и систем промышленного управления (Industrial Control System, ICS). В этой структуре также участвуют Check Point Software, BlackBerry Cylance, Forescout, Fortinet, Microsoft, Mocana, NCC Group, Qualys, SCADAFence, Splunk и Wärtsilä.

У альянса OTCSA пять основных направлений деятельности. Усиление кибербезопасности на физическом уровне для сред OT и интерфейсов взаимодействия OT/IT. Обучение операторов OT тому, как защитить свою инфраструктуру OT с помощью систем управления рисками и использования лучших рекомендуемых архитектур/конструкций, которые полностью соответствуют международным стандартам, таким как IEC 62443. Поддержка поставщиков OT в вопросах безопасности архитектур систем OT, соответствующих интерфейсов и функций безопасности. Поддержка разработок, закупок, установки,

эксплуатации, обслуживания и внедрения более безопасных и надежных объектов критически важной инфраструктуры. Сокращение сроков внедрения безопасных и надежных объектов критически важной инфраструктуры.

Поскольку 60% организаций, использующих ICS, сообщили, что в прошлом году столкнулись с несанкционированным доступом в свои системы, а 97% указали на наличие проблем с безопасностью из-за сближения IT и OT, создание альянса OTCSA является критически важным этапом. Количество и сложность кибератак на OT и объекты критически важной инфраструктуры возрастают, что влияет на работу во всех отраслях – от нарушения производственных процессов и функционирования коммунальных систем до остановки систем жизнеобеспечения. Потенциально нарушение работы OT может оказать более серьезное воздействие, чем нарушение в информационных средах, и привести к гибели людей, экологическому ущербу и негативным финансовым последствиям…» ***(ABB вступила в глобальный альянс по кибербезопасности операционных технологий // Компьютерное Обозрение (https://ko.com.ua/abb_vstupila_v_globalnyj_alyans_po_kiberbezopasnosti_operacionnyh_tehnologij_130708). 01.11.2019).***

***

«Президент Литовської Республіки Гітанас Науседа та Президент України Володимир Зеленський під час візиту останнього до Вільнюса підписали низку двосторонніх документів. Про це заявив Науседа під час спільної пресконференції…

"Ми підписали нашу спільну декларацію президентів, яка охопить основні напрямки нашої роботи на найближчі роки. Також ми підписали декларацію про взаємне визнання електронної ідентифікації та довірчих послуг та електронних транзакцій. Також декларацію про наміри співробітництва у сфері кібербезпеки", - сказав литовський лідер...» ***(Саша Картер. Зеленський підписав низку двосторонніх документів з Литвою //Інформаційне агентство «Українські Національні Новини (https://www.unn.com.ua/uk/news/1838105-zelenskiy-ta-prezident-litvi-pidpisali-nizku-dvostoronnikh-dokumentiv). 27.11.2019).***

***

«Наступного року в Києві буде створено Центр кібербезпеки. Таку домовленість було досягнуто під час проведення 12-ї сесії Парламентської асамблеї Організації за демократію та економічний розвиток – ГУАМ.

До складу ГУАМ сходять чотири країни – Україна, Азербайджан, Грузія та Молдова. Як розповів… Глава ПА ГУАМ, керівник Постійної делегації Верховної Ради України у ПА ГУАМ Святослав Юраш, Центр кібербезпеки діятиме як освітній центр, і він має на меті запобігати та протистояти міжнародним кіберзлочинам, кіберзагрозам, сприяти боротьбі з комп‘ютерними вірусами.

"Сподіваюся, усі питання щодо створення Кіберцентру вирішаться до кінця року, - сказав Юраш. - Ідея Кіберцентру – це спільна інституція чотирьох країн ГУАМ, яка зможе здійснювати превенцію кіберзлочинів. Є ще також організація Гуам+ (це країни, які не входять до ГУАМ, але сприяють їй – Японія, США), а також Балтійська ассамблея, яка підписала з ПА ГУАМ домовленість про

співпрацю. І ми дуже активно співпрацюватимемо і з ними щодо створення Кіберцентру, щоб до нього долучилися кращі світові експерти".» ***(Наступного року в Києві буде створено Центр кібербезпеки // Голос України (http://www.golos.com.ua/news/104643). 27.11.2019).***

***

«Володимир Зеленський з прем'єр міністром Естонії Юрі Ратасом обговорили модернізацію освітньої програми в Україні та збільшення студентського обміну

Президент України Володимир Зеленський висловив уряду Естонії подяку за послідовну підтримку суверенітету й територіальної цілісності України та позицію щодо санкцій проти Росії. Про це йдеться у повідомленні пресслужби президента за підсумками його зустрічі з естонським прем'єрміністром Юрі Ратасом під час офіційного візиту до Таллінна.

Володимир Зеленський відзначив актуальність вивчення провідного досвіду Естонії у сферах діджиталізації, е-урядування та кібербезпеки.

«У вас є чудові фахівці у цифровій сфері. Ми хочемо використати ваш досвід у трансформації нашої країни. Бо у нас є великий проект «Держава у смартфоні», – наголосив Володимир Зеленський…» ***(Україна перейматиме досвід Естонії у сферах діджиталізації та кібербезпеки, - Зеленський // Українські медійні системи (https://glavcom.ua/news/ukrajina-pereymatime-dosvid-estoniji-u-sferah-didzhitalizaciji-ta-kiberbezpeki-zelenskiy-642582.html). 26.11.2019).***

***

«Секретар РНБО України Олексій Данілов провів зустріч з Надзвичайним і Повноважним Послом Держави Ізраїль в Україні Джоелем Ліоном під час якої обговорили співпрацю у сфері медицини та кібербезпеки…

"Серед ключових сфер співпраці Секретар РНБО України назвав кібербезпеку, засоби зв’язку та сучасну медицину. У свою чергу, Дж. Ліон запевнив, що Ізраїль і надалі підтримуватиме Україну, і висловив впевненість в успішності практичного співробітництва між нашими державами", - сказано у повідомленні.

Данілов наголосив, що Україну та Ізраїль об’єднує велика спільна історія та інтереси, тому "ми приречені на тісне співробітництво".

Також під час зустрічі сторони обмінялися думками щодо безпекової ситуації на Близькому Сході та у світі, а також обговорили актуальні питання двостороннього співробітництва та перспективи його поглиблення…» ***(Валерія Гуржий. Данілов обговорив з послом Ізраїлю співпрацю у сфері медицини та кібербезпеки // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1837918-danilov-obgovoriv-z-poslom-izrayilyu-spivpratsyu-u-sferi-meditsini-ta-kiberbezpeki). 26.11.2019).***

***

«Делегація ЦВК, яка наразі з робочим візитом перебуває в місті Осло, мала зустріч із Рором Торном – заступником директора Норвезької державної організації з безпеки та електронних сервісів (G.S.S.O). Організація підпорядкована як Службі розвідки, так і Міністерству оборони, розробляє заходи у

сфері кіберзахисту та запобігання тероризму. Контроль за її діяльністю здійснює відповідна комісія Стортінгу (Парламент Норвегії).

Представники організації розповідають, що особливо вразливими є бази політичних партій, де зберігається важлива інформація про партійну діяльність та їхніх членів. Витоки такої інформації часто мають різні насідки, однак здебільшого підривають довіру до політичної системи загалом.

Тому питання кібербезпеки стало пріоритетом державної політики, починаючи з парламентських виборів 2017 року. Держава запропонувала партіям провести консультації і тренінги щодо захисту власних ресурсів і платформ та ефективної протидії неправдивій інформації.

Норвезька державна організація з кібербезпеки здійснювала стрес-тести на проникнення до ресурсів партій. Їх метою було виявлення слабких місць і посилення кібербезпеки партій. За результатами було підготовлено поради щодо вдосконалення системи кіберзахисту.

Норвежці дуже активно взялись за кібербезпеку, взявши за мету бути готовим 24/7 виявити і запобігти кіберінцидентам.

Отже, підбиваючи підсумки, класифікуємо принципи, за якими працює Норвезька організація з кібербезпеки:

- ініціювання переговорів з політичними партіями;
- зустріч з керівництвом партій;
- проведення тренінгів з кібербезпеки, надання технічної оцінки та консультацій щодо кіберзахисту і кібербезпеки;
- запровадження постійних каналів зв'язку для подолання кіберзагроз і реагування на кіберінциденти…» ***(Кібербезпека виборів у Норвегії стала пріоритетом державної політики // Багнет (http://www.bagnet.org/news/politics/412380/kiberbezpeka-viboriv-u-norvegiyi-stala-prioritetom-derzhavnoyi-politiki). 22.11.2019).***

***

«Представники Держспецзв'язку взяли участь у засіданні національних контактних осіб з використання комунікаційної мережі ОБСЄ з проблематики кібербезпеки, яке відбулося в м. Відень (Австрія).

У засіданні, організованому Департаментом протидії транснаціональним загрозам Секретаріату ОБСЄ, взяли участь представники 40 держав-учасниць ЄС…

Під час засідання учасники заслухали доповіді та роз'яснення з впровадження заходів зі зміцнення довіри в кіберсередовищі, необхідності обміну інформацією для підтримки подальшої роботи та зміцнення міжнародного співробітництва.

Учасники з Нідерландів, Чехії та Словаччини наголосили на необхідності створення проекту Комітету з безпеки. Крім того, в рамках засідання розглядалися питання щодо проведення заходів та тренінгів з підвищення довіри ОБСЄ, розробки національної стратегії кібербезпеки, оновлення та адаптації законодавства у сфері кібербезпеки і безпеки інформаційно-комунікаційних технологій.

Крім того, під час засідання організатори провели ситуаційний тренінг-моделювання. В рамках тренінгу було змодельовано ситуацію кібератаки, учасники

мали відпрацювати протокол прийняття рішень та каналів міжнародної взаємодії при фіксуванні, нейтралізації та ліквідації наслідків кіберінцидентів та глобальних кібератак на об'єкти критичної інфраструктури…» ***(Представники Держспецзв'язку взяли участь у міжнародному засіданні з кібербезпеки // Агенція інформації та аналітики (https://galinfo.com.ua/news/predstavnyky_derzhspetszvyazku_vzyaly_uchast_u_mizhnarodnomu_zasidanni_z_kiberbezpeky_331412.html?print). 22.11.2019).***

***

Україна і НАТО мають активізувати співпрацю у сфері кібербезпеки, оскільки кіберзагрози з боку Російської Федерації є вкрай небезпечними як для України, так і для країн-членів Альянсу.

Про це заявив секретар РНБО Олексій Данілов під час зустрічі з делегацією Представництва НАТО в Україні на чолі з головою Представництва Александером Вінніковим, повідомляє прес-служба РНБО на офіційному сайті.

«В Україні Росія відпрацьовує кібератаки, які у майбутньому можуть бути спрямовані проти країн-членів НАТО, Європейського Союзу», - наголосив секретар РНБО.

На думку Данілова, нинішні виклики у безпековій сфері потребують нестандартних підходів до їх вирішення.

Як зазначається, сторони детально обговорили практичні аспекти двостороннього співробітництва, зокрема, матеріальну, технічну та консультативно-дорадчу допомогу, що надається Україні в рамках трастових фондів НАТО. Секретар РНБО України запевнив голову Представництва НАТО в готовності до інтенсифікації і посилення такої співпраці з боку РНБО України.

Своєю чергою Вінніков наголосив, що Альянс підтримує суверенітет і територіальну цілісність України і продовжуватиме «спільну роботу на благо її євроатлантичної інтеграції».

За його словами, НАТО і надалі надаватиме допомогу Україні як у рамках Комплексного пакета допомоги НАТО Україні, так і у питаннях підтримки законодавчого забезпечення реформування сектору безпеки і оборони.» ***(Україна і НАТО активізують співпрацю у сфері кібербезпеки, - Данілов // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (http://day.kyiv.ua/uk/news/191119-ukrayina-i-nato-aktyvizuyut-spivpracyu-u-sferi-kiberbezpeky-danilov). 19.11.2019).***

***

«В Киеве прошел информационный день программы НАТО "Наука ради мира и безопасности" (НРМБ), на которой представили разработки украинских ученых, созданные в рамках этой программы. Главная цель мероприятия - презентация возможностей сотрудничества для украинских ученых…

С 1991-го НАТО при помощи программы "Наука ради мира и безопасности" финансирует изыскания украинских ученых…

Из новых проектов, представленных на информационном дне программы НАТО "Наука ради мира и безопасности", интересен совместный проект двух украинских вузов - Черниговского национального технического университета и

КПИ в соавторстве с исследовательской лабораторией армии США и институтом обороны Болгарии. Ученые работают над программой киберзащиты, которая способна не только находить и отслеживать фейковые новости в сети, но и определять уровень напряжения в обществе. Общий бюджет этого исследования, рассчитанного на три года, составляет 433 тыс. евро. Часть КПИ, к примеру, более 153 тыс. евро. В эту сумму входят покупка оборудования, необходимого для исследований, стажировка за границей, оплата командировок, а также стипендии для молодых ученых - они составляют около 500 евро в месяц…» ***(Марина СИТНИК. Роботы-саперы и фейковые новости. Что делают украинские ученые для НАТО // DsNews (http://www.dsnews.ua/society/roboty-sapery-i-feykovye-novosti-chto-delayut-ukrainskie-22112019100000). 22.11.2019).***

***

Світові тенденції в галузі кібербезпеки

«Компанії ESET, Lookout та Zimperium допомагатимуть Google виловлювати з Play Store шкідливі додатки.

Як пише Google в офіційному блозі, її операційна система Android зараз встановлена на 2,5 млрд девайсах, що робить її «привабливою мішенню» для зловмисників.

Шкода може бути завдана через спеціальні програми чи частину коду, завдяки якому викрадатимуть дані користувачів чи шпигуватимуть за ними. Щоб боротися з такими явищами компанії створюють «Альянс захисту додатків».

«В рамках цього альянсу ми інтегруємо наші системи виявлення Google Play Protect зі скануючими системами кожного партнера. Це створить новий масив даних про додатки, які стоять у черзі на публікацію. Партнери проаналізують ці дані і будуть діяти ще один дуже важливий фільтр, перш ніж додаток почне відображатися у Play Store», — пише компанія…» ***(Google та компанії з кібербезпеки створюють «Альянс захисту додатків» // MediaSapiens (https://ms.detector.media/web/cybersecurity/google_ta_kompanii_z_kiberbezpeki_stvoryuyut_alyans_zakhistu_dodatkiv/). 07.11.2019).***

***

«Chronicle появился как экспериментальный проект подразделения X, принадлежащего Alphabet. Позднее он вырос в самостоятельный стартап, разрабатывающий технологии, связанные с безопасностью. В частности, в его распоряжении оказалась антивирусная система VirusTotal. Изначально предполагалось, что это будет независимая компания со своими контрактами и политикой – по крайней мере, так говорил её генеральный директор Стивен Джиллетт (Stephen Gillett). Однако в июне этого года Chronicle утратила свой статус после того, как официально присоединилась к Google, чтобы стать частью подразделения Google Cloud. И, согласно изданию Motherboard, это одна из главных причин её скорой гибели.

По-видимому, многие сотрудники Chronicle узнали об этом в день официального анонса, что рассматривалось некоторыми как предательство.

Проблема возникла и с оплатой труда, поскольку поисковый гигант не захотел проводить корректировку зарплат, которые оказались ниже, чем у других сотрудников Google. Люди начали покидать компанию из-за «дистанцирования генерального директора» и «отсутствия ясности относительно будущего Chronicle».

Сам Джилетт ушёл на другую должность в Google, в то время как соучредитель и главный директор по безопасности Майк Вячек (Mike Wiacek) покинул компанию. В своём прощальном сообщении он сказал, что у Chronicle была одна из самых здоровых и ярких корпоративных культур. О своём уходе также заявил и директор по технологиям Уилл Робинсон (Will Robinson).

Прежде чем стать частью Google, Chronicle анонсировала свой первый коммерческий продукт под названием Backstory, идея которого была позаимствована у Google Photos. Сервис обрабатывает большие объёмы данных, выгруженных компаниями с устройств (или серверов) сотрудников, выявляет ложные тревоги и потенциальные опасности для более тщательного анализа.

Google в свою очередь заявила, что Chronicle является «критически важным» элементом в области безопасности, поэтому поисковый гигант «активно инвестирует» в команду стартапа.» ***(Игорь Мозуль. Стартап по кибербезопасности Chronicle находится на грани закрытия, и причина этому – Google // ООО «ХОТЛАЙН» (https://itc.ua/news/startap-po-kiberbezopasnosti-chronicle-nahoditsya-na-grani-zakrytiya-i-prichina-etomu-google/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+itc-ua+%28ITC.ua%29). 11.11.2019).***

***

«Сегодня по всему миру насчитывается не больше 2,8 миллионов специалистов по информационной безопасности. Спрос, по данным ИБ-консорциума «(ISC)²» Cybersecurity Workforce Study 2019 превышает 4 миллиона заявок. Это – 154% разницы.

В основу исследования легли опросы 3237 высокопоставленных специалистов, отвечающих за вопросы кибербезопасности в различных секторах на территории Северной, Латинской Америки, в Европе и Тихоокеанско-Азиатском регионе.

«Чтобы в полное мере понять запрос и принципы работы сегмента кибербезопасности в бизнес-секторе, “(ISC)²” опрашивали как сертифицированных профессионалов на официальных должностях, так и ИТ -специалистов, которые тратят на вопросы кибербезопасности не менее 25% своей рабочей недели», - говорится в опубликованном “(ISC)²” отчете. – «Эти вопросы могут включать безопасность данных, оценку и управление рисками, приведение практики киберзащиты, выявление угроз и минимизацию их последствий»

Отдельным звеном выделили архитектуру сетевой безопасности, а также мониторинг, обслуживание и поддержку систем кибербеззащиты. По подсчетам исследователей, наибольший дефицит кадров наблюдается в Тихоокеанско-Азиатском регионе (2,6 млн человек). Это не удивительно, учитывая, что в этот ареал входят самые густонаселенные страны мира. На втором месте Латинская Америка, там недостаток специалистов составляет 600 тысяч человек. На третьем - Североамериканский регион - 561 тысяча человек.

Лишь в 62% крупных организаций со штатом более 500 человек есть должность директора по информационной безопасности. И только в половине компаний меньшего размера встречаются отдельные директора по ИБ. 48% опрошенных организаций планируют увеличить расходы на обучение персонала основам информационной безопасности. Помимо состоявшихся специалистов, компании готовы нанимать выпускников университетов (28%), сотрудников консалтинговых компаний и переманивать кадры у подрядчиков (27%) и поставщиков оборудования и решений по вопросам безопасности (25%), а также переводить в подразделение ИБ сотрудников других отделов внутри своей организации (26%) и лиц, готовых переучиваться с нуля (24%). Только 42% опрошенных экспертов заявили, что начинали свою карьеру с информационной безопасности; остальные пришли в эту область из других сфер деятельности…» ***(Предложение и спрос на ИБ-специалистов. 154% разницы // SecureNews (https://securenews.ru/predlozhenie-i-spros-na-ib-specialistov/). 13.11.2019).***

***

«Avast будет финансировать исследования CTU в сфере искусственного интеллекта и машинного обучения кибербезопасности…

Богатые данные Avast из более чем 400 миллионов устройств по всему миру будут объединены с исследованием сложных угроз CTU для проведения исследований по средствам предотвращения и пресечения попыток киберпреступников использовать новые технологии, включая искусственный интеллект. Цели лаборатории включают публикацию прорывных исследований в этой области, а также усовершенствование механизма обнаружения вредоносных программ Avast.

«Сила этого партнерства в том, чтобы облегчить обмен новаторскими исследованиями и их реальным применением. Чтобы ИИ работал хорошо в контексте кибербезопасности, нам нужно много информации. Но нам также нужны специалисты по кибербезопасности и ученые для детального анализа вредоносного ПО». Сотрудничество с CTU предназначено для объединения самого богатого в мире набора данных по кибербезопасности с одними из лучших специалистов в области искусственного интеллекта, чтобы мы могли учиться друг у друга», - сказал генеральный директор Avast Ондрей Волчек…» ***(Avast и Чешский технический университет создают совместную лабораторию искусственного интеллекта и кибербезопасности // SecureNews (https://securenews.ru/cheshskiy-universitet-i-avast/). 06.11.2019).***

***

«В общей сложности $315 тыс. заработали участники хакерских соревнований Pwn2Own 2019, проходивших 6-7 ноября в Токио. В ходе соревнований участниками было обнаружено 18 ранее неизвестных уязвимостей, о которых производители затронутых продуктов были сразу же уведомлены. На исправление проблем производителям отведен срок в 90 дней.

Организатором Pwn2Own является Trend Micro Zero Day Initiative (ZDI), а призовой фонд составил $750 тыс. Наибольшую сумму по итогам двух дней ($195 тыс.) выиграла хорошо известная по прошлым соревнованиям команда

Fluoroacetate в составе двух человек – Амата Камы (Amat Cama) и Ричарда Чжу (Richard Zhu). По итогам двух дней Pwn2Own Fluoroacetate стала чемпионом уже третий раз подряд.

В первый день соревнований участники Pwn2Own заработали $195 тыс. за эксплуатацию уязвимостей в смарт-телевизорах, маршрутизаторах и смартфонах. Для взлома им было предоставлено 17 различных устройств, в том числе «умный» дисплей Portal и шлем виртуальной реальности Oculus Quest от Facebook. Оба эти устройства участвовали в Pwn2Own впервые.

Участники соревнований осуществили 10 попыток взлома, и большинство из них оказались успешными. Команде Fluoroacetate удалось взломать смарт-телевизоры Sony X800G и Samsung Q60, «умную» аудиоколонку Amazon Echo и смартфон Xiaomi Mi9, а также похитить изображение с Samsung Galaxy S10 через NFC.

Команда Flashback взломала «умные» маршрутизаторы NETGEAR Nighthawk Smart WiFi Router (R6700) и TP-Link AC1750 Smart WiFi Router. Команда F-Secure Labs попыталась взломать маршрутизатор TP-Link и смартфон Xiaomi Mi9, однако попытки оказались успешными только частично.

Во второй день соревнований участники Fluoroacetate смогли выполнить произвольный код на Samsung Galaxy S10, за что получили $50 тыс. Команды Flashback и F-Secure Labs взломали маршрутизатор TP-Link AC1750, получив $20 тыс. каждая. Во второй день F-Secure Labs все-таки удалось взломать Xiaomi Mi9 и заработать $30 тыс.» ***(Pwn2Own 2019 в Токио: Итоги двух дней соревнований // SecurityLab.ru (https://www.securitylab.ru/news/502389.php). 08.11.2019).***

***

«В прошлом месяце крупнейшие игроки доменной индустрии решили объединиться против киберпреступности…

По итогам обсуждения ведущие реестры и регистраторы доменных имен выработали документ, который называется «Структура борьбы со злоупотреблениями в DNS». Представитель группы объединившихся компаний тогда сказал в интервью сайту CircleID, что: «Компании, которые поучаствовали в создании документа, признают, что здоровье и безопасность DNS имеют важнейшее значение для доверия к Интернету и его безопасности».

Также участники признали, что «они играют важную, но зачастую неправильно понимаемую роль как распорядители этого общественного ресурса». Злоупотребления в DNS группа определила как 5 широких категорий вредоносной активности: «вредоносные программы, бот-сети, фишинг, фарминг и спам (когда он служит механизмом доставки для других форм злоупотреблений в DNS)».

Мы задали несколько вопросов Саманэ Таджализадехуб (Samaneh Tajalizadehkhoob) — ведущему специалисту по безопасности, стабильности и отказоустойчивости функционирования Интернета в ICANN — международной некоммерческой организации по управлению доменными именами и IP-адресами. Нас интересовало то, как объединение регистраторов повлияет на регуляцию Интернета.

Как вы думаете, может ли инициатива регистраторов DNS привести Интернет к более саморегулирующемуся состоянию, чем сейчас?

Саманэ: Безусловно, усилия ведущих реестров и регистраторов доменных имен, направленные на борьбу со злоупотреблениями в DNS — это пример усилий отрасли по саморегулированию. Чем больше сделают лидеры рынка, тем больше участников отрасли к ним присоединятся. Кроме того, будет снижена существующая в настоящее время информационная асимметрия среди участников отрасли о средоточиях злоупотреблений, а это может привести к снижению затрат на мониторинг и смягчение злоупотреблений. И да, в отрасли могут возникнуть дополнительные стимулы, чтобы противодействовать нарушениям в DNS.

Из-за того, что Интернет это сильно взаимосвязанная сеть, трудно будет заметить как усилия отдельного оператора по противодействию нарушениям в ДНС скажутся на других [проще говоря, это не то же самое как если Марк Цукерберг запретит оскорбительный контент в Facebook, в котором сидит полмира — тогда новую политику соцсети почувствуют все]. Это еще раз подчеркивает важность коллективной инициативы, такой как эта.

Возможно ли ограничить вмешательство правоохранительных органов в нашу цифровую жизнь, если регистраторы DNS будут играть более значительную роль в противодействии киберпреступности?

Саманэ: Цифровая жизнь — это широкий термин, и вмешательство правоохранительных органов может сильно отличаться от страны к стране. Вполне вероятно, что правоохранительные органы будут продолжать играть свою роль, особенно когда существует ощущение вакуума, в котором могут действовать нарушители. Дополнительные инициативы, направленные на решение этой проблемы, могут снизить необходимость участия правоохранительных органов.

Несмотря на то, что упреждающие меры со стороны регистраторов очень важны и могут повлиять на противодействие нарушениям, мы должны помнить, что они могут принимать только определенные меры в дополнение к обмену информацией: это отключение или перенаправление доменных имен, используемых для веб-сайтов и других сервисов. Таким образом, средства, необходимые регистраторам для устранения злоупотреблений в DNS, ограничены и несут в себе потенциальный побочный ущерб, например, если будет установлено, что одна из страниц на Facebook несёт неправомерный контент, приостановка доменного имени facebook.com, скорее всего, будет неуместна.

Кроме того, другие субъекты, участвующие в защите доменного имени, такие как владелец веб-сайта, владелец регистрации и хостинг-провайдер, который размещает веб-сайт, могут быть также или даже более эффективны в противодействии нарушениям, в зависимости, конечно, от типа нарушений. Например, если вредоносная программа размещена на взломанном сервере, то именно хостинг-провайдер может принять эффективные меры.» ***(Специалист ICANN — об инициативе DNS-регистраторов против киберпреступности // РосКомСвобода (https://roskomsvoboda.org/52019/). 12.11.2019).***

***

«Власти США пытаются убедить максимальное количество союзников и колеблющихся членов Генеральной ассамблеи ООН голосовать против российской резолюции «О противодействии использованию информационно-коммуникационных технологий в преступных целях».

В Вашингтоне и столицах стран Евросоюза считают, что инициатива «позволит таким странам, как Россия и Китай, создать одобренный ООН инструмент блокировки критических по отношению к властям сайтов и слежки за диссидентами»…

По словам одного из не названных по имени европейских собеседников The Washington Post, российская инициатива «не про борьбу с киберпреступностью», а про «контроль над интернетом». Россия и Китай, по мнению источника, «используют все средства», чтобы навязать мировому сообществу нормы, усиливающие полномочия властей по управления сетью.

Четырехстраничная резолюция, внесенная Россией на рассмотрение Третьего комитета Генассамблеи ООН (занимается социальными и гуманитарными вопросами, а также правами человека) и поддержанная его членами на этой неделе, представляет собой обновленную версию документа, впервые представленного Москвой в прошлом году.

«Ни одна страна мира, вне зависимости от уровня ее технологического развития, не может бороться с этими угрозами в одиночку и даже группой стран, — было сказано в начале ноября текущего года в выступлении представителя РФ М.В.Заболоцкой на презентации проекта резолюции. — Во многом это связано с тем, что киберпреступность является транснациональным феноменом и имеет трансграничную природу, против которой региональных мер на сегодняшний день уже недостаточно. Многие страны до сих либо находятся на пути к формированию специализированного законодательства для борьбы с киберкриминалом, либо не имеют его вовсе. Несмотря на масштабы проблемы, международное сообщество не имеет полноценной международно-правовой базы сотрудничества и даже единой терминологии. В данном контексте становится очевидной необходимость выработки универсального международно-правового механизма в этой области».

Первый вариант российской резолюции тоже встретил сопротивление США и их союзников, но в итоге был поддержан 94 членами Генассамблеи ООН при 58 проголосовавших против. При этом сама резолюция на первый взгляд никаких революционных формулировок не содержит.

Неприемлемым для западных стран документ делает, по сути, один абзац: о необходимости созыва «межправительственного комитета экспертов открытого состава для разработки международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях».

США и их союзники убеждены, что новые международно-правовые инструменты в этой сфере не нужны, поскольку есть Будапештская конвенция Совета Европы о компьютерных преступлениях 2001 года. На сегодняшний день ее ратифицировали 64 страны и подписали еще 4, включая все страны ЕС, а также США, Японию, Австралию и Израиль.

До недавнего времени единственными странами—членами Совета Европы, не подписавшими конвенцию, были Россия и Сан-Марино. Но в этом году Сан-Марино все-таки присоединилось к большинству. Россию же не устраивает ст. 32 конвенции о «трансграничном доступе к хранящимся компьютерным данным». Она

позволяет различным спецслужбам без официального уведомления проводить операции в компьютерных сетях третьих стран.

Отстаивая необходимость новой конвенции, заместитель постпреда РФ при ООН Геннадий Кузьмин заявил в понедельник: «Преступления в сфере информационно-коммуникационных технологий носят трансграничный характер. Однако законодательство государств является фрагментарным и не гармонизировано с точки зрения как материального, так и процессуального права. Ряд государств имеют возможность пользоваться региональными инструментами, однако их число и сфера географического охвата ограниченны. Налицо необходимость углубления международного сотрудничества государств в этой области, выведения его на новый универсальный уровень». При этом дипломат пообещал, что спецкомитет будет учитывать в своей работе имеющиеся международные и региональные инструменты, включая Будапештскую конвенцию.

Противники нововведений, однако, обещаниям Москвы не верят. Накануне голосования в Третьем комитете базирующаяся в США Ассоциация прогрессивных коммуникаций (APC) опубликовала открытое письмо 36 своих членов, в котором содержится призыв высказаться против российской резолюции. Правозащитники опасаются, что российская инициатива «подорвет использование интернета в качестве инструмента реализации прав человека, а также социального и экономического развития».

«Учитывая действия российских властей по усилению контроля над сетью, последним проявлением чего стало принятие в России закона «о суверенном интернете», ее шаги по разработке юридически обязывающей конвенции по киберпреступности требуют особо критического изучения»,— настаивают подписанты.

«Завалить» российскую резолюцию, однако, несмотря на публичную и кулуарную работу ее противников, не получилось. За документ в Третьем комитете проголосовало 88 стран, против — 58. Но решающим станет голосование на Генеральной ассамблее, которое пройдет в декабре текущего года.

Документы Генассамблеи ООН сами по себе не являются юридически обязывающими, однако могут запустить механизмы, результатом работы которых в итоге станет имеющая силу закона конвенция. Так это в свое время было, например, с Конвенцией ООН против коррупции и Конвенцией ООН против транснациональной организованной преступности. Москва, судя по всему, рассчитывает именно на такой вариант.» ***(США выступили против российской резолюции о киберпреступности на Генассамблее ООН // РосКомСвобода (https://roskomsvoboda.org/52402/). 20.11.2019).***

***

«Компания Palo Alto Networks, занимающая ведущие позиции на глобальном рынке кибербезопасности, заключила определяющее соглашение о покупке калифорнийского стартапа Aporeto примерно за 150 млн долл. деньгами. Сделка должна быть завершена в течение II-го финансового квартала Palo Alto Networks.

Основанный в 2016 г., Aporeto предлагает платформу облачной безопасности «нулевого доверия» (zero-trust), которая автоматически генерирует подмножества

идентификационных параметров для любой рабочей нагрузки, анализируя метаданные из любой доступной системы и сведения о личности пользователя. Zero-trust это приобретающая всё большую популярность концепция, базирующаяся на требовании сохранять жёсткий контроль доступа и на доверять никому по умолчанию, даже тем пользователям, кто уже находится в сети.

Как заявил в интервью соучредитель стартапа, Амир Шариф (Amir Sharif), решения Aporeto облегчают комплексную аутентификацию, авторизацию и шифрование для всех прикладных сегментов, включая виртуальные машины, контейнеры и микросервисы.

«Они позволяют системе безопасности следить за приложением где угодно, независимо от архитектуры сети, включая прохождение глобальной сети через разрозненные облака, — сказал Шариф. — Поскольку безопасность Aporeto встроена в инфраструктуру, она делает защиту незаметной и необременительной для разработчика. Это позволяет разработчикам двигаться быстрее и сосредоточиться на основной функциональности, а не на утомительном соблюдении требований безопасности».

Председатель правления и CEO Palo Alto Networks Никеш Апора (Nikesh Arora) сообщил, что уникальная технология микросегментации Aporeto обеспечит дальнейшее совершенствование возможностей нативной облачной безопасности, обеспечиваемых Prisma Cloud. Кроме того, покупка расширит клиентскую базу Palo Alto Networks, добавив в неё такие организации, как Comcast Ventures, Bart, British Columbia, Informatica и Exact Transactions.

Новое поглощение стало уже седьмым для Palo Alto Network за два последних года. В марте 2018 г. она купила Evident.io за 300 млн долл., спустя месяц — Secdo за 100 млн долл., в октябре 2018 г. — RedLock за 173 млн долл. Уже в текущем году, в феврале, компания купила Demisto за 560 млн долл., в мае — Twistlock (410 млн долл.) и PureSec, а 5 сентября — Zingbox за 475 млн долл.» ***(Palo Alto Networks купит провайдера облачной безопасности за 150 млн долл. // Компьютерное Обозрение (https://ko.com.ua/palo_alto_networks_kupit_provajdera_oblachnoj_bezopasnosti_za_150_mln_doll_131033). 27.11.2019).***

***

Сполучені Штати Америки

«Отвечающим за кибербезопасность сотрудникам Белого дома поручили активнее выявлять утечки информации…

В документе говорится, что отслеживать подозрительные действия необходимо в круглосуточном режиме. Больше всего Служба безопасности переживает за сведения, касающиеся передвижений и графика Президента страны.

Новостной портал Axios также опубликовал признания сотрудников спецотделов. Они рассказали, что в их задачи входил просмотр истории в браузерах работников Белого дома. Кроме того, они использовали программы, позволяющие идентифицировать тех, кто открывал служебные документы, в частности график

Главы государства. Журналисты сделали вывод, что таким образом Дональд Трамп пытается избавиться от персонала, нанятого еще при Бараке Обаме.

Белый дом комментировать публикацию отказался.» ***(Дональд Трамп приказал ужесточить контроль за распространением информации // SecureNews (https://securenews.ru/donald-trump-prikazal-uzhestochit-kontrol-informatcii/). 16.11.2019).***

***

«Агентство связи и информации НАТО (NCI) опубликовало тендер на сумму 20 млн. евро (22 148 300 долларов США) для апгрейда служб кибербезопасности…

«Благодаря этим закупкам, НАТО заменит аппаратное и программное обеспечение, чтобы организация могла поддерживать наивысшую степень киберзащищенности на всем предприятии», - говорится в пресс-релизе.

Программа CP120 освежит все системы безопасности Коммуникационных и Информационных Систем поэтапным подходом, «таким образом уменьшая риски и сбои в работе СНГ, не отставая от современных инструментов. Каждый этап также будет включать в себя ряд улучшений. Первый проект, «Срочное управление устареванием», направлен на повышение эффективности всех систем, срок эксплуатации которых истекает в текущий срок исполнения.

Агентство планирует заключить контракт к концу 2019 года и приступить к реализации в начале первого квартала 2020 года.» ***(НАТО потратит $22 миллиона на обновление систем кибербезопасности // SecureNews (https://securenews.ru/nato-potratit-mnogo-deneg-na-kiberbezopasnost/). 10.11.2019).***

***

«Судья в штате Джорджия (США) обвиняется в хакерстве за попытку очистить свой рабочий компьютер от шпионского ПО. Как сообщает издание Daily Report, против Кэтрин Шрэдер (Kathryn Schrader) и троих нанятых ею исследователей выдвину ты обвинения по трем пунктам в незаконном проникновении.

В феврале нынешнего года Шрэдер заподозрила, что прокурор округа Гуиннетт Дэнни Портер (Danny Porter) установил на компьютер в ее офисе шпионскую программу. С целью выяснить, так это или нет, судья обратилась к частному детективу Ти Джей Уорду (TJ Ward), который в свою очередь нанял IT-специалистов Эда Крэмера (Ed Kramer) и Фрэнка Кэрика (Frank Karic).

Для поиска потенциального шпионского ПО Крэмер и Кэрик установили на компьютер судьи инструмент для перехвата пакетов Wireshark. Однако следователи уверены, будто Шрэдер и нанятые ею специалисты устроили незаконную слежку за компьютерной сетью суда штата. В частности, их обеспокоил перехват трафика с помощью Wireshark.

Дело усложняется еще и тем, что Крэмер ранее был осужден по серьезной статье и отбывал наказание в тюрьме, но был отпущен досрочно по медицинским причинам. В феврале, когда его нанял Уорд, Крэмер был снова арестован, и тем самым условия его досрочного освобождения были нарушены. По мнению

следствия, в связи с этим у Крэмера не должно быть никакой возможности доступа к IT-системам, связанным с судебными материалами.

В ожидании суда Шрэдер была отстранена от всех текущих дел. Судья, частный сыщик и двое нанятых им IT-специалистов свою вину отрицают. Уорд и Кэрик были отпущены под залог в размере $25 тыс., а Крэмер находится в тюрьме.

По словам защитников Шрэдер, даже если судья и наняла частного детектива с целью проинспектировать свой компьютер на предмет наличия на нем шпионской программы, она имела на это полное право. В конце концов, это ее компьютер и она может его исследовать.» ***(Судья обвиняется в хакерстве за попытку найти на своем ПК шпионское ПО // SecurityLab.ru (https://www.securitylab.ru/news/502392.php). 08.11.2019).***

***

Країни ЄС

«14 ноября 2019 года французское правительство подписало трехлетний пакт о кибербезопасности с восемью ведущими компаниями в стране. Инициатива пришлась на тот период, когда крупнейшие в мире страны усиливают меры безопасности на фоне громких инцидентов.

Как сообщает агентство Reuters со ссылкой на заявление властей Франции, было заключено соглашение с компаниями Airbus, Dassault Aviation, Thales, Safran, Ariane Group, MBDA, Naval Group и Nexter. Финансовые и другие подробности этой сделки не раскрываются.

За год до подписания этого акта по кибербезопасности Эммануэль Макрон представил «Парижский призыв к обеспечению доверия и безопасности в киберпространстве» — декларацию правил поведения государств и частных игроков в киберпространстве. Идейное ядро документа — девять направлений действий: от предотвращения атак на критическую инфраструктуру до противодействия распространению вредоносного программного обеспечения.

Одна из тем — предотвращение кибервмешательства в ИТ-инфраструктуру, обеспечивающую проведение выборов.

Власти Франции давно всерьез озаботились современными вызовами в сфере кибербезопасности и в 2019 году решили выделить €1,6 млрд на борьбу с несанкционированными вмешательствами в киберпространстве.

Был создано специальное управление кибербезопасности. В него, а также в главное управление внешней безопасности (DGSE) и генеральную дирекцию по вооружению (DGA) дополнительную тысячу кибервоенных планируется привлечь тысячу военных киберспециалистов до 2025 года.

Эммануэль Макрон предлагал создать независимую от США армию, которая бы защищала в том числе и киберпространство. Трамп назвал предложение французского лидера «очень оскорбительным», заметив, что «Европа должна сначала заплатить свою справедливую долю в НАТО». ***(Франция заключила пакт о кибербезопасности с крупнейшими в стране компаниями // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5624334-Franciya-zaklyuchila-pakt-o-kiberbe.html). 15.11.2019).***

***

«Финский центр регистрации населения провел симуляцию атаки вирусов-вымагателей на системы городских администраций. Согласно данным, в эксперименте участвовало около 200 городов и общественных организаций Финляндии.

Таким образом, власти страны оттачивают реакцию в случае атаки хакеров, которые будут требовать выкуп в цифровой валюте. Во время тестирования преступники атаковали 235 систем, а также угрожали совершить кибератаки, если они не получат выкуп в биткоинах к определенной дате. Центр регистрации населения Финляндии, работающий при Министерстве финансов, провел уже две подобных симуляции, а третья должна пройти на следующей неделе.» ***(Финляндия готовится отбивать атаки киберпреступников // PAYSPACE MAGAZINE (https://psm7.com/security/finlyandiya-gotovitsya-otbivat-ataki-kiberpprestupnikov.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Payspacemagazine+%28Payspacemagazine%29). 25.11.2019).***

***

Російська Федерація та країни ЄАЕС

«…В окупованому Криму вже почали спостерігатися проблеми із захистом особистих даних користувачів інтернету у зв'язку з набранням чинності в РФ закону «Про стійкий інтернет у Росії».

Про це… заявила експертка Кримської правозахисної групи Ірина Сєдова.

«Діють обмеження щодо блокування деяких сайтів, які Росія вважає "неправильними", екстремістськими або ж просто небажаними. Вони іноді вибірково блокуються за рішеннями судів, іноді просто довільно з незрозумілих причин. Ми знаємо, що російські соцмережі видають доступ до персональних даних людей, яких держава вважає екстремістами чи терористами, або ж не сподобався якийсь допис. Вони можуть відкрити кримінальну справу і запитати ці дані у власника сайту через спецслужби. Такі випадки теж були, ми це фіксуємо», – розповіла Сєдова.

Відповідно до положень цього закону, за наявності загрози безпеці Роскомнагляд може брати на себе централізоване керування мережею, тобто фактично керувати трафіком і блокувати доступ до того чи іншого сайту без попередження, пояснюють у IMI.

Дія цієї системи буде також поширена і на анексований Росією Крим, нагадують правозахисники…» ***(У Криму є проблеми із захистом особистих даних користувачів — Ірина Сєдова // MediaSapiens (https://ms.detector.media/web/cybersecurity/v_krimu_e_problemi_iz_zakhistom_osobistikh_danikh_koristuvachiv_irina_sedova/). 19.11.2019).***

***

«Новый документ, который сейчас готовится в профильных министерствах, перечислит вещи, в ответ на обнаружение которых Роскомнадзор сможет переходить на централизованное управление Рунетом

…В данный момент проект постановления со списком угроз Рунету находится на согласовании в профильных министерствах. Издание приводит список из трех видов угроз.

Угроза безопасности

Помимо, ресурсов запрещенных федеральным законом «Об информации», которые согласно документу представляют угрозу безопасности российской Сети, существует ещё несколько угроз, под которыми понимаются кибератаки и другие, «как преднамеренные, так и непреднамеренные информационных воздействий на средства и сети связи, в результате которых может быть нарушено их функционирование, а также угрозы нарушения доступности для граждан информационных онлайн-ресурсов органов федеральной и региональной власти и органов местного самоуправления».

В список также входят «угрозы нарушения информационной безопасности автоматизированных систем управления сетями связи операторов и технологических сетей связи, систем управления точками обмена трафиком, технических средств и ПО центра мониторинга и управления сетью связи общего пользования, технических средств противодействия угрозам, национальной системы доменных имён, критической информационной инфраструктуре РФ».

Угроза устойчивости

Под ней понимается угроза, «при которой нарушается работоспособность сети связи при отказе части её элементов, а также в условиях внешних дестабилизирующих воздействий природного и технологического характера». К таким угрозам, по данным источника издания, отнесут: невозможность доступа к услугам связи из-за аварий или перегрузки узла связи, из-за которых для физ- и юрлиц становятся недоступными услуги связи или невозможно вызвать экстренные службы, а также невозможность доступа к услугам связи для критически важных объектов, которая может привести к нарушению или прекращению их функционирования.

Угроза целостности

Под ней понимается угроза «нарушения способности взаимодействия сети связи, при котором становится невозможным установление соединений между пользователями услуг связи или информационными ресурсами. Речь идет, во-первых, об угрозах нарушения взаимодействия сети связи общего пользования с зарубежными сетями электросвязи, из-за чего становится невозможным организация соединений с пользователями услугами связи или информресурсами, расположенными за рубежом, а во-вторых, об угрозах нарушения функционирования интернета, из-за которых невозможна организация взаимодействия российских интернет-пользователей с другими, в том числе теми, кто находится за границей».

Созданный правительством список угроз российской Сети появился в СМИ спустя несколько дней после вступления в силу закона о «суверенном Рунете». В этом законе говорится, что Роскомнадзор, в случае возникновения вышеприведенных угроз, может переходить на централизованное управление российским интернетом.» ***(Правительство определило угрозы Рунету. В них***

вошло распространение запрещенной информации // РосКомСвобода (https://roskomsvoboda.org/51819/). 06.11.2019).

***

«Минюст зарегистрировал приказ Роскомнадзора 31.07.2019 № 225 «Об утверждении Положения о Центре мониторинга и управления сетью связи общего пользования»…

Центр обеспечивает исполнение организационно-технических мер, необходимых для реализации Роскомнадзором полномочий, предусмотренных федеральным законом №126-ФЗ «О связи».

В задачи данного Центра входят:

— обеспечение учета информации;

— проведение мониторинга в целях выявления угроз;

— обеспечение информирования в случае возникновения угроз;

— обеспечение осуществления централизованного управления;

— обеспечение предоставления операторам связи технических средств противодействия угрозам и их установки.

Центр взаимодействует с федеральными органами исполнительной власти, с государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности РФ, лицами, участвующими в централизованном управлении, иными организациями, в том числе международными, целью функционирования которых является обеспечение информационной безопасности.

Центр осуществляет сбор, хранение и обработку, в том числе проверку и классификацию информации:

1) о точках обмена трафика;

2) об инфраструктуре ССОП, полученную в хоже мониторингга ССОП;

3) о линиях связи, пересекающих госграницу РФ;

4) представляемой в соответствии с требованиями 126-ФЗ операторами связи, собственниками или иными владелльцами технологических сетей связи, имеющими номер автономной системы (об имеющемся у низх номере автономной системы, а также о сетевых адресах; о взаимодействии с имеющими такой номер операторами; о местах подключения своих средств связи, пересекающими госграницу; и т.п.);

5) о функционировании технических средств противодействия угрозам.

Закон о «суверенизации Рунета» Президент РФ Владимир Путин подписал в начале мая текущего года, и с начала ноября госведомства должны централизовано управлять российским сегментом Сети, фильтруя трафик, а провайдеры — устанавливать устройства «по противодействию угрозам устойчивости». ***(За «суверенностью» Рунета проследит Центр мониторинга // РосКомСвобода (https://roskomsvoboda.org/52606/). 25.11.2019).***

***

«Федеральная служба безопасности подвергла критике законопроект №747513-7 о создании цифровых профилей граждан РФ. По мнению ФСБ, система, в которой, по замыслу разработчиков, должны сконцентрироваться

персональные данные всех россиян, включая силовиков и судей, будет постоянно подвержена угрозе взлома и утечек. О замечаниях ФСБ к законопроекту о цифровом профиле говорится в письме руководителя службы оперативной информации и международных связей ФСБ Сергея Беседы начальнику государственно-правового управления президента РФ Ларисе Брычевой…

Единая база, считает ФСБ, грозит утечками информации, в том числе о лицах, подлежащих государственной защите — судьях, прокурорах, следователях и сотрудниках силовых ведомств. ФСБ отмечает, что в законопроекте не были учтены замечания, и он по-прежнему нуждается в доработке.

…эксперты отметили, что ФСБ опасается «крайне опасной идеи централизации информации». Кроме того в законе не прописан механизм интегрирования данных из различных ведомств…» ***(ФСБ боится утечек цифровых профилей силовиков // РосКомСвобода (https://roskomsvoboda.org/52111/). 13.11.2019).***

***

Інші країни

«Министр обороны Швейцарии Виола Амхерд открыла новый центр Cyber Defence Campus, направленный на развитие сотрудничества между армией, учеными и хакерами в области кибербезопасности.

Цель этого центра, расположенного в Высшей технической школе Цюриха (ETH), состоит в том, чтобы задействовать таланты и возможности таких учреждений, как Цюрихский центр информационной безопасности и конфиденциальности (Zurich Information Security & Privacy Center - ZISCВнешняя ссылка) и Швейцарский инновационный парк в Цюрихе (Switzerland Innovation Park ZurichВнешняя ссылка). Основным направлением партнерства является содействие обмену технологиями и инновациями с приоритетом технологий киберзащиты, информационной безопасности, научных данных и искусственного интеллекта…

Одним из первых мероприятий, которые организует Cyber Defence Campus, станет конференция по авиационной кибербезопасности, запланированная на 19 и 20 ноября. Мероприятие будет посвящено уязвимости авиационной инфраструктуры для злонамеренных, в том числе хакерских атак…» ***(Надежда Капоне. Министр обороны открыла в Цюрихе «Кампус киберзащиты» // SWI swissinfo.ch (https://www.swissinfo.ch/rus/%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80-%D0%BE%D0%B1%D0%BE%D1%80%D0%BE%D0%BD%D1%8B-%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D0%BB%D0%B0-%D0%B2-%D1%86%D1%8E%D1%80%D0%B8%D1%85%D0%B5--%D0%BA%D0%B0%D0%BC%D0%BF%D1%83%D1%81-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B7%D0%B0%D1%89%D0%B***

8%D1%82%D1%8B--/45356046?utm_source=multiple&utm_campaign=swi-rss&utm_medium=rss&utm_content=o). 08.11.2019).

***

«Правительство Австралии опубликовало проект кодекса по обеспечению безопасности «Интернета вещей» (IoT). Документ вынесен на общественное обсуждение, которое продлится до 1 марта 2020 года.

Кодекс Code of Practice: Securing the Internet of Things for Consumers предоставит индустрии лучшие рекомендации и советы по обеспечению кибербезопасности. Он охватывает все IoT-устройства, включая «повседневные интеллектуальные девайсы, подключаемые к интернету, такие как смарт-телевизоры, часы и домашние звуковые колонки».

Кодекс основан на 13 принципах, подробно изложенных на трех страницах. Первые три имеют наивысший приоритет и включают в себя отсутствие встроенных дублированных или слабых паролей, реализацию политики раскрытия уязвимостей (производители устройств, поставщики услуг и разработчики приложений должны иметь общедоступную точку контакта) и постоянное обновление программного обеспечения, в том числе и прошивки.

Также в кодексе содержатся меры по обеспечению безопасного хранения учетных данных, защиты персональной информации и применению «адекватного отраслевого стандарта» шифрования к данным в хранилищах и в Сети.

Согласно кодексу, устройства и службы должны работать по принципу наименьших привилегий с отключенной неиспользуемой функциональностью, проверять программное обеспечение с использованием механизмов безопасной загрузки, обеспечивать устойчивость систем к сбоям и мониторинг данных телеметрии на предмет кибераномалий, содержать инструкции для пользователей для работы с персональными данными, а также сделать установку и обслуживание простым.» ***(Австралия разработала проект кодекса по обеспечению безопасности «Интернета вещей» // SecurityLab.ru (https://www.securitylab.ru/news/502708.php). 19.11.2019).***

***

«Совместное исследование Marsh и Risk and Insurance Management Society (RIMS) содержит вывод о том, что кибернетические инциденты второй год подряд считаются главным риском для бизнеса Индии.

…62% респондентов оценивают кибернетические риски наиболее серьезной угрозой для бизнеса. На втором месте (17%) – риски, связанные с погодными явлениями, на третьем (9%) – риск финансового кризиса.

«Индия, как и другие страны, подвержена кибератакам, и среди корпораций растет осознание необходимости обеспечения надлежащих мер контроля за кибербезопасностью», — сказал Санджай Кедия, главный исполнительный директор Marsh India. Он также подчеркнул, что использование передовых технологий в бизнесе должно сопровождаться соответствующей кибернетической защитой, которая требует дополнительных инвестиций.

Отчет составлен на основании опроса, в котором приняли участие 179 респондентов, среди которых, — топ-менеджеры и высокопоставленные

специалисты по управлению рисками из 23 отраслей.» ***(Индийский бизнес больше всего опасается кибератак, аномальной погоды и финансового кризиса // УкрСтрахование (https://www.ukrstrahovanie.com.ua/news/indijskij-biznes-bolshe-vsego-opasaetsya-kiberatak-anomalnoj-pogody-i-finansovogo-krizisa). 27.11.2019).***

***

«…На этой неделе цифровые платформы Лейбористской партии Великобритании подверглась мощной DDoS-атаке. Лидер партии Джереми Корбин охарактеризовал атаку как «сложную и масштабную», однако, по данным пресс-службы Лейбористской партии, она не увенчалась успехом, благодаря «надежной системе безопасности».

Вслед за атакой участники Lizard Squad заявили, что в их распоряжении имеется ботнет для осуществления масштабных DDoS-атак. По их словам, атака на Лейбористскую партию Великобритании является политически мотивированной. «Сегодняшняя DDoS-атака на Лейбористскую партию является демонстрацией того, что правительство, поддерживающее террористов, не может управлять страной», - цитирует киберпреступников издание The Independent.

Как заявили Lizard Squad, персональные учетные записи членов семьи Корбина также были скомпрометированы.

По словам исследователя безопасности компании Mimecast Джонатана Майлза (Jonathan Miles), незадолго до атаки Lizard Squad активно рекламировали в Twitter свой сервис по осуществлению заказных DDoS-атак. Возможно, атака на Лейбористскую партию была заказной, считает Майлз. Сразу после инцидента бывший глава Центра правительственной связи Брайан Лорд (Brian Lord) предположил, что ответственность за него лежит на враждебном государстве. Представители самой партии отказываются строить какие-либо предположения по поводу происхождения и мотивов атак.» ***(Группировка Lizard Squad взяла ответственность за атаку на Лейбористскую партию // SecurityLab.ru (https://www.securitylab.ru/news/502645.php). 15.11.2019).***

***

«У США низка відомств опублікували спільну заяву, в якій йдеться, що Росія, Китай, Іран "й інші недружні іноземні" країни спробують втрутитися в президентські вибори 2020 року

Спільна заява глав міністерства юстиції, міністерства оборони, міністерства національної безпеки, директора Національної розвідки, ФБР, АНБ і Агентства кібербезпеки і захисту інфраструктури була опублікована на сайті Пентагону.

За даними уряду і американських спецслужб, втручання у вибори буде здійснюватися "за допомогою різноманітних засобів, включаючи кампанії в соціальних ЗМІ, операції з дезінформації або руйнівні кібератаки на федеральну і локальну виборчу інфраструктуру".

Відзначається, що наразі в США немає ознак зламу або руйнування виборчої інфраструктури, які дозволили б стороннім силам перешкодити проведенню голосування, вплинути на його підсумки або перешкодити підрахунку голосів, проте відстеження можливих загроз триває.

Для захисту виборчого процесу глави міністерств і спецслужб закликають громадян США бути пильними і повідомляти про всі підозри в місцеві відділення виборчих органів, ФБР і міністерство національної безпеки.

Щоб перешкодити втручанню і своєчасно виявити загрози, уряд США співпрацює з усіма 50 штатами, місцевими відділеннями виборчих органів і партнерами в приватному секторі…» ***(У США назвали три країни, які можуть втрутитися у вибори-2020 // Espreso.tv (https://espreso.tv/news/2019/11/06/u_ssha_nazvaly_try_krayiny_yaki_mozhut_vtrutytysya_u_vybory_2020). 06.11.2019).***

***

«Контррозвідка Великої Британії MI5 провела секретну операцію по захисту телефонів депутатів Палати громад від атак російських хакерів…

…деякі телефонні номери політиків зазнали кібератак.

На час операції депутатам заборонили користуватися особистими телефонами та комп'ютерами, а також рекомендували не піднімати на засіданнях питання про зломи.

За словами одного з парламентаріїв, йому повідомили, що було здійснено «узгоджену спроба злому моїх банківських рахунків з боку іншої держави».

У Великій Британії очікують публікацію доповіді, в якій розглядається втручання Росії в британську політику, включаючи фінансування Консервативної партії та вплив на результати референдуму щодо Brexit 2016 року.

Прем'єр-міністра Великої Британії Бориса Джонсона звинувачують у затягуванні публікації доповіді. Спочатку комітет з розвідки і безпеки парламенту мав оприлюднити звіт 4 листопада, проте публікацію відклали до проведення парламентських виборів, запланованих на 12 грудня…» ***(У Великій Британії пройшла секретна операцію із захисту телефонів депутатів від російських хакерів — ЗМІ // ТРК «ТВА» (https://tva.ua/2019/11/10/u-velykij-brytanii-projshla-sekretna-operatsiiu-iz-zakhystu-telefoniv-deputativ-vid-rosijskykh-khakeriv-zmi/). 10.11.2019).***

***

«Пана Альзабара, колишнього інженера Twitter, звинувачують у отриманні доступу до особистих даних понад 6 тис. користувачів Twitter у 2015 році після того, як його нібито завербували агенти Саудівської Аравії.

У оприлюднених 6 листопада звинуваченнях США стверджують, що саудівські агенти шукали особисту інформацію про користувачів Twitter, включаючи відомих критиків уряду Саудівскької Аравії.

Про це йдеться у документах суду назвали цих осіб: громадянин США Ахмед Абуаммо та Алі Альзабара з Саудівської Аравії…

Третя особа, громадянин Саудівської Арамії Ахмед Алмутаїрі, також звинувачується у шпигунстві.

Повідомляється, що громадянам Саудівської Аравії вперше пред'явлено звинувачення у шпигунстві всередині США. У звинуваченнях стверджується, що пан Алмутаїрі виступав посередником між двома працівниками Twitter та саудівськими чиновниками.

Ахмад Абуаммо з'явився в суді в Сіетлі і був затриманий до чергового слухання, яке відбудеться в п'ятницю, 8 листопада. Також його звинувачують у фальсифікації документів та дачі неправдивих даних ФБР. Пан Абуаммо покинув роботу менеджера з питань медіапартнерства у Twitter у 2015 році…

Зараз Алі Альзабара та Ахмед Алмутаїрі, скоріше за все, перебувають у Саудівській Аравії.

Пана Альзабара, колишнього інженера Twitter, звинувачують у отриманні доступу до особистих даних понад 6 тис. користувачів Twitter у 2015 році після того, як його нібито завербували агенти Саудівської Аравії.

У заяві компанії Twitter визнали, що розуміють ризики цієї ситуації…» ***(Колишніх співробітників Twitter у США звинуватили у шпигунстві на користь Саудівської Аравії // MediaSapiens (https://ms.detector.media/web/cybersecurity/kolishnikh_spivrobitnikiv_twitter_u_ssha_zvinuvatili_u_shpigunstvi_na_korist_saudivskoi_aravii/). 07.11.2019).***

***

«В СМИ стала появляться информация о новой, ранее неизвестной технологии GPS-спуфинга, предположительно тестируемой правительством КНР. Уже более года жертвами новой атаки становятся суда в порту Шанхая и его окрестностях.

В отличие от ранее известных атак на GPS, когда приемники GPS-сигнала в определенной области отображали свое местоположение в ограниченном спектре фиксированных ложных координат, новая атака заставляет ретрансляторы сразу нескольких кораблей одновременно показывать ложные координаты. Вместе эти координаты образуют кольцеобразные узоры, которые некоторые эксперты уже успели окрестить «кругами на полях».

Как сообщает MIT Technology Review, летом 2018 года американское грузовое судно Manukai следовало по реке Хуанпу в порт Шанхая. Согласно международному законодательству, все коммерческие суда (за исключением мелких) должны быть оснащены автоматической идентификационной системой (АИС). Каждые несколько секунд АИС транслирует название, курс, местоположение и скорость судна, а также отображает все эти данные для других судов поблизости. Данные о местоположении АИС получает от спутников GPS.

Капитан Manukai увидел на экране АИС судно, следующее по одному с ним курсу со скоростью 8 узлов. Внезапно судно исчезло, а через несколько минут появилось снова, но уже в доке. Затем судно исчезло и появилось в проливе, а потом снова оказалось в доке и так несколько раз. Для того чтобы выяснить, где все-таки находится корабль, капитан взглянул в бинокль. Как оказалось, все это время судно не покидало док.

В конечном итоге рапорт о произошедшем попал в поле зрения Центра современной обороны C4ADS в Вашингтоне. Эксперты изучили данные систем АИС, приобретенные у стартапа, регистрирующего данные АИС по всему миру, и

обнаружили, что наибольшая интенсивность атак пришлась на июльский день 2018 года. В тот день помимо Manukai жертвами спуфинга также оказалось порядка 300 кораблей вблизи Шанхая.

При визуализации данных, охватывающих дни и недели, координаты судов образовывали большие круги. Подобные «узоры» привели специалистов C4ADS в недоумение. Эксперты также установили, что загадочные круги образовывали не только корабли. Проанализировав карту передвижений шанхайских велосипедистов, использующих фитнес-приложение Strava, исследователи также увидели кругообразные узоры. То есть, атака затронула все устройства с поддержкой GPS, не только корабли…» ***(Ранее неизвестная атака на GPS создает «корабли-призраки» // SecurityLab.ru (https://www.securitylab.ru/news/502739.php). 20.11.2019).***

***

Створення та функціонування кібервійськ

«Британская контрразведка провела учения, в рамках которого аккаунты некоторых политиков страны были взломаны так называемыми «российскими хакерами». Из-за этого обладателям взломанных аккаунтов на время запретили пользоваться гаджетами.

Как стало известно газете The Mirror , МИ-5 организовала сверхсекретную операцию для защиты британских парламентариев от российски хакеров. Часть политиков и их сотрудники получили предупреждения после того, как контрразведчики обнаружили, что их аккаунты были взломаны.

На время операции контрразведчики запретили политикам пользоваться гаджетами и рассказывать об атаках русских хакеров. Это привело к срыву кампаний и проблемам с подготовкой к выборам.

Парламентариям также было сказано не разглашать, что их данные оказались в доступе у «постороннего источника», но сообщать в МИ-5, если они заметят что-то странное в телефоне или компьютере.

Один из парламентариев рассказал газете, что контрразведчики обнаружили согласованные усилия по взлому аккаунтов со стороны иностранной державы.

Издание отмечает, что теперь политики знают, как надо поступать при любых «странных действиях» на их телефонах и компьютерах — обращаться в MI5.» ***(Mi5 защитила политиков от русских хакеров // SecurityLab.ru (https://www.securitylab.ru/news/502407.php). 10.11.2019).***

***

«Правительство государства-острова совместно с представляющим интересы США Американским институтом на Тайване (АИТ) анонсировали проведение киберучений. В центре внимания угрозы, исходящие от «Северной Кореи и других субъектов», хотя ранее официальный Тайвань говорил, что большинство кибератак осуществляется с материкового Китая.

Учения будут проводиться чуть меньше недели, и одной из их составляющих станет защита от попыток взлома правительственных сайтов путём введения госслужащих в заблуждение. Частные компании также будут задействованы.

Для Тайваня, по словам Вирла Ноувенса (Veerle Nouwens) из Британского Королевского института исследований в области обороны и безопасности UK, материковый Китай рассматривается как один из основных источников кибератак на острове. Гендиректор Тайваньского агентства кибербезопасности, также отмечает Ноувенс, сообщил о порядка 30 миллионов кибератак в месяц на правительственные сети, и около половины из этих нападений происходит из КНР. «Поэтому, независимо от страны происхождения [атак], усиление кибербезопасности становится всё более приоритетной задачей для любого правительства или компании частного сектора», — подытоживает он.

Кибернаступательные и защитные учения были официально запущены и.о. директора АИТ Рэймондом Грином (Raymond Greene) на организованном Microsoft мероприятии. Он охарактеризовал их как «обозначение новой границы» в киберсотрудничестве Вашингтона и Тайбэя. В последнее время между Китаем и Тайванем снова обострились отношения, но самая большая угроза сегодня, уверяет Грин, «не высадка войск на берег, а попытки непримиримых оппонентов использовать открытость наших обществ и сетей против нас». Во многих отношениях он считает киберугрозы наиболее значительным риском. Он добавил, что злоумышленники пытаются подорвать выборы, поставить под угрозу критическую инфраструктуру и нанести ущерб финансово-торговой отрасли.

В борьбе за защиту Тайваня принимают участие должностные лица других стран, включая Австралию, Индонезию, Японию. Тренировки будут проводиться с помощью специального американского симулятора международных компьютерных атак, используемого в учениях Cyber Storm раз в два года.» ***(США и Тайвань отрабатывают совместное противостояние кибервойнам // РосКомСвобода (https://roskomsvoboda.org/51736/). 05.11.2019).***

***

Кіберзахист критичної інфраструктури

«Некоммерческая организация MITRE при поддержке ряда частных компаний учредила технологический фонд Engenuity, призванный стимулировать развитие критической инфраструктуры на предприятиях. Организация займется привлечением инвестиций для проектов в таких сферах, как ИБ, телекоммуникации, здравоохранение и транспорт.

С 1958 года MITRE, финансируемая рядом государственных агентств США, накопила значительный междисциплинарный опыт и планирует использовать его для реализации проектов по улучшению критической инфраструктуры.

В отличие материнской организации, Engenuity финансируется за счет частного капитала. Среди учредителей фонда — компании Microsoft, Bank of America, Fujitsu, Siemens и другие корпорации. Как считают создатели проекта,

участие подобных организаций позволит быстрее переводить разработки ученых в практическую плоскость.

Первым крупным проектом фонда стал Центр продуманной защиты от киберугроз (The Center for Threat-Informed Defense). Он займется разработкой и наполнением MITRE ATT&CK — специализированного фреймворка с данными о кибератаках. База данных содержит сведения об инцидентах в сфере ИБ, упорядоченные по этапам — от первоначального проникновения до кражи данных или перехвата управления системой.

Помимо этого, Центр сосредоточит усилия на прикладных исследованиях для создания учебных продуктов, имитирующих реальные атаки, а также составления рейтинга угроз.

Среди других направлений деятельности Engenuity упоминают практические способы повышения безопасности сетей 5G с помощью развития методов шифрования, а также анализ данных для повышения эффективности транспортной и медицинской системы.

Председателем совета директоров Engenuity стал ИБ-эксперт и бывший конгрессмен США Майк Роджерс (Mike Rogers).

Инициатива MITRE может стать ответом на развивающиеся угрозы — по мнению экспертов, современные кибератаки становятся более динамичными благодаря средствам автоматизации. Как выяснили ИБ-аналитики, ранее нападение состояло в среднем из семи последовательных этапов, но сейчас их число сократилось до трех.» ***(Egor Nashilov. Организация MITRE создала фонд для внедрения ИБ-решений // Threatpost (https://threatpost.ru/mitre-starts-engenuity-foundation-to-help-critical-infrastructure/34839/). 15.11.2019).***

***

Захист персональних даних

«Директор з партнерських платформ Facebook Константінос Папамілтіадіс заявив, що нові правила щодо даних користувачів не були повністю реалізовані, тому близько сотні розробників додатків все ж змогли отримати до них доступ.

Близько сотні розробників додатків для соціальної мережі Facebook, незважаючи на заборону компанії, отримали доступ до даних користувачів…

Директор з партнерських платформ Facebook Константінос Папамілтіадіс у своєму блозі заявив, що нові правила щодо даних користувачів не були повністю реалізовані, і близько сотні все ж змогли отримати до них доступ. Хоча, додав він, цей доступ для них вже обмежили.

За його словами, не було виявлено, що цей витік завдав шкоди користувачам. У компанії говорять, що тепер всіх партнерів «відрізали» від цих даних.

В той же час пишуть, що компанія Facebook звернулася до 11 розробників з проханням видалити дані користувачів, які ті отримали за останні кілька місяців.

Але в компанії не назвали додатків, які збирали інформацію про користувачів. Відомо, що такі додатки були створені для того, аби ділитися відео в

групах соцмережі…» ***(У Facebook знову стався черговий витік даних — ЗМІ // MediaSapiens (https://ms.detector.media/web/cybersecurity/u_facebook_znovu_stavsya_chergoviy_vitik_danikh_zmi/). 07.11.2019).***

***

«Офшорный банк Cayman National Bank на острове Мэн подтвердил утечку данных в результате взлома, - передает Медуза.

Масштаб утечки банк не раскрывает. UnicornRiot утверждает, что объем украденных данных сопоставим с «панамским архивом». Хакеры, по данным UnicornRiot, получили доступ к данным и счетам не менее 3800 компаний, фондов и физических лиц. Речь идет в том числе о клиентах с Кипра, из Великобритании и с Британских Виргинских островов.

О взломе 17 ноября сообщил сайт Motherboard, ответственность за кражу данных взял на себя хакер Финеас Фишер (Phineas Fisher). Он назвал атаку политически мотивированной и призвал других хакеров присоединиться к «борьбе с неравенством и капитализмом».

Финеаса Фишера связывают с группировкой Anonymous (действует с 2003 года). Фишер брал на себя ответственность за взлом британско-германского производителя систем видеонаблюдения Gamma Group и за атаку на серверы итальянской Hacking Team, которая выпускает софт для взлома по заказу полиции и спецслужб. Кроме того, в 2016 году во время попытки военного переворота в Турции Фишер заявил о взломе компьютеров правящей партии страны.» ***(Хакеры взломали мировой офшорный банк. Утечку сравнивают с «панамским архивом» // SecureNews (https://securenews.ru/hakeri-vzlomali-ofshorniy-bank/). 19.11.2019).***

***

«***Сфера здравоохранения – мировой рекордсмен по «сливу» данных.*** К таким выводам пришла команда киберсоциологов Университета Мичиган и Университета Джона Хопкинса, - передает CyberScoop. В рамках исследования ученые выяснили, что за последние несколько лет госпитали, больницы и страховые компании «слили» больше данных, чем похищено хакерами.

Исследование охватило более 3000 случаев утечек информации за 2009-2019 годы более чем 33 американских госпиталей и, в большинстве своем, эти утечки происходили из-за некомпетентности исполнительных лиц, самих медиков и систем защиты конфиденциальных данных. Более 164 пациентов пострадали в ходе раскрытия приватной информации. При этом, 53% утечек связаны с ошибками в работе сотрудников, обеспечивающих защиту секретной информации пациента.

В качестве примеров, иллюстрирующих данный процесс, специалисты предъявили личные разговоры медиков с членами семьи, распределение данных о пациентах на неавторизованных устройствах, и ошибки с пересылкой личной информации не тем адресатам. Разумеется, реальных примеров куда больше.

Как бы там ни было, исследование позволяет глубже взглянуть на проблему распределения и шифрования личной пользовательской информации. Понять, как медицинские данные могут быть использованы в маркетинговых целях, кому это нужно. На данный момент специалисты работают над продвижением нового плана

киберзащиты здравоохранения.» ***(Сфера здравоохранения – мировой рекордсмен по «сливу» данных // SecureNews (https://securenews.ru/rekordsmen-po-slivu-dannih/). 14.11.2019).***

***

«Компьютерные системы американской компании InfoTrax Systems были взломаны более 20 раз в период с мая 2014 года по март 2016 года. Компания узнала о взломе только после того, как на сервере закончилось свободное место из-за архива, созданного злоумышленником.

Как сообщает Федеральная торговая комиссия США (FTC), взлом произошел в мае 2014 года, когда киберпреступник использовал уязвимости на сервере и на web-сайте одного из клиентов компании для получения удаленного контроля над сервером компании и доступа к конфиденциальной информации 1 млн клиентов.

FTC подала в суд на InfoTrax Systems за неспособность защитить персональные данные клиентов. Преступник тайно получал доступ к системе 17 раз в течение 21 месяца, а 2 марта 2016 года начал собирать персональную информацию клиентов, включающую имена, номера социального страхования, физические адреса, адреса электронной почты, номера телефонов, логины и пароли для учетных записей 4100 дистрибьюторов и администраторов в службе InfoTrax. Утечка данных также включала информацию о платежных картах некоторых клиентов (полные или частичные номера карт, CVV и даты истечения срока действия), а также информацию о банковских счетах, включая номера счетов и банковские коды.

Компания обнаружила компрометацию 7 марта 2016 года. После обнаружения утечки злоумышленнику удалось взломать системы компании по меньшей мере еще два раза. 14 марта 2016 года преступник похитил более 2300 уникальных номеров платежных карт, включая имена, физические адреса, CVV и даты истечения срока действия, а также другие платежные данные. Затем он внедрил еще один вредоносный код для сбора свежих данных с web-сайта клиента.

Согласно FTC, InfoTrax Systems не справилась с «инвентаризацией и удалением устаревших персональных данных, проверкой кода своего программного обеспечения и тестированием сети, обнаружением загрузки вредоносных файлов, адекватным сегментированием сети и внедрением средств защиты для обнаружения необычной активности». В результате, теперь компания должна внедрить комплексную программу защиты данных, а также каждые два года проводить проверку своих систем.» ***(Американская компания обнаружила взлом, когда на сервере закончилось свободное место // SecurityLab.ru (https://www.securitylab.ru/news/502584.php). 14.11.2019).***

***

«4-терабайтная база данных оказалась в свободном доступе на облаке Google, её владелец пока не установлен

Специалисты по информационной безопасности нашли на просторах интернета базу данных с личных данными 1,2 миллиарда человек, пользователей соцсетей. Это одна из самых больших утечек в истории. Wired сообщает, что пострадали пользователи Facebook, Twitter, LinkedIn и Github.

Утечку нашли специалисты по информационной безопасности Боб Дьяченко и Винни Тройя. Базу данных они обнаружили на облаке Google и сразу после обнаружения обратились в ФБР, чтобы бюро приняло меры. ФБР временно отключило сервер, на котором находилась база данных, однако за то время, что она там была, любой желающий из любой страны мира мог воспользоваться чужими личными данными.

Что было в базе?

В базе данных было найдено 50 миллионов мобильных номеров и больше 600 миллионов емейлов, а также истории трудоустройства с LinkedIn. Особенно примечательно то, что такая большая база с личными данными хранилась в одном месте. Винни Тройя отмечает, что «это первый раз, когда я вижу столько профилей из социальных сетей с информацией о пользователях, собранных в базу данных такого размера. <…> С точки зрения преступника, если ты хочешь ограбить этих людей, у тебя достаточно данных, чтобы начать».

Как произошла утечка?

Обнаружившие утечку специалисты думают, что найденная база данных — часть базы данных компании People Data Labs. PDL — это торговец большими данными. Компания собирает данные и продаёт их различным сервисам для настройки маркетинга. Исследователь Винни Тройя сравнил найденные данные с базой данных компании и сделал вывод, что они почти идентичны. В найденном массиве не было данных разве что об образовании пользователей, но информация о 50 случайных пользователях совпала с той, что хранится в People Data Labs. Однако пока нет 100% доказательств, что в сеть утекла база данных именно этой компании. Напомним, что летом этого года Facebook получил рекордный штраф в $5 млрд, за то, что данные 87 миллионов пользователей были незаконно получены и использованы Cambridge Analitica.» ***(Из Facebook, Twitter и LinkedIn утекли данные 1,2 миллиарда пользователей // РосКомСвобода (https://roskomsvoboda.org/52614/). 25.11.2019).***

***

«Соцмережі Facebook та Twitter повідомили про витік даних сотень користувачів Android. Причиною витоку стало використання власних акаунтів у цих соцмережах для входу в окремі додатки…

Експерти з кібербезпеки зазначили, що додаток для розробки програмного забезпечення під назвою One Audience надавав доступ до особистих даних користувачів стороннім розробникам.

У Facebook видалили додатки One Audience і Mobiburn та закликали користувачів уважніше ставитися до додатків, в яких вони авторизуються за допомогою акаунтів в соцмережах.

Twitter звернувся до компаній Google та Apple з проханням вжити додаткових заходів з посилення безпеки.

Витік даних не зачепив користувачів iOS…» ***(Facebook та Twitter повідомили про витік даних сотень користувачів // Дзеркало тижня. Україна (https://dt.ua/TECHNOLOGIES/facebook-ta-twitter-povidomili-pro-vitik-danih-soten-koristuvachiv-331060_.html). 27.11.2019).***

***

«Мабуть, кожного обурила інформація про витік даних у Facebook. Нас дуже засмучує, що різні сайти збирають про нас персональні дані. Але часто у цьому винні самі користувачі.

Таку думку…висловив експерт із кібербезпеки у компанії Dell Бернхард Отупал.

"Дуже часто проблема із витоком персональних даних – це вина самих користувачів. Більшість просто не читає умови, а одразу погоджується, навіть не знаючи на що дає свою згоду. Останнім часом було дуже багато критики навколо збору даних Facebook. Але соцмережа збирає лише ті дані про користувачів, на які вони дають згоду", – пояснив експерт.

Тож він радить уважніше читати умови, на які користувач дає згоду. При цьому він визнає, що умови згоди, які надають ресурси, зазвичай дуже довгі та незрозумілі. Це теж проблема, адже дехто може не зрозуміти, на що погоджується, або банальне не зможе дочитати до кінця.

"Я думаю, їх потрібно зробити коротшими і зрозумілішими для широкого кола людей. В Євросоюзі існує регламент щодо захисту персональних даних усіх осіб (GDPR). Це важливий крок щодо регуляції захисту персональних даних", – додав Отупал…» ***(Сторонні ресурси збирають персональні дані – чому у цьому винні самі користувачі // (https://24tv.ua/techno/storonni_resursi_zbirayut_personalni_dani__chomu_u_tsomu_vinni_sami_koristuvachi_n1236368). 20.11.2019).***

***

«Крупный мобильный оператор Германии T-Mobile заявил о крупной утечке данных. Несанкционированный доступ к личным данным более 1 млн клиентов был зафиксирован подразделением T-Mobile по кибербезопасности.

Похищенные данные не включают в себя финансовую информацию, номера социального страхования или пароли. Мошенники получили доступ к именам пользователей, их почтовым адресам, номерам счетов и номерам телефонов.

Представители компании заявили, что кибератака уже пресечена, но могли быть скомпрометированы данные до 1,5% пользователей услуг T-Mobile. Общее количество пользователей немецкого мобильного оператора составляет около 75 млн человек…» ***(Хакеры получили доступ к конфиденциальным данным клиентов T-Mobile // PAYSPACE MAGAZINE (https://psm7.com/security/xakery-poluchili-dostup-k-konfidencialnym-dannym-klientov-t-mobile.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Payspacemagazine+%28Payspacemagazine%29). 25.11.2019).***

***

«Павел Дуров заявил, что всем нужно срочно удалить WhatsApp со смартфонов и других устройств. Действительно, к безопасности и конфиденциальности этого мессенджера давно скопилось много вопросов. Соберём всю важную информацию по этой теме, чтобы вы знали, какие опасности могут поджидать в самом популярном мессенджере. Разбираемся, что не так с WhatsApp.

Павел Дуров заявил: WhatsApp – это троян

Дуров написал: WhatsApp не только не защищает ваши сообщения WhatsApp – это приложение постоянно используется в качестве трояна для слежки за фото и сообщениями, которые не относятся к WhatsApp. Зачем им [разработчикам] это делать? Facebook был частью программ слежки задолго до того, как купил WhatsApp.

Разработчик Telegram подчеркнул: все баги, которые находят в WhatsApp, идеально подходят для слежки за пользователями. А если вспомнить утиный тест (если оно выглядит как утка, плавает как утка и крякает как утка, то это, вероятно, и есть утка), то от приложения действительно хочется избавиться.

По словам Дурова, “Facebook и WhatsApp делились практически всем с теми, кто утверждал, что работает на правительство”.

Израильтяне добились впечатляющих успехов во взломе WhatsApp

В мае 2019 года эксперты по кибербезопасности нашли в системе голосовых звонков WhatsApp дыру, которую использовали для слежки за активистами. Работало это и на Android, и на iOS.

Вредонос разработала израильская компания NSO Group. Он позволял установить на смартфон с WhatsApp шпионские приложения. Чтобы взломать смартфон, хакеры просто звонили жертве по WhatsApp. Приложение автоматически принимало звонок – без ведома владельца! Затем на смартфон загружали шпионское ПО для кражи данных. Записи о звонках удалялись, чтобы никто ничего не заподозрил.

В WhatsApp проблему признали. Разработчики сравнили код вредоноса с другими разработками NSO Group и пришли к выводу, что почерк действительно один и тот же. Затем они за четыре дня разработали патч безопасности и попросили всех пользователей (1,5 млрд человек, на минуточку!) установить его… Когда о проблеме с WhatsApp стало известно всем, в NSO Group развели руками. Дескать, мы проверяем всех клиентов и расследуем случаи злоупотребления. Не мы охотимся за правозащитниками, а значит, мы ни в чем не виноваты и ничего не нарушили…» ***(Чем опасен WhatsApp – его взломали полностью // Український телекомунікаційний портал (https://portaltele.com.ua/news/events/chem-opasen-whatsapp-ego-vzlomali-polnostyu.html). 22.11.2019).***

***

«Десять организаций, включая разработчиков решений в сфере информационной безопасности и обществ по защите жертв домашнего насилия, объединились в международную группу по борьбе со сталкерским ПО (Coalition Against Stalkerware), чтобы защитить пользователей от слежки через цифровые устройства. Среди членов коалиции – «Лаборатория Касперского», Avira, американский фонд Electronic Frontier Foundation, Европейская сеть по работе с виновными в домашнем насилии (European Network for the Work with Perpetrators of Domestic Violence), G DATA CyberDefense, Malwarebytes, американская Национальная сеть по противодействию домашнему насилию (National Network to End Domestic Violence), NortonLifeLock, американское объединение НКО Operation Safe Escape и немецкая некоммерческая организация WEISSERRING.

Сталкерское ПО – это коммерческие программы для слежки, которые часто используются для скрытого наблюдения и вторжения в личную жизнь человека. В частности, такими программами могут пользоваться инициаторы домашнего насилия. С помощью сталкерских приложений можно получить доступ к личным данным жертвы: сообщениям, фотографиям, страничкам в соцсетях, данным геолокации, аудио- и видеозаписям (в том числе в режиме реального времени). Отличительной особенностью такого шпионского ПО является то, что для его установки и настройки необходим физический доступ к устройству жертвы. При этом такие программы работают в скрытом фоновом режиме, а жертва даже не подозревает об их присутствии.

На протяжении последних лет количество сталкерского ПО неуклонно растет, а вместе с тем увеличивается и число его жертв. По данным «Лаборатории Касперского», количество пользователей, столкнувшихся со сталкерским ПО за первые восемь месяцев 2019 г., выросло на 35% по сравнению с аналогичным периодом 2018 г. Более того, в текущем году компания обнаружила по меньшей мере 380 образцов сталкерского ПО – почти на треть больше, чем годом ранее.

До сих пор в индустрии кибербезопасности не было единого стандарта для определения и распознавания сталкерского ПО, что значительно затрудняло работу по борьбе с этой угрозой. Вот почему члены Coalition Against Stalkerware решили начать свою деятельность с разработки четкого определения и согласования критериев распознавания сталкерского ПО.

Также Coalition Against Stalkerware в ближайшее время запустит сайт. Его цель – помогать жертвам сталкерского ПО, просвещать пользователей об опасностях подобных программ, способствовать распространению знания о проблеме и обмену информацией между членами коалиции, а также формировать практики этичной разработки ПО.

На этом портале пользователи смогут найти информацию о том, на что способны программы для слежки, и о том, как защитить себя. На сайте будет приведен список индикаторов, сверившись с которым пользователь сможет выяснить, насколько велика вероятность установки на его устройство сталкерского приложения. Также портал предложит рекомендации относительно того, как себя вести в случае обнаружения факта слежки за собой. К примеру, прежде чем удалять сталкерскую программу, эксперты советуют подумать, не создаст ли этот шаг еще большую опасность, поскольку преследователь будет оповещен об удалении ПО через свое собственное приложение.

«Как показывают исследования, 70% женщин, становившихся жертвами сталкерского ПО, подвергались физическому или сексуальному насилию со стороны своих партнеров. Мы должны помешать нарушителям следить за своими близкими людьми через телефоны и привлечь их к ответственности. Coalition Against Stalkerware позволяет нам поделиться своими знаниями о гендерном насилии с ИТ-компаниями, и мы сможем вместе работать над тем, чтобы с помощью новых технологий положить конец насилию в отношении женщин», – отметила Анна МакКензи (Anna McKenzie), менеджер по коммуникациям в European Network forthe Work with Perpetrators of Domestic Violence.

Учитывая глобальную социальную значимость проблемы, связанной со сталкерским ПО, а также принимая во внимание то обстоятельство, что новые образцы подобных программ для слежки появляются на регулярной основе, Coalition Against Stalkerware открыта для новых партнерств и призывает различные организации к сотрудничеству.» ***(Создана коалиция по борьбе со сталкерским ПО // Компьютерное Обозрение (https://ko.com.ua/sozdana_koaliciya_po_borbe_so_stalkerskim_po_130954). 20.11.2019).***

***

Кіберзлочинність та кібертерроризм

«…У день запуску, 12 листопада, стрімінговий сервіс Disney+ дав збій, що тривав протягом багатьох годин…

Як виявилося, причиною падіння сервісу Disney+ стала атака хакерів, які зламали тисячі облікових записів користувачів…

Зараз багато з цих облікових записів пропонуються безкоштовно на хакерських форумах. Журналісти також помітили, що деякі акаунти також продаються за цінами від $3 до $11…

Після запуску стримінгового сервісу у соцмережах і на сайтах, які відслідковують активність ресурсів, з'явилися численні скарги на роботу нового сервісу. Користувачі повідомили, що не можуть дивитися фільми і шоу. Також вони скаржилися на втрату доступу до своїх облікових записів. За даними видання, багато користувачів помічали зміну електронних адрес на облікових записах.

Але навіть попри серйозний збій в роботі сервісу у день запуску, за два дні після запуску стрімінговий сервіс Disney+ залучив 10 млн підписників…» ***(Збій у Disney+ стався через хакерів, які атакували акаунти користувачів // MediaSapiens (https://ms.detector.media/web/cybersecurity/zbiy_u_disney_stavsya_cherez_khakeriv_yaki_atakuvali_akaunti_koristuvachiv/). 18.11.2019).***

***

«Иранский облачный провайдер Arvan Cloud столкнулся с DDoS-атакой, построенной на базе прокси-серверов Telegram. Эксперты предупреждают, что новый метод можно использовать для затруднения работы любых сайтов и веб-сервисов.

Проблемы начались утром 6 ноября и продолжались в течение нескольких дней. Пиковая мощность составила около 5000 запросов в секунду, что не создает серьезных трудностей для крупной телекоммуникационной компании, но может вызвать сбои у отдельных интернет-ресурсов…

Специалисты компании сразу отметили необычность DDoS-атаки. Злоумышленники использовали протокол передачи данных, работающий на канальном уровне (Layer 2), — в большинстве случаев для таких кампаний используются Layer 3/4 и 7. Целью атаки были пограничные серверы Arvan Cloud.

Специалисты установили источник вредоносного трафика простым угадыванием. К правильному ответу их подтолкнула популярность в Иране MTProxy-серверов, которые помогают местным пользователям обходить государственную блокировку Telegram. Эти системы шифруют трафик, затрудняя его фильтрацию. Об эффективности подобных мер говорит тот факт, что Иран быстро достиг первого места по аудитории Telegram, а данные, которыми обмениваются местные пользователи мессенджера, занимают 60% во всем сетевом трафике этого государства.

В то же время, говорят специалисты Arvan Cloud, MTProxy-серверы легко можно использовать для проведения DDoS-атак. Эксперты подтвердили это на практике, смоделировав атаку: в ходе эксперимента им удалось создать такой же трафик, как до этого они наблюдали в своей инфраструктуре.

По словам Arvan Cloud, этот прецедент особенно опасен в иранских условиях, поскольку теперь администраторы MTProxy-серверов смогут использовать свои системы в зловредных целях…» ***(Maxim Zaitsev. DDoS-атака в Иране велась через прокси-серверы Telegram // Threatpost (https://threatpost.ru/ddos-attack-against-arvan-cloud-found-using-mtproxy-servers/34830/). 14.11.2019).***

***

«Хостинг-провайдера SmarterASP.NET атаковал шифровальщик. В результате инцидента пострадали как данные клиентов сервиса, так и собственные веб-ресурсы компании. Во вторник представители провайдера опубликовали сообщение, что основная часть файлов восстановлена, однако некоторые серверы работают нестабильно.

Информация о неполадках на стороне SmarterASP.NET появилась 9 ноября этого года. Пользователи сервиса жаловались на недоступность своих ресурсов и отсутствие писем от техподдержки сервиса. Тогда же в Twitter появились скриншоты, из которых очевидно, что файлы зашифрованы и получили расширение .kjhbx. Издание ZDNet предполагает, что хостинг-провайдер заразился зловредом Snatch.

Веб-сайт компании SmarterASP.NET тоже на какое-то время оказался офлайн, что означает, что данные провайдера тоже были закодированы. Позднее работоспособность интернет-портала была восстановлена, и на нем появилось следующее сообщение:

«Ваш аккаунт подвергся атаке, и злоумышленники зашифровали все ваши данные. В настоящий момент мы совместно с ИБ-специалистами пытаемся восстановить информацию, а также исключить возможность повторного нападения. Оставайтесь на связи для получения дополнительной информации».

Специалисты SmarterASP.NET устраняют последствия атаки шифровальщика

Утром 11 ноября представители SmarterASP.NET заявили, что работоспособность 90% аккаунтов восстановлена. Во вторник 12 ноября на странице компании в Facebook появилась информация, что расшифрованы все данные, но некоторые серверы работают нестабильно. Провайдер не сообщает, заплатил ли он выкуп или же использовал резервные копии. По некоторым данным,

киберпреступники, стоящие за Snatch, требуют у жертвы выкуп в размере от $500 до $1500 в биткойнах.

SmarterASP.NET предоставляет клиентам специализированный хостинг на базе фреймворка ASP.NET, разработанного Microsoft. На серверах провайдера не только размещались веб-ресурсы его подписчиков, но и хранились резервные копии важных данных. По данным с официального сайта компании, ее услугами пользуются более 440 тыс. клиентов…» ***(Julia Glazova. Шифровальщик атаковал хостинг-провайдера SmarterASP.NET // Threatpost (https://threatpost.ru/smarterasp-net-attacked-by-ransomware/34806/). 13.11.2019).***

***

«По оценке «Лаборатории Касперского», в июле и августе на DDoS-фронте наблюдалось относительное затишье. Активность злоумышленников, как и год назад, заметно повысилась лишь в сентябре. На этот месяц пришлось больше половины атак, зафиксированных в течение квартала, притом в 60% случаев мишенями дидосеров являлись онлайн-ресурсы образовательных учреждений.

Подобные DDoS-атаки, по словам исследователей, обычно коротки и плохо подготовлены — судя по всему, их проводят из хулиганских побуждений школьники, вернувшиеся с каникул. В топ стран, где были замечены инциденты в сфере образования, попала и Россия.

Общее количество DDoS-атак, зафиксированных экспертами, за квартал увеличилось почти на треть — за счет сентября, а их средняя продолжительность упала на 39 процентных пунктов. Подавляющее большинство зафиксированных инцидентов (84,42%) были кратковременными, менее четырех часов. Самая затяжная атака длилась более 11 суток (279 часов) — этот максимум почти в два раза меньше рекордного показателя II квартала…» ***(Maxim Zaitsev. Статистику Kaspersky по DDoS-атакам подправили школьники // Threatpost (https://threatpost.ru/kaspersky-ddos-activity-report-3q2019/34799/). 12.11.2019).***

***

«Бренд Microsoft оказался безусловным фаворитом у организаторов фишинговых кампаний. Как рассказали эксперты Akamai, по количеству поддельных страниц американский IT-гигант в разы обгоняет Paypal, DropBox и DHL, которые также заняли верхние строчки рейтинга.

Такие данные содержатся в очередном исследовании State of the Internet, которое посвящено фишинговым технологиям. Авторы вывели на первый план значение фишинг-паков — готовых к работе решений, которые позволяют разворачивать вредоносные страницы и красть пользовательские данные…

Содержание подобных пакетов варьируется от простых HTML-форм до многофункциональных продуктов, способных скрываться от защитных систем и атаковать цели по точным настройкам таргетинга. Фишинг-паки можно взять в аренду — злоумышленники разворачивают полноценные интернет-сервисы с возможностью анализировать и настраивать кампании, отслеживать обновления ПО.

За неполные девять месяцев исследования эксперты обнаружили тысячи вредоносных доменов, на которых использовались десятки различных наборов. Чаще всего преступники оформляют посадочные страницы под сайты Microsoft — специалисты увидели этот бренд в 62 пакетах, развернутых на 3,9 тыс. сайтов. На втором месте по популярности оказался сервис PayPal (14 фишинг-паков, 1,7 сайтов). Далее идут социальная сеть LinkedIn (6 пакетов, 1,6 тыс. доменов) и система цифровых подписей DocuSign (4 пакета, 400 доменов)…

По словам аналитиков, у злоумышленников есть два пути — они могут выкладывать фишинг-паки на собственных площадках или встраивать их в чужие веб-ресурсы.

Второй вариант помогает преступникам дольше избегать блокировки. Аналитические системы постоянно отслеживают и блокируют домены, на которые поступают жалобы о нежелательной активности, причем новые площадки привлекают особое внимание. Прикрываясь чужим сайтом, фишеры получают некоторый запас времени за счет его положительной репутации.

Однако чтобы взломать интернет-ресурс, преступникам нужно найти уязвимость в его CMS или веб-сервере, а это может быть непросто. Поэтому чаще фишеры предпочитают вести кампании на множестве собственных доменов, которые они закупают в оптовых масштабах. Исследователи подсчитали, что около 90% таких адресов оказываются заблокированы в первые сутки. Преступникам хватает этого времени, чтобы окупить затраты на создание сайта и даже выйти в плюс. Еще 5% ресурсов прекращают работу в течение трех дней.

Чтобы продлить жизнь вредоносной страницы, их создатели проверяют, не связаны ли сетевые данные очередной жертвы с ИБ-компаниями или крупными интернет-организациями вроде Amazon и Google. Многие вредоносные пакеты автоматически генерируют URL и прочие данные, затрудняя блокировку по черным спискам…

Как указали исследователи, угрозы фишинговых кампаний не ограничиваются компрометацией частной и корпоративной информации. Зачастую такая атака оказывается лишь первым звеном в цепочке вредоносных действий, а преступники стремятся не просто перепродать украденные данные, а установить долгосрочную слежку за жертвой.

Так, почти 80% случаев кибершпионажа так или иначе связаны с фишинговой активностью. Авторитарные государства используют эти методы, чтобы заразить устройства диссидентов, недобросовестные компании пытаются узнать секреты конкурентов. В других сценариях фишинговый инцидент помогает взломщикам собрать данные об инфраструктуре целевой организации, получить доступ к ее партнерам и контрагентам, подготовить почву для атаки шифровальщика.

Менее очевидные угрозы связаны с особенностями разработки фишинг-паков. Как рассказали исследователи, создатели такого ПО не гнушаются плагиатом — в продуктах встречаются идентичные участки кода. Таким образом ошибки и баги оригинального фишинг-пака распространяются на его копии. Если такой пакет попадает на легитимный веб-ресурс, пораженная площадка становится уязвимой перед другими атаками.

Эксперты подчеркивают, что в нынешних условиях для защиты от фишинга уже недостаточно обучения пользователей. Преступники учитывают растущую цифровую грамотность жертв и постоянно развивают методы атак. Чтобы не пострадать от их действий, компаниям следует использовать специализированные защитные решения, которые автоматически блокируют подозрительную активность внутри инфраструктуры…» ***(Egor Nashilov. Akamai: 90% фишинговых сайтов остаются онлайн менее суток // Threatpost (https://threatpost.ru/akamai-on-phishing-in-soti-report/34704/). 02.11.2019).***

***

«Ежегодные убытки компаний от кибератак в глобальном масштабе к 2021 году будут превышать 6 трлн долларов, прогнозирует старший аналитик исследовательского агентства Wikibon Дэйв Велланте, - передает DailyComm. По его словам, эти убытки, в частности, включают расходы на восстановление компьютерных систем, пострадавших от взлома, а также потери от снижения производительности труда.

Эксперт говорит, что активность хакеров увеличивается по мере роста количества устройств, которые используются в компаниях и которые нуждаются в защите. Хотя бизнес все чаще хранит огромные объемы данных в нескольких публичных и частных облаках, количество эксплуатируемых смартфонов и подключенных периферийных устройств продолжает расти, создавая новые возможности для кибератак…

Теперь информационная безопасность стала более фрагментированной как никогда: появились сотни продуктов и огромное количество стартапов, которых становится все больше. Среднестатистическая компания из списка крупнейших Fortune 500 использует до 72 ИБ-продуктов для защиты своих данных и ИТ-систем. Но далеко не все эти решения справляются со своими функциями.

Одна из вероятных причин роста киберпреступности Дэйв Велланте считает, что поставщики сервисов для запуска облачной инфраструктуры, включая Amazon Web Services, используют так называемую «модель безопасности с общей ответственностью», которую понимают не все клиенты. В случае с AWS эта модель обеспечивает безопасность его S3 и инфраструктуры EC2, при этом клиент берет на себя ответственность за применение политик и настройку систем для предотвращения несанкционированного доступа через устройства.

Люди думают, что, если их данные находится в популярном облаке, то они защищены лучше, чем если бы компании самостоятельно обеспечивали безопасность. Но это не всегда так, предупреждает аналитик.

Аналитики IDC ожидают, что мировые продажи оборудования, программного обеспечения и сервисов, которые предназначены для киберзащиты, в 2019 году достигнут 106,6 млрд долларов, увеличившись на 10,7% относительно 2018-го. В ближайшие пять лет объем рынка будет увеличиваться на 9,4% ежегодно и составит 151,2 млрд долларов в 2023 году.» ***(Из-за кибератак в 2019 году мировой бизнес потерял 6 триллионов долларов (это – 12 нулей) // SecureNews (https://securenews.ru/mnogo-mnogo-poter/). 12.11.2019).***

***

«Исследователи из компании EfficientIP провели опрос среди 1000 ведущих IT-фирм из Северной Америки, Европы и Азиатско-Тихоокеанского региона и выяснили, что мировые правительства ежегодно теряют в среднем около $7 млн из-за DNS-атак. Такие выводы содержатся в отчете IDC 2019 Global DNS Threat Report.

Как показали результаты опроса, государственные организации по всему миру становятся жертвами в среднем 12 DNS-атак в год, каждая из которых обходится в полмиллиона долларов или $6,7 млн в общем. Большая часть финансовых убытков связана с перебоями в работе и кражей данных.

Больше половины респондентов (51%) сообщили о том, что за последние 12 месяцев неоднократно сталкивались с недоступностью собственных приложений в результате DNS-атак, а 43% отметили перебои в работе облачных сервисов. 41% опрошенных пострадали от взломанных web-сайтов, что также ставило под угрозу безопасность данных. 19% опрошенных сообщили о краже конфиденциальной информации или IP-адресов через DNS.

51% респондентов были вынуждены отключить серверы для противодействия атакам, что указывает на низкий уровень реагирования на инциденты и готовности к ним. По словам 32% респондентов из правительственных организаций, уровень безопасности их DNS-систем является низким или средним.» ***(Правительственные организации ежегодно теряют миллионы долларов из-за DNS-атак // SecurityLab.ru (https://www.securitylab.ru/news/502716.php). 20.11.2019).***

***

«Один из крупнейших производителей спортивной атрибутики Boardriders подвергся кибертаке с использованием вредоносного ПО, затронувшей также некоторые из его дочерних компаний — QuikSilver и Billabong. Атака вынудила компанию отключить свои компьютерные системы по всему миру.

После атаки в интернет-магазинах компании появились сообщения, предлагающие клиентам скидку в 20% и сообщающие о том, что Boardriders испытывает задержки с доставкой.

«Наши IT-команды работают над быстрым восстановлением наших систем для поддержки наших операций, которые в настоящее время в основном осуществляются и доставляются в обычном режиме», — сообщила Boardriders порталу ShopEatSurf.

На данный момент нет информации, о каком именно вымогательском ПО идет речь и требуемой сумме выкупа.

Помимо Boardriders, в минувшие выходные кибератаке с использованием вымогательского ПО подвергся крупный хостинг-провайдер SmarterASP.NET, число клиентов которого превышает более 440 тыс. Неизвестно, заплатила ли компания выкуп вымогателям или восстановила системы из резервных копий.

Атака затронула не только данные клиентов, но и системы SmarterASP.NET. Web-сайт компании был недоступен целые сутки и возобновил свою работу лишь на следующий день после нападения. Поскольку работа над восстановлением

сервера проходит медленно, многие клиенты по-прежнему не имеют доступа к своим учетным записям и данным.

Согласно сообщениям в Twitter, все файлы клиентов были зашифрованы с помощью программы-вымогателя, добавляющей расширение «.kjhbx» к каждому файлу.» ***(Спортивная компания Boardriders пострадала от вымогательского ПО // SecurityLab.ru (https://www.securitylab.ru/news/502418.php). 11.11.2019).***

***

«Исследователи безопасности предупредили Индийскую организацию космических исследований (ISRO) о кибератаке предположительно северокорейских преступников, которая является частью широкомасштабной вредоносной кампании. Предупреждение поступило в период проведения лунной миссии «Чандраян-2», сообщает Financial Times со ссылкой на знакомые с ситуацией источники.

По словам исследователя Яша Кадакии, ISRO оказалась в числе критически важных правительственных учреждений, на которые нацелились преступники в последние месяцы. По данным FT, атаки осуществлялись с помощью фишинговых электронных писем, содержащих вредоносное ПО. По словам представителей ISRO, компания получила предупреждение о кибератаке, но в ходе расследования не обнаружила ничего подозрительного.

«Наши системы не были скомпрометированы и не пострадали. Лунная миссия не была скомпрометирована атакой, поскольку у нас есть внутренняя сеть, на 100% изолированная от интернета», — сообщил представитель ISRO…» ***(Северокорейские киберпреступники нацелились на индийское космическое агентство // SecurityLab.ru (https://www.securitylab.ru/news/502380.php). 07.11.2019).***

***

«Две крупные испанские компании, в частности, радиосеть Cadena SER и IT-фирма Everis, стали жертвами целенаправленной атаки с использованием вымогательского ПО.

Как сообщает испанская ежедневная газета ABC, атаки начались утром 4 ноября. Предположительно, вымогательское ПО, заразившее системы Everis, является версией BitPaymer , которая все чаще используется злоумышленниками для блокировки взломанных систем в сети. Злоумышленники потребовали от Everis выкуп в размере 750 тыс. евро за ключ для расшифровки файлов.

Пока неизвестно, какой именно вредонос применялся в ходе атаки на Cadena SER, но исследователи из Национального института кибербезопасности (Instituto Nacional de Ciberseguridad, INCIBE) Испании в настоящее время помогают восстанавливать зашифрованные данные и возобновить работу систем.

Департамент национальной безопасности Испании подтвердил факт кибератаки на Cadena SER, заявив, что «целью преступников было шифрование файлов, которое оказало широкое влияние на все компьютерные системы компании».

В качестве меры предосторожности обе пострадавшие компании отключили свои компьютеры и сети от интернета.» ***(Две крупные испанские компании***

атакованы вымогательским ПО // SecurityLab.ru (https://www.securitylab.ru/news/502294.php). 05.11.2019).

***

«Крупнейший в США независимый поставщик солнечной и ветровой энергии компания sPower стала жертвой кибератаки. Данный инцидент является первым случаем, когда оператор электросетей в США потерял связь с установками по производству электроэнергии в результате вмешательства киберпреступников, сообщает издание E&E News.

Атака была обнаружена еще в апреле нынешнего года, однако только сейчас стало известно название компании, которая подверглась атаке, а также другие подробности.

5 марта нынешнего года неизвестный злоумышленник проэксплуатировал уязвимость в межсетевом экране от Cisco, вызвав сбой в работе устройства и разорвав связь ветровых и солнечных электростанций sPower с главным командным центром компании. Как сообщается, данная атака не была целенаправленной — злоумышленник не продолжил атаку, а также не проник в сеть sPower.

«Принимая во внимание отсутствие определенных последующих действий со стороны злоумышленника, может показаться, что кто-то тестирует или сканирует уязвимость и непреднамеренно затрагивает инфраструктуру коммунальных услуг в ходе атаки», — предположил исследователь безопасности из компании Dragos Джо Словик (Joe Slowik).

Компания sPower исправила данную уязвимость, установив соответствующее обновление прошивки межсетевого экрана.» ***(Киберпреступники атаковали поставщика ветровой и солнечной энергии в США // SecurityLab.ru (https://www.securitylab.ru/news/502246.php). 01.11.2019).***

***

«Эксперты по кибербезопасности бьют тревогу. В 2019 году число кибератак на интернет вещей (IoT) выросло на 300%...

Согласно новому отчету компании F-Secure, общее число атак в 2019 году превысило 2,9 млрд. случаев. Для подсчета компания использует серверы-приманки, называемые “Honeypots” (“горшочек с мёдом”). Приманки замаскированы таким образом, чтобы в сети выглядеть как обычные IoT-устройства. Этот камуфляж привлекает так называемые “повседневные атаки” - те, от которых могут страдать обычные пользователи. 2019 год стал первым, когда число таких атак перевалило за миллиард. Прежде они исчислялись миллионами.

Эксперты считают, что рост атак на интернет вещей связан с увеличением числа IoT-устройств. Проще говоря, у злоумышленников появилось больше слабозащищенных целей.

О проблемах с безопасностью интернета вещей специалисты кричат уже не один год. Некоторые IoT-устройства имеют старые прошивки или устаревшую архитектуру. Для многих простых устройств вообще никогда не выпускались патчи безопасности. Ситуацию ухудшает то, что IT-отделы крупных компаний могут даже не подозревать об уязвимых девайсах в их сети. Защитить то, о чем ты не

знаешь, невозможно. Злоумышленники же будут использовать взломанное устройство как точку проникновения во внутреннюю сеть. Таким образом, один единственный уязвимый принтер может скомпрометировать безопасность огромной компании…» ***(Число кибератак на интернет вещей выросло на 300%. Рассказываем, как защитить себя // IGate (https://igate.com.ua/news/24106-chislo-kiberatak-na-internet-veshhej-vyroslo-na-300.-rasskazyvaem-kak-zashhitit-sebya). 21.11.2019).***

***

«Кибератаки не только наносят ущерб компьютерным системам больниц, но и приводят к серьезному нарушению процесса оказания медицинской помощи

Об этом идет речь в исследовании Школы менеджмента Университета им. Оуэна Вандербильта, передает "ДС" со ссылкой на KrebsOnSecurity.

В частности, в результате кибератак, которые приводят к задержкам с передачей данных, на 10 тыс. случаев сердечных приступов ежегодно приходится до 36 смертей, вызванных перебоями в работе сетей.

Согласно исследованию, которое базируется на данных из британских больниц, по меньшей мере 10% более чем 3 тыс. сертифицированных больниц, пострадали от кибератак.

"Усилия по устранению нарушений были связаны с ухудшением своевременности оказания медицинской помощи и результатов лечения пациентов", - обнаружили авторы.

"Действия по исправлению могут вносить изменения, которые задерживают, усложняют или нарушают процессы здравоохранения и обслуживания пациентов"…» ***(Кибератаки приводят к смерти от сердечного приступа, - исследование // DsNews (http://www.dsnews.ua/world/kiberataki-privodyat-k-smerti-ot-serdechnogo-pristupa---issledovanie-18112019215900). 18.11.2019).***

***

«Компания Positive Technologies обнародовала развёрнутый отчёт «Актуальные киберугрозы: III квартал 2019 года», в котором подробно рассматривается ситуация с безопасностью во Всемирной сети.

Эксперты фиксируют дальнейший рост числа целенаправленных атак (APT): теперь на них приходится две трети (65 %) от общего количества кибернападений. Для сравнения: во второй четверти текущего года данный показатель равнялся 59 %.

«Организации по всему миру находятся под угрозой сложных целенаправленных атак. Наибольший интерес для злоумышленников представляют государственные учреждения, промышленные компании, финансовый сектор и организации сферы науки и образования», — отмечается в отчёте.

Ещё одна тенденция минувшего квартала — рост количества кибератак, направленных на кражу информации. Их доля в сегменте юридических лиц в течение трёх месяцев поднялась с 58 % до 61 %. В сегменте частных пользователей рост оказался более существенным — с 55 % до 64 %.

Доля финансово мотивированных атак для юридических и частных лиц сравнялась и составила 31 %. Такие нападения в сегменте юридических лиц преимущественно связаны с заражениями троянами-шифровальщиками, требующими выкуп за восстановление зашифрованных данных. В атаках на частных лиц киберпреступники ищут финансовую выгоду, распространяя навязчивую рекламу и мобильные приложения, подписывающие на платные услуги.

В то же время специалисты Positive Technologies отметили снижение доли атак с применением майнеров криптовалюты — до 3 % в случае организаций и до 2 % в случае частных лиц.

Говорится также, что три четверти атак в корпоративном сегменте и 62 % атак среди обычных пользователей сопровождались заражениями различного рода зловредами.» ***(Две трети кибератак носят целенаправленный характер // Український телекомунікаційний портал (https://portaltele.com.ua/news/internet/dve-treti-kiberatak-nosyat-tselenapravlennyj-harakter.html). 22.11.2019).***

***

Діяльність хакерів та хакерські угруповування

«Эксперты Positive Technologies проанализировали деятельность APT-группировок, атакующих российские организации на протяжении последних двух лет. Девять из них фокусируются на организациях топливно-энергетического комплекса (ТЭК), а 13 объединений злоумышленников видят целью промышленные компании. Некоторые группировки атаковали и промышленные, и энергетические компании.

В двух новых исследованиях специалисты Positive Technologies описали специфику APT-атак на промышленные компании и организации ТЭК. Помимо этого, эксперты провели опрос среди посетителей сайта компании Positive Technologies, аудитории интернет-портала SecurityLab.ru и участников ряда отраслевых сообществ.

По данным этого опроса, более половины (60%) респондентов из сферы промышленности и топливно-энергетического комплекса признают, что вероятность успешной кибератаки достаточно высока. При этом лишь 11% участников опроса уверены в том, что их предприятие сможет противостоять APT-атаке.

Большинство представителей организаций считают, что основной целью APT-группировки при атаке на их компании будет являться нарушение технологических процессов и вывод из строя инфраструктуры. При этом 55% участников опроса сообщили, что их организации уже становились жертвами атак. Каждый четвертый участник отметил, что одним из итогов такой атаки стал простой инфраструктуры.

При этом во многих компаниях используются лишь базовые средства защиты, которые практически бесполезны для противодействия таким сложным

угрозам, как APT. Так, лишь 5% респондентов, работающих в промышленных и топливно-энергетических компаниях, сообщили, что в их организациях используются специализированные инструменты борьбы с целевыми атаками.

На практике типовые защитные решения оказываются неэффективными для противодействия APT-атакам. Кибергруппировки запутывают код своего вредоносного ПО, чтобы антивирусные решения на компьютерах сотрудников не могли распознать угрозу в момент атаки. Пять из девяти группировок, нацеленных на ТЭК, используют вредоносное ПО, выполняющееся сразу в оперативной памяти и не оставляющее следов на жестком диске. Киберпреступники добавляют в зловред специальные модули для определения версии используемого в системе антивируса, а также модули для обнаружения выполнения в «песочнице» и виртуальной среде, что позволяет обойти динамические проверки систем защиты в момент атаки.

Большинство APT-группировок шифруют канал связи с командными серверами, чтобы скрыть вредоносный трафик и обмануть системы обнаружения вторжений. При атаках на промышленные компании каждая вторая группа (46%) с этой целью использует известные алгоритмы шифрования, а 38% — их модифицированные версии. Вредоносный трафик часто маскируется под легитимный: при атаках на промышленный сектор 77% APT-группировок обмениваются информацией с командным центром по широко распространенным протоколам. Отдельные группировки, нацеленные на сектор ТЭК, размещают командные серверы по адресам, которые схожи с названиями известных в отрасли компаний.

Злоумышленников не останавливает даже полная изоляция технологического сегмента сети от ее корпоративного сегмента и интернета. Если их цель находится в промышленном сегменте, то в компанию могут быть подброшены съемные носители (например, флешки) с вредоносным ПО, или их может подключить к USB-разъемам критически важных систем внедрившийся в компанию инсайдер (техника Replication Through Removable Media).

По словам директора экспертного центра безопасности Positive Technologies (PT Expert Security Center) Алексея Новикова, зачастую более эффективным подходом к обнаружению APT является выявление активности злоумышленников уже после проникновения в инфраструктуру: «Выявить APT-атаку в момент проникновения нарушителя в компанию — крайне сложная задача, но если цель злоумышленника — надежно закрепиться в инфраструктуре и контролировать ключевые системы максимально длительное время, то обнаружить его можно и на более поздних этапах атаки, например при его перемещении между серверами уже во внутренней сети. Такие перемещения непременно оставляют артефакты в сетевом трафике и на самих узлах, это позволяет обнаружить произошедшее ранее проникновение ретроспективно и устранить угрозу до того, как злоумышленник перейдет к активным деструктивным действиям или украдет важную информацию». ***(Эксперты Positive Technologies рассказали об особенностях APT-атак в промышленности и ТЭК // Positive Technologies (https://www.ptsecurity.com/ru-ru/about/news/eksperty-positive-technologies-rasskazali-ob-osobennostyah-apt-atak-v-promyshlennosti-i-tek/). 18.11.2019).***

***

«Система муниципальных школ штата Нью-Мексико отключила все компьютерные системы в связи с хакерской атакой. Пострадало более 1000 американских учреждений образования…

ИТ-отдел муниципалитета обнаружил, что некоторые серверы были взломаны и скоро отреагировали, отключив компьютерную сеть района. Связь со школами осуществляется через мобильную связь и портативные радиостанции. Не смотря на то, что инцидент серьезный, школы работают в штатном режиме.

«В настоящее время мы не считаем, что данные сотрудников или учащихся школ были скомпрометированы», - заявили представители округа в Las Cruces Sun News. В том же сообщении говорится, что Университет штата Нью-Мексико предупредил своих сотрудников, чтобы они не открывали электронные письма от государственных школ Лас-Крусес (LCPS), поскольку они могут содержать вредоносное ПО.

Были введены дополнительные меры предосторожности, типа блокировки прямого доступа к сети через LCPS и входящий трафик, пока ситуация не прояснится.

Причина, по которой эти цифры тревожно высоки (более 1000), заключается в том, что киберпреступники осознавали, что атака на государственный сектор имеет больший шанс на успех, поскольку школы недостаточно подготовлены к кибератакам и вынуждены продолжать свою деятельность для предоставления государственных услуг.» ***(Крупная кибератака обрушилась на школы Нью-Мексико // SecureNews (https://securenews.ru/kiberataka-na-scholi/). 01.11.2019).***

***

«Спонсируемая иранским правительством киберпреступная группировка APT33, также известная как Elfin, MAGNALLIUM или Refined Kitten, создала собственную частную VPN-сеть для подключения к своим C&C-серверам, проведения разведки в сетях будущих целей и просмотра web-страниц. Как сообщают исследователи из компании Trend Micro, группировка APT33 на сегодняшний день является самым технически продвинутым киберпреступным подразделением Ирана.

Группировка считается разработчиком вредоносного ПО для удаления данных с жестких дисков, известного как Shamoon (DistTrack), которое вывело из строя более 35 тыс. рабочих станций компании Saudi Aramco в Саудовской Аравии в 2012 году.

По словам исследователей, инфраструктура группировки является многослойной и изолированной, позволяя APT33 избегать обнаружения. Эксперты выделили четыре уровня инфраструктуры группировки. Уровень VPN представляет собой специально построенную сеть VPN-узлов для маскировки реального IP-адреса и местоположения оператора. Уровень Bot Controller является промежуточным. Уровень C&C Backend — фактические внутренние серверы, через которые группа управляет своими вредоносными ботнетами. Уровень прокси является набором облачных прокси-серверов, маскирующих C&C-серверы от зараженных хостов.

«Частную VPN-сеть можно легко настроить, арендовав пару серверов у центров обработки данных по всему миру и используя программное обеспечение с открытым исходным кодом, такое как OpenVPN», — отмечают исследователи.

Однако на самом деле собственная VPN-сеть, наоборот, облегчает ее отслеживание. Поскольку APT33 использует исключительно свои выходные узлы VPN, специалистам удалось в течение года отслеживать некоторые узлы ...

Помимо подключения к управляющему C&C-серверу, группа использовала VPN-сеть «для разведки в сетях, имеющих отношение к цепочке поставок нефтяной промышленности», а также для доступа к web-сайтам компаний, занимающихся проведением тестирования на проникновение, почтовым сервисам, сайтам, связанными с уязвимостями, и подпольным ресурсам, посвященным криптовалюте. Кроме того, группировка интересовалась сайтами, специализирующимся на подборе сотрудников в нефтегазовой отрасли.» ***(Иранская группировка APT33 создала собственную VPN-сеть // SecurityLab.ru (https://www.securitylab.ru/news/502572.php). 14.11.2019).***

***

«Министерство обороны США обвинило киберпреступников, работающих на правительство Северной Кореи, в кибератаках на финансовый сектор, в том числе на сеть SWIFT, с целью обогащения.

Киберкомандование США (CYBERCOM) опубликовало на VirusTotal семь новых образцов вредоносного ПО, используемых в ходе текущей вредоносной кибероперации против финансового сектора. «В настоящее время эти образцы вредоносного ПО используются для генерирования денежных средств и вредоносной активности, в том числе для удаленного доступа, сигнализации и выполнения вредоносных команд», - сообщает CYBERCOM.

Кто стал жертвами вредоносной кампании, и каковы ее масштабы, CYBERCOM не уточняет.

Со своей стороны ФБР также выявило вредоносное ПО и связало его с Северной Кореей. Бюро выпустило уведомление (есть в распоряжении журналистов SyberScoop) с описанием индикаторов компрометации (IOC), совпадающими с IOC прошлых кампаний северокорейских хакеров и ранее проанализированными южнокорейской ИБ-компанией Alyac.

В уведомлении ФБР представлена информация о троянах для удаленного доступа (RAT), инструментах командной строки и web-оболочках, позволяющих получать удаленный доступ к компьютерам жертв, загружать и выгружать файлы и выполнять произвольный код. Связаны ли уведомления CYBERCOM и ФБР между собой, пока неизвестно.

По словам специалиста компании Symantec Викрама Такура (Vikram Thakur), загруженные CYBERCOM вредоносные образцы являются «созданными под заказ, сложными и хорошо написанными». Среди образцов есть билдеры бэкдоров, загрузчики бэкдоров и собственно сами бэкдоры.

Некоторые RAT могут включать микрофон на зараженном устройстве и записывать звук. Бэкдоры позволяют похищать учетные данные, перехватывать нажатия клавиш на клавиатуре, просматривать историю браузера, загружать

дополнительные вредоносные модули и управлять обратной web-оболочкой для установки связи между зараженным компьютером и сервером злоумышленников.

Некоторые бэкдоры имеют сходство с вредоносными ПО, используемым северокорейскими правительственными хакерами в течение уже многих лет. К примеру, один из образцов является вариантом бэкдора CHEESETRAY, ранее использовавшегося северокорейцами в атаках на сеть SWIFT. Ряд образцов имеют схожие черты с бэкдором ROCKEYE, чей код был позаимствован у ROGUEEYE, использовавшегося киберпреступниками в кибератаках с целью получения финансовой выгоды.» ***(США обвинили Северную Корею в кибергрблениях // SecurityLab.ru (https://www.securitylab.ru/news/502465.php). 12.11.2019).***

***

«Хакеры могут зарабывать на продаже уязвимостей столько же, сколько ИБ-эксперты, принимающие участие в программах вознаграждения за найденные уязвимости, или так называемые «серые шляпы», занимающиеся реверс-инжинирингом для правительства. Так считает глава исследовательского отдела компании Tenable Оливер Рочфорд (Oliver Rochford). По его словам, исследование уязвимостей — дорогостоящий процесс, и «белый», «черный» и «серый» рынки используют одинаковые методы при поиске уязвимостей, несмотря на легальную или нелегальную специфику.

Основная разница между преступными и легальными сторонами заключается в наличии этики. Механизм (обнаружение уязвимостей, исследование эксплоитов и разработка) одинаков как для преступников, так и для исследователей, но разница заключается в том, как стороны используют уязвимости. Например, злоумышленники действуют с целью шпионажа, саботажа и мошенничества, в то время как ИБ-специалисты проводят анализ существующих угроз.

По словам Рочфорда, в некоторых случаях возможно заработать намного больше легальным способом (в данной сфере хакеры могут заработать примерно $75 тыс.). По его данным, на подпольных рынках за уязвимость в Apache или Linux можно заработать около $1 млн, тогда как брокеры эксплоитов предлагают примерно $500 тыс. Уязвимости в WhatsApp для Android также могут принести $1 млн на «черном» и «сером» рынках. В рамках программ bug bounty наиболее прибыльными являются уязвимости, затрагивающие Safari в iOS, а в общем на багах в iOS можно заработать примерно $1 млн, на «сером» рынке — $2 млн.

По словам Рочфорда, у злоумышленников в среднем есть 7 дней на эксплуатацию уязвимости прежде, чем ИБ-эксперты начнут ее анализировать, именно поэтому «компаниям необходимо принимать меры по усилению безопасности».

Согласно недавнему отчету Bromium, доход от киберпреступности оценивается в $1,5 трлн, в то время как общий объем рынка кибербезопасности в 2019 году составил $136 млрд.» ***(Хакеры могут зарабывать на продаже уязвимостей столько же, сколько ИБ-эксперты на программах bug bounty // SecurityLab.ru (https://www.securitylab.ru/news/502461.php). 11.11.2019).***

***

«По оценке исследователей из Check Point, в настоящее время в состав ботнета Phorpiex входит более 1 млн зараженных Windows-компьютеров. Он используется в основном для кражи криптовалюты и скрытого майнинга. Противозаконная деятельность ежегодно приносит ботоводам около полумиллиона долларов.

Вредоносные боты обладают способностью к самораспространению, а также могут быть загружены с помощью эксплойт-пака (RIG) или другого зловреда (Smoke Loader).

Ботнет Phorpiex также известен ИБ-сообществу под другим именем — Trik. Вначале управление сетью осуществлялось через IRC-каналы, а когда она разрослась, операторы перешли на HTTP. В этом году наблюдатели из Check Point не обнаружили ни одного активного C&C-сервера, доступного по IRC, хотя резидентные боты Trik, заточенные под такую связь, до сих пор исчисляются тысячами.

Сменивший Trik модульный зловред, на основе которого функционирует современный Phorpiex, именуется Tldr. Его основным назначением является загрузка дополнительных файлов. Некоторые образцы этой вредоносной программы способны самостоятельно распространяться через сменные носители. Эксперты также обнаружили варианты Tldr, обладающие функциональностью файлового вируса.

Новый бот, как и его предшественник, также умеет работать с буфером обмена — распознавать адреса криптокошельков и осуществлять подмену в пользу своих хозяев. Благодаря этому операторы Phorpiex имеют возможность получать доход без дополнительных усилий и даже при отключенных центрах управления. По данным Check Point, за три года ботоводы украли таким образом более 17 биткойнов.

Для добычи цифровой валюты Tldr загружает на зараженную машину майнер XMRig. По подсчетам экспертов, криптоджекинг приносит ботоводам более $14 тыс. в месяц. Они также оказывают услуги по распространению вредоносных программ — шифровальщиков (GandCrab), похитителей информации (Raccoon, Predator). В настоящее время загрузка вымогательского ПО не производится; после закрытия RaaS-сервиса GandCrab операторы Phorpiex переключились на рассылку вымогательского спама, который за полгода принес им более 14 биткойнов.

Ежемесячный объем данных, которыми боты обмениваются с центрами управления, по оценке Check Point, может превышать 70 Тбайт. Это солидный трафик, и для сокрытия командной инфраструктуры ботоводы используют выделенные подсети, зарегистрированные на подставных лиц. Как оказалось, Tldr обращается к тем же C&C-серверам, которые ранее командовали IRC-ботами Trik. Их IP-адреса и имена доменов вшиты в код зловреда; этот список регулярно обновляется.

Боты постоянно проверяют активность центров управления, перебирая позиции списка, и продолжают опрос, даже получив положительный ответ. Исследователям удалось зарегистрировать ряд доменов после анализа образцов

Tldr с различными конфигурационными файлами. Подменив C&C-серверы, они ежедневно фиксировали до 100 тыс. активных ботов (IP-адресов) и за два месяца насчитали более 1 млн уникальных хостов, пытавшихся установить соединение. Эти очаги заражения были в основном расположены в Азии, с высокой концентрацией в Индии, Китае, Таиланде и Пакистане. Некоторое количество ботов проникло также в США, Мексику и ряд африканских стран. Европейская популяция Phorpiex оказалась ничтожной.

В целом мониторинг активности этого ботнета в 2019 году выявил более 4000 различных образцов Tldr, около 300 вариантов конфигурационного файла и 3297 доменов и IP-адресов C&C. Из последних в настоящее время наибольшую активность проявляет IP 185[.]176[.]27[.]132 в блоке /24, выделенном некоему поставщику транспортных услуг в Казани, с вводом трафика через Болгарию, а также подсеть 92[.]63[.]197[.]0/24, зарегистрированная на имя харьковского предпринимателя, торгующего в розницу продуктами питания, алкоголем и табачными изделиями. Примечательно, что харьковский блок адресов ассоциируется не только с Phorpiex, но и с рядом других угроз — Smoke Loader, Necurs, сканами портов, фишингом и спам-рассылками.» ***(Maxim Zaitsev. Ботнет Phorpiex: незамысловат, но плодовит // Threatpost (https://threatpost.ru/phorpiex-botnet-not-too-sophisticated-but-very-prolific/34872/). 20.11.2019).***

***

«ИБ-специалисты нашли adware-зловред для Android, выдающий себя при этом за блокировщик рекламы. От атак приложения FakeAdsBlock пострадали как минимум 500 пользователей, однако, по мнению исследователей, кампания только набирает обороты.

Вредоносная программа распространяется под названием Ads Blocker через неавторизованные Android-репозитории. В процессе установки приложение запрашивает ряд разрешений, нехарактерных для программ блокировки рекламы. Например, зловред требует права на открытие VPN-соединения, показ сообщений поверх других окон и создание виджета на рабочем столе. Получив необходимые привилегии, приложение демонстрирует пользователю служебное сообщение, удаляет свою иконку и переходит в фоновый режим…

В арсенале FakeAdsBlock несколько вариантов демонстрации рекламы. Зловред может открывать свои окна во весь экран, запускать браузер с нужным сайтом, а также отправлять пользователю уведомления. Кроме того, приложение размещает на одном из рабочих столов прозрачный виджет, загружающий баннеры. Как отмечают ИБ-специалисты, после установки программа демонстрирует рекламные сообщения каждые пару минут.

Авторы FakeAdsBlock предусмотрели для него защитные механизмы: программа скрывает следы своего присутствия, и единственный индикатор ее работы — значок VPN-соединения в панели состояния. Зловред удаляет свое название и иконку из списка установленных приложений, отображаясь в нем как пустая строка.

Помимо фальшивого блокировщика рекламы, исследователи обнаружили код FakeAdsBlock в установочных комплектах с названиями фильмов. По мнению ИБ-аналитиков, это указывает на возможность распространения программы через

нелегальные онлайн-кинотеатры…» ***(Egor Nashilov. Преступники маскируют adware-зловред под блокировщик рекламы // Threatpost (https://threatpost.ru/fakeadsblock-poses-itself-as-an-adblocker-obviously-is-not/34859/). 18.11.2019).***

***

«Специалисты Visa обнаружили ранее неизвестный вредоносный скрипт, похищающий данные банковских карт со страниц интернет-магазинов. Зловред, получивший название Pipka, нашли как минимум на 16 сайтах, занимающихся онлайн-торговлей. Вредоносный JavaScript-сценарий можно настроить под конкретный веб-ресурс, при этом он способен самоликвидироваться после выполнения своей задачи.

Эксперты выяснили, что скиммер охотится за номерами банковских карт, CVV, учетными данными PayPal и другой финансовой информацией — в зависимости от структуры целевого сайта. Один из вариантов программы, попавший в руки исследователей, справлялся с двухэтапным вводом сведений, когда биллинговые данные запрашиваются на разных страницах…

Исследователей удивила способность зловреда самоудаляться из HTML-кода инфицированного интернет-магазина. Как только скрипт загружается на сайт, он очищает все свои теги, не оставляя видимых следов присутствия в системе. Такое поведение серьезно затрудняет обнаружение Pipka как средствам безопасности, так и администратору ресурса.

Вредоносный сценарий передает собранные данные на командный сервер, предварительно закодировав их при помощи шифра ROT13 и по Base64. Прежде чем отправить очередную порцию информации, программа проверяет, не загружала ли она эти сведения ранее, чтобы избежать дублирования данных.

Киберкампания, зафиксированная в сентябре этого года, затронула веб-ресурсы, расположенные в Северной Америке. Один из сайтов, инфицированных Pipka, был ранее заражен скиммером Inter, однако специалисты не берутся утверждать, что обе программы написаны одним автором.

Аналитики также не назвали движок, на котором работали зараженные сайты. В начале октября ИБ-специалисты нашли скиммер на сайте разработчика решений для Magento. Похититель информации перехватывал платежные данные покупателей плагинов Extendware, а также мог быть внедрен в исходный код расширений, скачиваемых из репозитория.» ***(Egor Nashilov. Скиммер Pipka умеет удалять себя с зараженного сайта // Threatpost (https://threatpost.ru/pipka-skimmer-removes-itself-after-successful-execution/34848/). 16.11.2019).***

***

«Киберпреступники, стоящие за шифровальщиком Sodinokibi, используют эксплойт-пак RIG для доставки зловреда на целевые машины. Нападающие эксплуатируют баги в браузерах, чтобы скрытно установить полезную нагрузку и заблокировать файлы. ИБ-специалисты пока не нашли способа расшифровать данные, затронутые атакой вымогателя.

Sodinokibi атакует через баги в Internet Explorer

Первоначальное заражение происходит через рекламные баннеры в блогах и онлайн-играх. Объявление ведет жертву на криминальный ресурс, который скрытно пытается запустить на компьютере вредоносный скрипт из арсенала RIG.

Киберпреступники действуют через Flash-уязвимости в браузерах и в случае успешного взлома отправляют на устройство полезную нагрузку. Нападение не требует взаимодействия с пользователем — он может догадаться об атаке лишь по сообщениям с ошибками, которые выводит Internet Explorer.

На первом этапе на машину при помощи вредоносного JavaScript доставляется обфусцированный VBS-сценарий, исполняющий функции загрузчика и установщика для Sodinokibi. Вымогатель скрытно шифрует файлы, после чего устанавливает обои рабочего стола и создает текстовый документ с требованием выкупа. Зловред присваивает инфицированному устройству уникальный идентификатор и добавляет его в качестве расширения ко всем закодированным объектам.

О новом векторе атаки рассказал в Твиттере ИБ-специалист с псевдонимом mol69. По мнению эксперта, кампания нацелена на пользователей из Южной Кореи, Малайзии, Вьетнама и других стран Юго-Восточной Азии. Чуть позже аналитик сообщил, что нападения ведутся также через эксплойт-пак Fallout.

В сентябре этого года независимый исследователь под ником Security Aura выяснил, что для распространения Sodinokibi киберпреступники применяли оверлеи на страницах взломанных сайтов. По его словам, злоумышленники внедряли в код уязвимого WordPress-ресурса скрипт, который выводил поверх легитимной страницы фрейм с фальшивым интернет-форумом, где одно из сообщений содержало вредоносную ссылку. Для большей убедительности сообщения ветки подбирались с учетом тематики инфицированного сайта.» ***(Egor Nashilov. Вымогатель Sodinokibi распространяют через эксплойт-пак RIG // Threatpost (https://threatpost.ru/sodinokibi-propagates-via-rig-exploit-kit/34804/). 12.11.2019).***

***

«ИБ-специалист Алекс Ланштейн (Alex Lanstein) обнаружил оригинальный вектор для распространения RAT-трояна. Киберпреступники доставляют зловред, перенаправляя жертву через открытый редирект с сайта Cisco на зараженную страницу, где размещен фальшивый клиент WebEx — ПО для онлайн-конференций.

Вредоносные письма маскируются под приглашение WebEx

Атака начинается с письма, содержащего приглашение на WebEx-конференцию. В качестве отправителя указан официальный сайт системы, а внешний вид сообщения соответствует легитимным образцам. В тексте размещена ссылка, по которой жертва якобы может присоединиться к беседе.

Киберпреступники используют механизм открытого редиректа, который позволяет отправить посетителя на сторонний ресурс через легитимный сайт. Несмотря на то, что ссылка из фальшивого приглашения включает в себя официальный домен Cisco, в действительности она открывает страницу злоумышленников. Жертве предлагают скачать файл webex.exe, якобы

необходимый для начала конференции, однако вместо утилиты на компьютер попадает троян WarZone, который способен:

загружать, удалять и запускать файлы;

перехватывать ввод с клавиатуры;

активировать службы удаленного доступа к машине;

дистанционно управлять видеокамерой;

похищать сохраненные пароли из Firefox и Chrome.

Специалисты не смогли точно определить принадлежность бэкдора к тому или иному семейству. Некоторые сервисы определяют его как WarZone, другие идентифицируют как троян AveMariaRAT. Программа внедряется в системный процесс MusNotificationUx, который отвечает за всплывающие уведомления о доступных обновлениях Windows. Вредонос также создает ярлык в списке автозапуска, чтобы продолжить работу после перезагрузки компьютера.

Согласно статистике, собранной специалистами Spamhaus, в III квартале этого года зловред AveMariaRAT занял предпоследнее место в топ-20 троянов по количеству командных серверов — на его счету 19 центров управления. Наибольшее число ресурсов у ботнета Lokibot, авторы которого держат 898 криминальных сетевых узлов.» ***(Egor Nashilov. Преступники дают ссылки на RAT-троян в приглашениях WebEx // Threatpost (https://threatpost.ru/cisco-webex-used-in-rat-trojan-delivery/34792/). 11.11.2019).***

***

«Специалисты «Лаборатории Касперского» рассказали о бэкдоре Titanium, который APT-группировка Platinum использует в атаках на организации в Юго-Восточной Азии. Зловред получает команды через код, зашифрованный в PNG-изображениях, и может манипулировать файлами на инфицированном компьютере. Для доставки основной полезной нагрузки в целевую систему проводится многоэтапная атака с применением шелл-кода и утилиты для создания задач в планировщике Windows…

Как выяснили ИБ-аналитики Kaspersky, первоначальное заражение производится через веб-ресурсы, ориентированные на посетителей из Индонезии, Вьетнама и Малайзии.

На первом этапе в системный процесс winlogon.exe внедряется шелл-код, который скачивает и распаковывает загрузчик. Последний представляет собой зашифрованный SFX-архив, декодируемый при помощи вшитого пароля.

Загрузчик связывается с командным сервером и скачивает зашифрованную полезную нагрузку. Вредоносная программа способна обрабатывать объекты различных типов и запускать как исполняемые файлы, так и DLL-библиотеки. Для доставки бэкдора дроппер использует системную службу Windows Background Intelligent Transfer Service (BITS), а также модуль IBackgroundCopyManager.

В зависимости от аргументов, полученных из центра управления, загрузчик может собрать и отправить киберпреступникам информацию об антивирусных продуктах, установленных на инфицированном компьютере. После доставки бэкдора загрузчик самоликвидируется.

Исследователи подчеркивают, что шифрование компонентов зловреда и бесфайловые методы запуска затрудняют его обнаружение антивирусными

сканерами. Кроме того, чтобы обмануть средства защиты, киберпреступники используют каталоги и названия файлов легитимного ПО…

Троян маскируется под легитимную программу для создания DVD-видео или приложение для настройки звуковых драйверов. За установку бэкдора отвечает специальный скрипт, который при помощи бесплатной утилиты с URL добавляет вредоносный процесс в планировщик задач Windows. Злоумышленники могут менять ход атаки через параметры сценария, подстраивая его действия под конкретную целевую систему.

Бэкдор отправляет командному серверу запрос, а в ответ получает PNG-файлы с зашифрованными в них командами. Киберпреступники используют стеганографию для внедрения кода в изображение. Как выяснили специалисты «Лаборатории Касперского», зловред способен читать, загружать, удалять и запускать любые файлы на зараженной машине, а также работать с командной строкой ОС…» ***(Egor Nashilov. APT-группа Platinum вооружилась бэкдором Titanium // Threatpost (https://threatpost.ru/titanium-backdoor-used-by-platinum-apt/34790/). 11.11.2019).***

***

«Организаторы самой продолжительной вредоносной кампании в истории сайтов на базе WordPress заражают веб-ресурсы без троянов и загрузчиков. Жертвы группировки WP-VCD сами устанавливают бэкдоры на свои ресурсы, загружая пиратские плагины и темы оформления.

Этот метод уже более двух лет позволяет злоумышленникам обходить защитные системы и зарабатывать на трансляции нежелательной рекламы. Как отметили аналитики, операторы WP-VCD наладили самоподдерживающийся механизм для наживы: круг жертв постоянно пополняется очередными любителями бесплатного ПО, а грамотно написанный бэкдор дает централизованное управление армией зараженных площадок.

Как проходят атаки WP-VCD

По данным аналитиков Wordfence, на данный момент WP-VCD — одна из самых масштабных вредоносных кампаний, нацеленных на WordPress-сайты. Зараженные бэкдором темы можно найти на множестве сайтов, причем мошенники выводят свои страницы на первые позиции в поисковиках с помощью скомпрометированных веб-ресурсов.

Когда владелец такой страницы разворачивает у себя зловред WP-VCD, тот создает PHP-файл, который встраивает бэкдор в уже установленные темы и плагины. Таким образом, даже если администратор со временем удалит загруженное ПО, преступники сохранят доступ к его ресурсу. Чтобы не вызывать подозрений, вредоносный скрипт также манипулирует системными данными скомпрометированных модулей, скрывая дату внесенных изменений.

Параллельно WP-VCD создает аккаунт администратора и передает на управляющий сервер данные очередной жертвы. Для доступа к каждой площадке зловред генерирует специальный пароль, используя MD5-хеш ее URL.

Закончив работу с обнаруженными темами и плагинами, WP-VCD сканирует хостинговую инфраструктуру, чтобы заразить сайты, связанные с пораженным ресурсом. На этих площадках он также устанавливает бэкдоры — набор их

функций совпадает с родительским образцом, за исключением возможности дальнейшего распространения. После этого зловред удаляется с сайта.

Возможности встроенных бэкдоров

Создатели бэкдора предусмотрели ряд специфических возможностей, которые позволяют им надежно закрепиться на ресурсе. В коде зловреда прописаны запасные адреса управляющих серверов на тот случай, если основной будет недоступен, а обновления кода единовременно поступают на все зараженные сайты. Даже если пользователь загружает скомпрометированный плагин годовой давности, то получает актуальную версию бэкдора.

Кроме того, управляющий сервер может передавать подконтрольным сайтам данные для продвижения вредоносных площадок в поисковиках. Именно поэтому сайты с опасными темами и плагинами стабильно возглавляют выдачу по релевантным запросам. Этот метод обеспечивает преступникам постоянный поток новых жертв, причем они могут повышать и понижать темпы продвижения.

Конечная цель всей кампании состоит в трансляции нежелательных баннеров на взломанных сайтах. Исследователи связывают рекламные показы с партнерской сетью Propeller Ads, которая уже была замечена в подобных кампаниях. Представители компании отрицают сотрудничество с мошенниками, однако не предпринимают особых усилий для проактивной блокировки нежелательных рекламодателей.

Эксперты призывают веб-администраторов загружать темы и плагины легально — это защитит ресурсы от атак WP-VCD. Если владельцы сайтов привлекают к оформлению сторонних специалистов, стоит убедиться, что подрядчики также используют только чистое ПО.

По данным ИБ-экспертов, до 98% уязвимостей WordPress-ресурсов связаны со сторонними компонентами. Чтобы помочь администраторам с защитой сайтов, разработчики CMS запустили рейтинг, который отражает соответствие плагинов практикам безопасной разработки.» ***(Egor Nashilov. WordPress-сайты заражают через пиратское ПО // Threatpost (https://threatpost.ru/wp-vcd-wordpress-malware-propagates-via-warez/34742/). 06.11.2019).***

***

«Киберпреступники активно используют политическую повестку, чтобы распространять вредоносное ПО. Исследователи предупредили о сотнях киберкампаний, в рамках которых шифровальщики, средства удаленного доступа и прочие нежелательные программы маскируются под статьи и документы по актуальным темам.

Эксперты решили изучить эту тему, когда обнаружили в одной из атак группировки Cobalt вредоносный файл trump.exe. Как показало дальнейшее расследование, это лишь одна из множества подобных приманок для потенциальных жертв.

Зловреды, играющие роль полезной нагрузки в ходе этих кампаний, давно известны ИБ-специалистам. Так, документ Word под названием «12 вещей, которые Трамп должен знать о Северной Корее» разворачивает на компьютере RAT-троян Konni, активный, по разным оценкам, с 2014 года. Эксперты замечали этот зловред

в атаках против государственных и частных организаций, которые также были связаны с КНДР.

Другой вредоносный документ, Excel-файл «Индикаторы администрации Трампа относительно инвестиций в Китай», содержал макросы для загрузки RAT PoisonIvy. Операторы этого зловреда ранее уже использовали актуальные темы — в 2014 году троян распространялся под видом материалов о пропавшем рейсе «Малазийских авиалиний» MH-370…

Президент США оказался не единственным политиком, чье имя использовалось в нынешних атаках. Материал якобы о северокорейском лидере Ким Чен Ыне заражал жертв трояном Nechta, а файл Papa-Putin.exe маскировал троян NjRAT. Имя Владимира Путина также встретилось экспертам в названии примитивного вымогателя, который блокирует на компьютере элементы управления и диспетчер задач.

По словам исследователей, с приближением американских выборов в 2020 году политические темы будут набирать популярность у киберпреступников. Как заметили ИБ-эксперты, злоумышленники не оставляют без внимания крупнейшие темы, будь то Чемпионат мира по футболу, Олимпийские игры или криптовалютная лихорадка. Пользователям следует учитывать этот факт и с особой осторожностью относиться к ресурсам и сообщениям под громкими заголовками.» ***(Egor Nashilov. Преступники используют имена политиков, чтобы завлечь жертв // Threatpost (https://threatpost.ru/politicians-names-are-used-to-lure-victims-for-malware/34740/). 06.11.2019).***

***

«В период с июля по сентябрь участники Антифишинговой рабочей группы (APWG) выявили 266 387 сайтов-ловушек — значительно больше, чем во II квартале. Столь высокую активность фишеров эксперты последний раз наблюдали в конце 2016 года. В минувшем квартале APWG также получила 122 359 отчетов о фишинговых рассылках — против прежних 112 163.

Количество торговых марок, заимствуемых при создании фишинговых сайтов, тоже возросло. Исследователи из MarkMonitor, регулярно принимающие участие в составлении квартальных отчетов APWG, в среднем ежемесячно фиксировали более 400 атакуемых брендов, тогда как в предыдущем квартале этот показатель составлял 313.

Основные мишени фишеров остались прежними — веб-почта и SaaS (ПО как услуга, совокупно 33% инцидентов); сбор учетных данных к таким сервисам значительно облегчает реализацию BEC-схем. На системы приема платежей в отчетный период пришлось 21% фишинговых атак, на финансовые институты — 19%.

По данным компании Agari, еще одного активного участника APWG, в 40% случаев BEC-мошенники отправляли поддельные письма с аккаунта, привязанного к специально зарегистрированному доменному имени, созвучному названию известной компании. Бесплатные почтовые ящики использовались с этой целью в 54% BEC-атак.

В Agari идентифицируют одну группировку такого профиля — ей присвоено кодовое имя Silent Starling. По словам экспертов, она состоит из трех основных

участников, которые обычно взламывают email-аккаунт поставщика, вендора или иного партнера намеченной жертвы и долго собирают информацию, копируя переписку.

Статистику по фишинговым доменам APWG обычно публикует на основании данных, собранных компанией RiskIQ. Согласно этому источнику, 65% поддельных страниц, обнаруженных в III квартале, пришлось на долю родовых доменов верхнего уровня .COM, .ORG, .NET и других давно существующих TLD-зон. Из региональных TLD по этому показателю лидируют .BR (Бразилия) и .GA (Габон), регистрация в котором бесплатна. Российский национальный домен занял в общем рейтинге 10 место, поделив его с .AU и .TOP.

По оценке PhishLabs, еще одного неизменного соавтора отчетов APWG, в настоящее время более двух третей (68%) фишинговых сайтов используют HTTPS — это самый высокий показатель за последние пять лет. В связи с этим исследователи напоминают, что значок замка в адресной строке браузера говорит лишь о защите соединений шифрованием и не гарантирует безвредность онлайн-ресурса.

Активность фишеров в Бразилии, которую исправно отслеживают в компании Axur, также продолжает расти; по словам экспертов, количество таких инцидентов в стране увеличилось более чем в два раза в сравнении с I кварталом. Эта тенденция особенно ярко выражена в почтовом веб-сервисе и SaaS. В то же время атаки мошенников в сфере электронной коммерции, участившиеся во II квартале, пошли на спад.» ***(Maxim Zaitsev. APWG зафиксировала трехлетний рекорд по фишингу // Threatpost (https://threatpost.ru/apwg-reports-phishing-activity-highest-in-three-yrs/34727/). 05.11.2019).***

***

«Модульный зловред QSnatch атакует сетевые хранилища QNap и крадет учетные данные пользовательских аккаунтов. Об этом сообщили специалисты Центра национальной компьютерной безопасности Финляндии (NCSC-FI). Удалить вредоносную программу можно при помощи специальной утилиты, выпущенной производителем, или сбросив настройки устройства до заводских.

ИБ-специалистам не известно, как QSnatch попадает в уязвимую систему. Скрипт внедряется в прошивку NAS-устройства и получает полезную нагрузку с командного сервера, используя алгоритм генерации адреса. Далее зловред блокирует работу встроенного антивируса, отключает механизм обновления системного ПО и вносит изменения в некоторые легитимные процессы…

Зловред открывает канал связи с командным сервером и передает на него все логины и пароли, связанные с инфицированным устройством. По словам ИБ-специалистов, QSnatch способен загружать из центра управления новые модули, расширяющие его функции. Для исправления ошибки и удаления зловреда из зараженных хранилищ QNap выпустила обновление программы Malware Remover и нескольких версий ОС QTS.

Безопасными считаются прошивки:

4.3.6 build 20190328;

4.3.4 build 20190322;

4.3.3 build 20190322;
4.2.6 build 20190322.

Пользователям NAS-устройств QNap рекомендуют срочно установить необходимые обновления или сбросить настройки ОС до заводских. При этом второй вариант приводит к уничтожению всей информации в хранилище.

Количество устройств, пострадавших от атаки, неизвестно, но, по мнению экспертов немецкого CERT, QSnatch заразил не менее 7000 хостов…» ***(Egor Nashilov. Инфостилер QSnatch атакует сетевые устройства QNap // Threatpost (https://threatpost.ru/qsnatch-attacks-qnap-nas-storages/34721/). 05.11.2019).***

***

«Исследователи кибербезопасности обнаружили шифровальщик, написанный на редком языке PureBasic, атакующий серверы под управлением Windows и Linux. Анализ кода заставил предположить, что этот вредоносный софт ранее был простым бэкдором, - передает SCNews.

Эксперты компании Intzer и подразделения IBM X-Force IRIS team опубликовали анализ нового шифровальщика PureLocker, характеризующегося целым рядом нетипичных для программ подобного рода особенностей. Шифровальщик атакует прежде всего корпоративные серверы под управлением Windows и Linux.

«Обращает внимание язык программирования, на котором он написан. Это далеко не самый распространённый язык. Он, во-первых, кроссплатформенный, во-вторых, как ни странно, многие антивирусы с трудом справляются с написанными на нём программами», - резюмируют представители IBM. - «Вдобавок, код PureBasic легко портируется на Windows, Linux, OS X, что упрощает атаки на различные платформы».

К нетипичным для шифровальщикам особенностям исследователи отнесли также его механизмы противодействия обнаружению. Например, этот вредонос пытается избежать перехвата функций API, NTDLL посредством скачивания другой копии ntdll.dll и разрешения API-адресов из неё. Перехват API позволяет антивирусным системам видеть, что именно делает любая функция, которую вызывает программа.

Исследователи отметили, что это - распространённая методика ухода от обнаружения, но шифровальщики ею пользуются весьма редко. Кроме того, вредонос вызывает утилиту Windows regsrv32.exe для «тихой» установки библиотечного компонента PureLocker - никаких диалоговых окон пользователю не выводится. Позднее шифровальщик проверяет, был ли произведён запуск regsrv32.exe, и файловое расширение - .dll Или .ocx; кроме того, он проверяет, установлен ли на машине 2019 год и наличие административных прав у жертвы. Если хоть одно условие не выполнено, вредонос деактивируется.

По мнению экспертов, такое поведение нетипично для шифровальщиков, которые обычно не проявляют особой избирательности. Напротив, они стремятся заразить как можно больше машин. При анализе кода, исследователи обнаружили в PureLocker заимствования из кода бэкдора more_eggs, который в даркнете предлагается в формате MaaS. Им активно пользуются финансовые киберкриминальные группировки Cobalt Group и FIN6.» ***(Редкий шифровальщик***

атакует Windows и Linux-серверы // SecureNews (https://securenews.ru/redkiy-shifrovalschik-atakuet-windows-i-linux/). 19.11.2019).

***

«Эксперты по безопасности не рекомендуют пользователям перезагружать свои компьютеры после заражения вымогательским ПО, поскольку ситуация может стать только хуже в определенных обстоятельствах. Перезагрузка может привести к перезапуску прерванного процесса шифрования файлов и потенциальной потере ключей шифрования, хранящихся в памяти.

Исследователи рекомендуют жертвам перевести компьютер в спящий режим, отключить его от сети и обратиться к профессиональным IT-специалистам. Выключение компьютера также является альтернативой, но спящий режим лучше, поскольку он сохраняет копию памяти, где некоторые вымогатели могут иногда оставлять копии своих ключей шифрования.

Группа экспертов из компании Symantec, Стэнфордского и Нью-Йоркского университетов провела опрос среди 1180 взрослых американцев, ставших жертвами вымогательского ПО в последние годы. По результатам, почти 30% жертв приняли решение перезагрузить свои компьютеры в качестве способа борьбы с инфекцией.

Перезагрузка в безопасном режиме является хорошим способом удаления старых вымогателей, использующих блокировщики экрана, однако специалисты не рекомендуют прибегать к данному варианту при работе с современными версиями вымогателей, которые шифруют файлы.

«Как правило, исполняемый файл вредоноса, шифрующий ваши данные, предназначен для сканирования через подключенные к определенной машине диски. Иногда он отключается или блокируется из-за проблем с разрешениями и прекращает шифрование. Если вы перезагрузите машину, вредонос запустится вновь и попытается завершить работу. Система может быть зашифрована только частично из-за какой-то удачной ошибки или проблемы, поэтому пользователи НЕ должны позволять вредоносному ПО завершить свою работу... не перезагружаться!», — отметил генеральный директор компании Covewar Билл Зигель (Bill Siegel).

По словам специалистов, жертвы вымогателей должны также пройти два этапа процесса восстановления после заражения. Первым делом необходимо обнаружить артефакты вымогателей (процессы и механизмы персистентности) и удалить их с зараженного устройства, а затем осуществить восстановление данных, если доступен механизм резервного копирования.

Как отмечает Зигель, когда компании пропускают первый шаг, перезагрузка компьютера часто перезапускает вымогатели и заканчивает процесс шифрования недавно восстановленных файлов, и тогда жертвам придется перезапускать процесс восстановления данных с нуля.» ***(Эксперты советуют не перезагружать компьютер после заражения вымогателями // SecurityLab.ru (https://www.securitylab.ru/news/502366.php). 07.11.2019).***

***

«ESET сообщает об обнаружении нового банковского трояна Mispadu, который использует фейковую рекламу McDonald's для распространения.

Ранее ESET описала вредоносы Amavaldo и Casbaneiro, похожие на Mispadu: они также написаны на Delphi и используют всплывающие уведомления Windows для выманивания личных данных жертвы.

Специалисты ESET сообщают, что атака совершается с помощью спама и вредоносной рекламы. Мошенники размещали коммерческие публикации на Facebook, которые предлагали скидочные купоны в McDonald's.

Кликая по рекламному объявлению, потенциальная жертва загружала ZIP-файл, который маскировался под скидочный купон. Запустив его, пользователь невольно загружал банковский троян Mispadu.

Попав на устройство жертвы, Mispadu мог делать скриншоты, имитировать движения мышкой и нажатия нужных клавиш на клавиатуре. Кроме того, он способен собирать следующие данные: версию ОС, список установленных банковских приложений и антивирусных программ, а также другие персональные данные.

Целевая аудитория Mispadu — пользователи из Мексики и Бразилии.

Что примечательно, в Бразилии Mispadu обнаружен в официальном магазине расширений Google Chrome. Троян обещает защитить браузер — но вместо этого пытается украсть банковскую информацию.» ***(Новый банковский троян распространяется через рекламу McDonald's // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5625108-Novyj-bankovskij-troyan-rasprostran.html). 19.11.2019).***

***

«**Эксперты назвали самые эффективные способы, которые позволяют заразить компьютеры вирусами.** Согласно проведенному исследованию, в период с января по июль лишь каждая 19-я загрузка вирусного ПО не была связана с электронной почтой.

В настоящее время активно развиваются технологии, позволяющие повысить кибербезопасность, вместе с тем, злоумышленники создают и реализуют новые способы их преодоления. Специалисты отмечают, что первое место по-прежнему занимает информация, передаваемая по e-mail. Речь идёт об электронных письмах, к которым прилагаются архивы. При получении подобного файла от неизвестного или непроверенного интернет-ресурса, следует проявить крайнюю осторожность. Опасность содержится в ссылках в таких посланиях, причём по своей сомнительный популярности они уступают архивам.

Хакеры пользуются возможностью обойти фильтры почтовых сервисов. Кибермошенники присылают письма в нерабочие часы, а имеющаяся в них ссылка временно недоступна, так как её активируют позднее. В этом случае письмо распознаётся как безопасное. Исследование проводилось специалистами в 60 странах мира.» ***(Митник Михайло. Названы самые популярные способы заражения компьютеров вирусами // iTechua (https://technoportal.com.ua/gadgets/37897). 25.11.2019).***

***

«Влада Ізраїлю розпочала процес екстрадиції до США громадянина Росії Олексія Буркова, якого підозрюють у вчиненні кіберзлочинів…

Міністр юстиції Ізраїлю Амір Охана підписав ордер на видачу Буркова до США 30 жовтня цього року.

Олексія Буркова затримали 13 грудня 2015 року за запитом США під час проходження паспортного контролю при виїзді з Ізраїлю.

США наполягали на екстрадиції громадянина Росії через наявні у них докази його причетності до кіберзлочинів. Російська сторона раніше також направила до Ізраїлю запит на екстрадицію Буркова, однак отримала відмову.» ***(Російського хакера екстрадують з Ізраїлю до США // Інформаційне агентство «1NEWS» (https://1news.com.ua/svit/rosijskogo-hakera-ekstraduyut-z-izrayilyu-do-ssha.html). 12.11.2019).***

***

«В конце прошлой недели окружной суд Северной Каролины вынес приговор по уголовному делу о продаже в Интернете услуг по проведению DDoS-атак. За преступный сговор с целью причинения вреда чужим компьютерам 21-летний житель штата Иллинойс Сергий Усатюк наказан лишением свободы на 13 месяцев.

Согласно материалам дела, молодой человек и его сообщник из Канады создали ряд онлайн-сервисов, работавших по модели DDoS как услуга, и управляли ими с августа 2015 года по ноябрь 2017-го. В деле фигурируют такие названия, как ExoStresser, QuezStresser, Betabooter, Databooter, Instabooter, Polystress и Zstress.

«Только за первые 13 месяцев работы эти сервисы выполнили заказы на проведение 3 829 812 DDoS-атак, — сказано в обвинительном заключении. — В рекламной записи на сайте ExoStresser от 12 сентября 2017 года говорится, что данный сервис инициировал проведение 1 367 610 DDoS-атак, обернувшихся для сетей жертв 109 186 часами (4549 днями) простоя».

Сообщники получали прибыль не только от сдачи в аренду ботнета и оказания иных DDoS-услуг подписчикам, но также за счет размещения рекламы «коллег по цеху». За время своей противоправной деятельности предприниматели суммарно скопили $542 925 — по крайней мере, такая сумма была обнаружена на счетах Усатюка после ареста.

Заявление молодого человека о признании вины суд заслушал в конце февраля этого года. По выходе на свободу осужденный проведет три года под надзором. У него также конфискуют капиталы, нажитые неправедным путем…» ***(Maxim Zaitsev. Оператор DDoS-сервисов получил тюремный срок // Threatpost (https://threatpost.ru/operator-of-seven-ddos-services-sentenced-to-13-months-in-prison/34851/). 18.11.2019).***

***

«Сотрудники китайских правоохранительных органов пресекли деятельность и арестовали участников киберпреступной группировки, управляющей DDoS-ботнетом из 200 тыс. инфицированных сайтов. Операция является первым серьезным шагом властей Китая в борьбе с впечатляющим местным рынком DDoS-услуг, пишет ZDNet.

После публикации в 2016 году исходного кода IoT-ботнета Mirai, китайские киберпреступники стали активно создавать на его основе новые ботнеты и сдавать их в аренду за деньги. В 2017 году специалисты Cisco Talos зафиксировали резкий всплеск числа китайских сервисов, предлагающих услуги по осуществлению DDoS-атак. Исследователи обвиняли правоохранительные органы КНР в бездействии и нежелании предпринимать какие-либо меры по борьбе со стремительно растущим рынком DDoS-сервисов.

В настоящее время китайские DDoS'еры существенно расширили свои горизонты и помимо IoT-устройств и Mirai стали использовать другие ресурсы. К примеру, для создания ботнетов они начали эксплуатировать уязвимости в web-серверах и PHP-фреймворке . В конце концов число ботнетов увеличилось настолько, что власти больше не могли игнорировать их, и полиции пришлось действовать.

Операция по закрытию крупнейшего в Китае ботнета началась еще в августе 2018 года. Как сообщали местные СМИ, полиции провинции Цзянсу стало известно об огромном количестве взломанных серверов, принадлежащих компании Xuzhou Telecom. Серверы были заражены бэкдорами, предоставляющими киберпреступниками контроль над ними.

В ходе дальнейшего расследования была выявлена преступная операция по внедрению вредоносного ПО на сайты через уязвимости. Скомпрометированными оказались 200 тыс. сайтов, в том числе правительственные порталы.

На этой неделе, спустя более года с начала расследования, сотрудники полиции в 20 городах КНР арестовали 41 подозреваемого, в том числе двух операторов ботнета, и конфисковали у них 10 млн юаней (порядка $1,4 млн). Управляемый киберпреступниками ботнет использовался в основном для осуществления DDoS-атак (пиковая мощность достигала 200 Гбит/с), однако иногда он также использовался для внедрения на взломанные сайты спама, рекламы и майнеров криптовалюты.» ***(Китайский рынок DDoS-услуг лишился крупнейшего ботнета // SecurityLab.ru (https://www.securitylab.ru/news/502365.php). 07.11.2019).***

***

«Подозреваемый выдавал себя за немецкие, итальянские и американские правительственные агентства для беспрепятственного проникновения в офисы компаний и установки фишингового вредоносного ПО. Под видом налогов итальянец выманил больше €630.000…

С октября итальянский хакер, чье имя не раскрывается в рамках следствия, выдавал себя за правительственные учреждения, рассылая фишинговые электронные письма, предназначенные для заражения американских и европейских организаций. Злоумышленник выдавал себя за Федеральное Министерство финансов Германии, Италии и Почтовую службу США.

«URL-адреса, используемые этим актером, были форматированы повторяющимся символом _ /. Tmp. На протяжении долгого времени хакер даже не вносил в них никаких изменений», - подытоживает представитель Proofpoint. «Исследователи нашей компании подозревают, что использование слова _ /. Tmp может быть связано с предыдущими хищениями, которые были обнаружены в прошлом полугодии сообществом infosec».

Преступная схема была проста: в приемную компаний приходил правительственный чиновник с «официальной проверкой безопасности систем» и, беспрепятственно устанавливал вредоносное ПО. В том числе в «репертуар» злоумышленника входила фишинговая рассылка, - организациям приходили письма с сообщением о возврате или задолженности по налогам. Жертвам было необходимо открыть документ Word и заполнить форму, а далее перейти на фейковую страницу безналичной оплаты.

Пресечь преступную деятельность смогли только немецкие финансисты, «пересчитав» декларацию о налогах и обратившись в правоохранительные органы.» ***(Под видом госчиновника итальянский хакер выманил больше €630.000 // SecureNews (https://securenews.ru/pod-vidom-goschinovnika/). 15.11.2019).***

***

«Нью-Йоркская прокуратура просит для гражданина РФ Станислава Лисова, участвовавшего в кибератаках с использованием трояна NeverQuest, наказание в виде пяти лет лишения свободы. Соответствующее ходатайство было внесено в базу данных федерального суда Южного округа штата Нью-Йорк в четверг…

Житель Таганрога Станислав Лисов был арестован в Барселоне 13 января 2017 года во время отпуска. Арест был произведен в связи с обвинениями, выдвинутыми против россиянина властями США. Американские власти обвиняли Лисова в создании и распространении вредоносного ПО NeverQuest и хищении с его помощью крупных сумм. В августе 2017 года суд Барселоны согласился выдать обвиняемого американским властям, и в феврале нынешнего года он признал свою вину по одному из двух пунктов. В частности, Лисов признал себя виновным в заговоре с целью осуществления кибератак.

Вынесение приговора обвиняемому несколько раз откладывалось, однако теперь оно назначено на 21 ноября. Прокуратура ходатайствует о пяти годах лишения свободы и не намерена требовать большего срока.

Как ранее предполагал адвокат Лисова Аркадий Бух, его подзащитный может быть приговорен к тому сроку, который он уже отбыл в Испании, а это в общей сложности 3 года. В таком случае после вынесения приговора россиянин будет сразу же отпущен.» ***(Российский оператор ботнета NeverQuest может сесть в тюрьму на 5 лет // SecurityLab.ru (https://www.securitylab.ru/news/502391.php). 08.11.2019).***

***

«Суд у США засудив російського хакера Станіслава Лісова до чотирьох років тюремного ув'язнення, однак з урахуванням відбутого під вартою терміну він вийде на свободу через кілька місяців…

Суддя Валері Капроні заявила, що росіянина засуджують до 48 місяців тюремного ув'язнення, однак погодилася зменшити цей термін на 15% "за хорошу поведінку", а також врахувала той факт, що він раніше вже провів в ув'язненні в Іспанії і США близько трьох років.

Крім того, росіянин повинен виплатити штраф у розмірі $50 тис., а також $480 тис. як відшкодування шкоди особам, постраждалим від його дій.

Після виходу з в'язниці Лісов, "найімовірніше, буде депортований в Росію", сказала суддя Капроні.

Адвокат росіянина Аркадій Бух зазначив, що Лісов, швидше за все, буде депортований в Росію "навесні 2020 року", однак не виключив, що процес депортації може затягнутися.

Станіслав Лісов був заарештований в Іспанії в січні 2017 року і екстрадований в США в січні 2018 року.

Американська влада звинуватила його в створенні шкідливої програми NeverQuest для крадіжки банківських даних і особистої інформації. За даними прокуратури, за допомогою NeverQuest хакери намагалися викрасти мільйони доларів. Лісов в період з червня 2012 року по січень 2015 року брав участь у створенні NeverQuest, а також управління комп'ютерною мережею, яка застосовувалася для поширення вірусу.

У лютому поточного року росіянин визнав свою провину по одному з двох пунктів звинувачення, який стосується змови з метою кібератак.

Спочатку йому загрожувало тюремне ув'язнення тривалістю до 35 років.» ***(Чотири роки в'язниці отримав в США російський хакер // Інформаційне агентство «1NEWS» (https://1news.com.ua/svit/chotyry-roky-v-yaznytsi-otrymav-v-ssha-rosijskyj-haker.html). 22.11.2019).***

***

«Правоохранители в Европе провели крупномасштабную кибератаку на инструменты интернет-пропаганды радикальных исламистов. В операции приняли участие правоохранители из 30 государств, включая Германию, заявили в Федеральном ведомстве по уголовным делам (ВКА) в понедельник, 25 ноября.

Координацией четырехдневного мероприятия занималась полицейская служба Европейского Союза (Европол). По ее данным, в ходе операции были заблокированы тысячи интернет-сайтов, имеющих отношение к террористической группировке "Исламское государство" (ИГ), а также группы и каналы в мессенджерах. Среди удаленного контента - пропагандистские видеоролики, а также материалы, которые "возвеличивают или поддерживают терроризм и экстремизм".

Ранее сотрудники профильного отдела ВКА направили в Европол предложения по удалению более 1300 аккаунтов в мессенджерах и свыше 200 интернет-ссылок. С октября 2018 года по ноябрь 2019-го провайдерам было предложено удалить почти 13 тысяч ссылок, они исполнили запросы примерно в 60 процентах случаев.

Первые удар по сетевой инфраструктуре близкого к ИГ информагентства Amaq прошли в августе 2016 года. Вторая операция против сетевой деятельности террористов была проведена в июне 2017 года под руководством Гражданской

гвардии Испании. Изъятие серверов в ходе этой акции позволило выявить радикалов в 133 странах. В апреле 2018 года состоялась еще одна операция против пропаганды ИГ, в рамках которой полиция изъяла серверы в Канаде, Нидерландах и США.» ***(Павел Мыльников. Полиция из 30 стран провела кибероперацию против пропаганды ИГ // Deutsche Welle (https://www.dw.com/ru/%D0%BF%D0%BE%D0%BB%D0%B8%D1%86%D0%B8%D1%8F-%D0%B8%D0%B7-30-%D1%81%D1%82%D1%80%D0%B0%D0%BD-%D0%BF%D1%80%D0%BE%D0%B2%D0%B5%D0%BB%D0%B0-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D1%8E-%D0%BF%D1%80%D0%BE%D1%82%D0%B8%D0%B2-%D0%BF%D1%80%D0%BE%D0%BF%D0%B0%D0%B3%D0%B0%D0%BD%D0%B4%D1%8B-%D0%B8%D0%B3/a-51413369?maca=rus-rss-MetaUA_rus_V_Mire-3045-xml-mrss). 26.11.2019).***

***

Технічні аспекти кібербезпеки

«…недавно в ходе глобального исследования выяснилось, какие типы файлов представляют наибольшую угрозу. Ими оказались zip-архивы и, что удивительно, аудиосообщения…

Согласно сообщению портала Techradar, авторитетное агентство Mimecast, занимающееся вопросами кибербезопасности, проанализировало 207 миллиардов электронных писем и сообщений с целью выявления наиболее эффективных средств взлома и заражения гаджетов простых пользователей. Анализ рисков затрагивал самые разные сферы — от обычных сервисов, которыми пользуемся мы с вами каждый день, до крупных секторов экономики вроде транспортных, юридических и банковских компаний.

Специалисты компании Mimecast проанализировали поток сообщений, прошедший через сеть с июля по сентябрь 2019 года. В результате из уже упомянутых 207 миллиардов электронных писем и сообщений, 99 миллиардов оказались заражены. Исследование Mimecast было сосредоточено также на выявлении основных типов атак.

Почему атаки с использованием различного рода сообщений должны быть вашей проблемой безопасности номер один? Дело в том, что подобные атаки нацелены на получение данных учетных записей администраторов устройств, будь то ПК или смартфоны. А имея эту информацию можно получить доступ и ко всей системе в целом. — говорится в докладе специалистов из Mimecast.

Было выявлено, что что киберпреступники запускают целые кампании по атакам на различные сервисы, которые длятся в целом несколько дней. Эти сложные атаки, скорее всего, выполняются организованными группами, так как они используют различные эксплойты, шифрование и другие методы для того, чтобы избежать обнаружения.

Самое интересное заключается в том, что был выявлен сравнительно новый тип хакерских атак, которые используют аудиосообщения в качестве инструментов для фишинга (воровство паролей и учетных записей пользователей) и заражения устройств аудиосообщения. С одной стороны, как заверяют в Mimecast это связано с тем, что под аудиосообщения довольно легко замаскировать вредоносные файлы, которые при этом смогут еще и воспроизводить звук, что собьет с толка жертву.

С другой стороны, хакеры часто начали использовать методы социальной инженерии, чтобы при помощи звонков из якобы серьезных организаций вести диалог с пользователем и выуживать из него нужную информацию, записывая семплы его голоса с нужными фразами. Данные фразы впоследствии можно «склеить» в предложения и, например, позвонить в банк от имени этого человека, используя его собственный голос. Так что будьте бдительны.

Другой распространенный тип атак — это атаки посредством zip-файлов. Дело в том, что антивирусные средства смартфонов все еще, по мнению Mimecast, недостаточно хорошо работают с проверками архивов. И таким образом довольно просто заразить смартфоны и планшеты жертв с целью похищения конфиденциальной информации.» ***(Почему голосовые сообщения представляют наибольшую опасность для пользователей // Український телекомунікаційний портал (https://portaltele.com.ua/news/software/pochemu-golosovye-soobshheniya-predstavlyayut-naibolshuyu-opasnost-dlya-polzovatelej.html). 21.11.2019).***

***

«Компания Trend Micro опубликовала исследование Securing 5G Through Cyber-Telecom Identity Federation. Его целью стало изучение слабых мест сетей пятого поколения, методов, которыми современные киберпреступники могут воспользоваться, чтобы скомпрометировать их, а также поиск решений, которые помогут защититься от атак.

В качестве объекта для своего исследования Trend Micro выбрала небольшую локальную NPN-сеть (непубличную сеть) условного общежития с поддержкой 5G, в которой используются SIM-карты. Общежитие в данном случае представляет собой пример закрытой сети пятого поколения, связанной с «внешним миром» через общедоступные телекоммуникационные каналы. Вскоре такие сети появятся повсеместно, например, на производственных объектах, предприятиях и в офисах крупных компаний. SIM-карты в оборудовании для таких сетей содержат идентификационные данные пользователя, поддерживают шифрование и даже оборудованы простейшим ПО и функцией удалённого обновления этого ПО и прошивки.

…все системы ИТ-безопасности касаются только самого объекта и его «облака», но никак не защищают трафик, передаваемый через внешние публичные и закрытые сети. Поэтому злоумышленники могут реализовать целый ряд кибератак, чтобы скомпрометировать телекоммуникационные каналы и через них саму сеть 5G. В исследовании упоминается три типа таких атак, целью которых может стать аппаратная часть сети, данные или удостоверения.

При атаках аппаратного уровня может использоваться метод удалённых манипуляций с SIM-картой (SIMjacking) в роуминге (то есть при работе вне «домашней» сети), например, модификация её настроек таким образом, чтобы

устройство пользователя подключалось не к публичной сети, а к сети, которой управляют киберпреступники. Благодаря изменениям в настройках SIM-карты хакеры затем смогут осуществлять прослушивание разговоров пользователя, инициировать инъекции вредоносного ПО и кибертаки или мешать алгоритмам машинного обучения.

При атаках на данные и саму сеть взломанная хакерами SIM-карта используется для того, чтобы ухудшить производительность самого устройства и сети, к которой оно подключено или даже изменить базовые настройки этой сети. Атаки salami и low-and-slow с многих устройств позволят со временем создать в инфраструктуре сети «слепые пятна», которые хакеры смогут использовать для более масштабных и разрушительных кибератак.

В атаках с применением телекоммуникационных каналов и удостоверений злоумышленники пользуются тем, что существует определённое несоответствие между способами обработки удостоверений в ИТ-системах и этих каналах. Большая часть удостоверений и учётных данных в телекоммуникационных каналах завязана на SIM-карту и обрабатывается на аппаратном уровне, а в ИТ-инфраструктуре – на уровне ПО. Соответственно, после кражи личности пользователя при помощи взлома карты, хакеры получают доступ и к ИТ-системам, которые настроены так, чтобы автоматически «доверять» устройству с этой SIM-картой. В результате они могут использовать эту уязвимость для обхода систем защиты от мошеннических действий, изменения функций сети и даже изменения конечных продуктов, если речь идёт о производстве.

В качестве решения возникающих проблем Trend Micro предлагает объединить три основных элемента, обеспечивающих безопасность сетей 5G (целостность и безопасность сетей передачи данных, SIM-карт и устройств, а также внешних сетей), в единую систему – см. рисунок выше. Её использование позволит вовремя обнаруживать «заражённые» устройства в «домашней» сети, защитить SIM-карты от взлома и перезаписи прошивок и даже применять элементы блокчейна, чтобы обеспечить безопасность SIM-карт при работе вне «домашней» сети.» ***(Trend Micro изучила потенциальные уязвимости сетей 5G // Компьютерное Обозрение (https://ko.com.ua/trend_micro_izuchila_potencialnye_uyazvimosti_setej_5g_131040). 27.11.2019).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Шифрование является одним из ключевых механизмов, которые Apple использует для защиты личных данных пользователей. В целях безопасности компания шифрует колоссальный массив данных – от маршрутов в Apple Maps до личной переписки в мессенджере и электронной почте.

Это делается для того, чтобы никто посторонний не мог прочесть конфиденциальную информацию и не мог воспользоваться ей в личных целях. Тем

не менее, иногда даже самые совершенные протоколы шифрования, направленные на нашу с вами защиту, дают сбой, и тогда Apple приходится несладко.

Почтовый сервис Apple принято считать одним из самых безопасных, но это заблуждение Исследователь в области кибербезопасности Боб Гендлер выяснил, что в macOS есть опасная уязвимость, из-за которой почта пользователей сохраняется в незашифрованном виде.

В теории это значит, что её может прочесть кто угодно, потому что содержимое посланий хранится в открытом виде вне зависимости от того, было использовано шифрование при их отправке или нет.

По словам Гендлера, он обнаружил баг ещё эти летом и сообщил о нём Apple. Однако в Купертино ответили, что знают о существовании сбоя и планируют исправить его в самое ближайшее время. Уязвимости macOS По состоянию на ноябрь 2019 года уязвимость по-прежнему присутствует в macOS, затрагивает сразу четыре версии операционной системы: Sierra, High Sierra, Mojave и Catalina.

Получается, что Apple не удосужилась исправить баг более чем за 100 дней, продолжая подвергать пользователей опасности. Впрочем, здесь есть несколько оговорок, о которых обязательно нужно знать, прежде чем начинать бить тревогу. Текст незашифрованных сообщений хранится в системном файле snippets.db, который использует Siri.

Правда, сохранение происходит только в том случае, если пользователь отправляет зашифрованные послания через штатное приложение «Почта», но при этом отключил системное шифрование FireVault. В случае, если вы используете сторонний почтовый клиент или защищаетесь при помощи FireVault, даже теоретическая угроза раскрытия личной переписки вам не грозит.

К тому же, чтобы получить доступ к содержимому сообщений нужно наверняка знать, где их искать, заполучив предварительно физический доступ к Mac жертвы, что не так-то просто.

После того как Гендлер предал огласке информацию об уязвимости в системе шифрования электронной почты в macOS, Apple признала её существование и пообещала исправить. По словам представителей компании, обновление с исправлением выйдет в ближайшее время, обеспечив пользователям и их переписке полнейшую конфиденциальность…» ***(В macOS есть уязвимость, которая позволяет читать зашифрованную почту // Український телекомунікаційний портал (https://portaltele.com.ua/news/events/v-macos-est-uyazvimost-kotoraya-pozvolyaet-chitat-zashifrovannuyu-pochtu.html). 11.11.2019).***

***

«То, что сейчас происходит с Apple, походит на чёрную полосу, которую компания никак не преодолеет. iOS 13 оказалась настолько проблемной, что теперь в Купертино вынуждены, не покладая рук, проектировать свежие обновления, чтобы устранить все уязвимости и системные баги, коих оказалось даже слишком много…

Агентство по кибербезопасности и безопасности инфраструктуры США рекомендует не пренебрегать установкой iOS 13.2 и macOS 10.15.1. В ведомстве объяснили, что обновление является необходимой мерой по обеспечению безопасности совместимых устройств и данных пользователей. Дело в том, что

предыдущие версии операционных систем уязвимы для хакерских атак, поскольку позволяют выполнить на устройствах произвольный код, перехватывать трафик и повышать привилегии без ведома пользователя…

Довольно необычно, что Агентство по кибербезопасности и безопасности инфраструктуры США вообще беспокоится о пользователях Apple. Во всяком случае, прежде подобных ситуаций не возникало, что в свою очередь может указывать на кардинальные перемены, произошедшие либо в ведомстве, из-за чего оно стало интересоваться рядовыми пользователями, либо с операционными системами Apple, которые стали настолько небезопасными, что теперь, учитывая их высокую степень распространения, представляют угрозу для огромного числа людей…» ***(Агентство по кибербезопасности США призывает срочно установить iOS 13.2 // Український телекомунікаційний портал (https://portaltele.com.ua/news/events/agentstvo-po-kiberbezopasnosti-ssha-prizyvaet-srochno-ustanovit-ios-13-2.html). 03.11.2019).***

***

«Разработчики WhatsApp исправили серьезную уязвимость, которая могла привести к отказу в обслуживании или удаленному выполнению кода. Баг получил заплатку еще в октябре, однако в Facebook предпочли не разглашать эту информацию, чтобы пользователи успели установить важное обновление. О проблеме стало известно лишь после публикации бюллетеня безопасности, который компания выпустила 14 ноября 2019 года…

Недостаток связан с неправильной обработкой метаданных элементарного потока при воспроизведении видео в формате MP4. Для эксплуатации уязвимости злоумышленник должен узнать номер телефона жертвы и отправить ей специально созданный файл. Воспроизведение вредоносного объекта в WhatsApp вызовет переполнение буфера стека и приведет к зависанию программы, а в некоторых случаях позволит атакующему запустить сторонний скрипт на устройстве.

Элементарный поток (Elementary Stream) — определенная стандартом MPEG зашифрованная последовательность данных одного типа, передаваемая на выход аудио- или видеодекриптора.

Уязвимость зарегистрирована в базе данных MITRE как CVE-2019-11931. Недостаток затронул мобильные версии WhatsApp для Android, iOS и Windows Mobile, а также варианты мессенджера для корпоративных клиентов…

Разработчики добавили патч, устраняющий проблему, в следующие версии WhatsApp:

Android 2.19.274;

iOS 2.19.100;

Business for Android 2.19.104;

Business for iOS 2.19.100;

Enterprise Client 2.25.3.

Актуальная на данный момент версия WhatsApp для Windows Phone 2.18.368 остается уязвимой для атак с использованием бага. Разработчик прекращает поддержку мессенджера для мобильной операционной системы Microsoft 31 декабря 2019 года. Будет ли до этого момента выпущен еще один релиз программы — неизвестно.

Представители Facebook заявили, что не знают о случаях эксплуатации CVE-2019-11931 в дикой природе…» ***(Maxim Zaitsev. Вредоносный видеофайл позволяет выполнить код в WhatsApp // Threatpost (https://threatpost.ru/whatsapp-rce-vulnerability-could-be-triggered-via-malicious-mp4-file/34868/). 19.11.2019).***

***

«Компания Intel выпустила очередной пакет обновлений, куда вошли заплатки к 77 уязвимостям. Пользователей защитили от утечек системных данных, взлома аутентификационных ключей и потери контроля над Windows-устройствами.

Уязвимости TPM-FAIL

Две проблемы обнаружились в модулях доверенных платформ (Trusted Platform Module, TPM) Intel fTPM и STMicroelectronics TPM. Эти компоненты используются в ноутбуках, персональных компьютерах, смартфонах и IoT-устройствах — они участвуют в генерации цифровой подписи для защищенного обмена данными.

Эксперты объединили уязвимости CVE-2019-11090 и CVE-2019-16863 под названием TPM-FAIL. Злоумышленники могут воспользоваться этими багами, чтобы восстановить долговременные приватные ключи и подделать цифровые подписи по алгоритму ECDSA. По данным исследователей, в результате такой атаки можно за несколько часов подобрать аутентификационный ключ VPN-сервера.

Уязвимые модули используются в большом количестве устройств, поэтому пользователям рекомендуют самостоятельно уточнять у производителей, коснулась ли их эта проблема.

Атака ZombieLoad v2

О первой версии уязвимости Zombieload инженеры Intel сообщили в мае — угроза связана с микроархитектурной выборкой данных (Microarchitectural Data Sampling, MDS). Этот баг позволяет читать конфиденциальную информацию в памяти процессоров, такую как ключи шифрования, пароли и прочие ценные данные.

Как выяснилось, весной производитель раскрыл только часть информации, чтобы дать специалистам время подготовить полноценную защиту. Атака Zombieload v2 (CVE-2019-11135), о которой стало известно сейчас, актуальна для процессоров с поддержкой технологии TSX (Transactional Synchronization Extensions). Разработчики научились манипулировать этой функцией и вызывать конфликт операций внутри интегральной схемы.

Как и в случае оригинальной Zombieload, результатом станет утечка закрытых данных. В Intel подчеркнули, что обновленная версия атаки не позволяет преступникам выбирать, какую информацию они получат. Тем не менее облачные провайдеры и владельцы масштабных серверных инфраструктур должны срочно обновить используемые продукты.

Уязвимая технология по умолчанию включена на всех чипах Intel, которые поступили в продажу с 2013 года. В список входят и процессоры последнего поколения Cascade Lake, представленные в апреле.

Проблемы с драйверами ядра

В комментарии к пакету обновлений директор по коммуникациям Джерри Брайант (Jerry Bryant) особо подчеркнул вклад сторонних специалистов в безопасность продуктов Intel. Внешние эксперты нашли 10 из 77 уязвимостей, вошедших в нынешний пакет. Это число включает и критические баги драйверов ядра, способные открыть злоумышленнику полный доступ к целевому устройству.

Подобная проблема коснулась нескольких десятков драйверов. Публичный список включает 39 позиций, наименования остальных станут известны, когда будут готовы соответствующие патчи.

Как рассказали эксперты, такие драйверы могут читать и редактировать физическую память, записывать данные в регистры процессора, а также пользуются доступом к операциям ввода-вывода и PCI-шине. Злоупотребление этими функциями грозит потерей контроля над устройством, причем под угрозой оказались чипы, выпущенные еще в 1999 году…» ***(Egor Nashilov. Разработчики Intel закрыли 77 багов, включая ZombieLoad v2 // Threatpost (https://threatpost.ru/intel-patches-77-vulns-including-zombieload-v2-an-tpm-fail/34828/). 14.11.2019).***

***

«Эксперты Microsoft предупредили пользователей о растущей угрозе кибератак на базе уязвимости BlueKeep. Как выяснили специалисты, преступники создали новый эксплойт, который уже применяется для распространения зловредов-криптомайнеров.

Уязвимость BlueKeep (CVE-2019-0708) содержится в сервисе удаленного подключения (Remote Desktop Service, RDS) к Windows 7, Windows Server 2008 и Windows Server 2008 R2. Она позволяет выполнить на компьютере сторонний код и автоматически распространять вредоносное ПО внутри инфраструктуры. Патч к этому багу был опубликован еще в мае, однако, по информации ИБ-аналитиков, количество уязвимых машин по-прежнему исчисляется сотнями тысяч.

О попытках массового использования BlueKeep ранее сообщил независимый исследователь Кевин Бомонт (Kevin Beaumont). В конце октября эксперт заметил серию критических ошибок на ханипотах, которые были созданы специально для привлечения BlueKeep-зловредов. Как выяснилось, сбои спровоцировал новый эксплойт, созданный на базе Metasploit-модуля.

Дальнейшее расследование, к которому подключились специалисты Microsoft и независимый исследователь Маркус Хатчинс (Marcus Hutchins), показало, что злоумышленники пытаются установить на уязвимые компьютеры ПО для добычи криптовалют. Используемый эксплойт работает нестабильно, что и вызывает многочисленные критические ошибки RDS. В то же время эксперты подчеркивают, что не стоит недооценивать возможные успешные атаки, которые остаются за кадром.

Аналитики связали криптоджекерскую кампанию с серией подобных атак в сентябре. Все инциденты объединяет один управляющий сервер. По словам специалистов, преступники экспериментируют со средствами доставки полезной нагрузки, и BlueKeep-эксплойт пополнил арсенал злоумышленников в начале октября.

География новых атак BlueKeep и будущее эксплойта

Значительная часть инцидентов пришлась на Францию (18%), Россию (16%) и Италию (10%). В отличие от предыдущих, полностью автоматизированных кампаний с применением BlueKeep, организаторы октябрьских атак вручную загружали эксплойт на уязвимые компьютеры. Далее зловред выполнял серию PowerShell-скриптов, чтобы развернуть майнер и закрепиться на машине.

Специалисты прогнозируют, что в будущем преступники станут применять новый эксплойт для доставки других типов вредоносного ПО. Эксперты уже нашли способ устранить проблемы, которые вызывали критические ошибки на взломанных компьютерах.

«Пользователям необходимо срочно обновить ПО, обращая особое внимание на RDP-приложения вендоров и прочих сторонних организаций, — подчеркнули исследователи Microsoft. — Такие системы нередко выпадают из поля проверки, и пока пользователи не найдут у себя все подобные программы, преступники смогут использовать BlueKeep, не оставляя очевидных следов в инфраструктуре»…» ***(Maxim Zaitsev. Специалисты Microsoft изучили попытки применения BlueKeep // Threatpost (https://threatpost.ru/microsoft-investigates-bluekeep-coin-mining-campaign/34794/). 11.11.2019).***

***

«Эксперты «Лаборатории Касперского» обнаружили серьезную ошибку нулевого дня в браузере Chrome. Уязвимость позволяет злоумышленникам выполнить вредоносный код, используя недостаток use-after-free в одном из компонентов интернет-обозревателя.

Киберпреступники уже взяли баг на вооружение и эксплуатируют его в кампании, получившей название Operation WizardOpium. Разработчики Google залатали уязвимость в свежей версии Chrome для Windows, macOS и Linux.

Недостаток нашли в ходе анализа ранее неизвестного эксплойта, зафиксированного антивирусными сканерами «Лаборатории Касперского». Программа распространяется через вредоносную инъекцию на одном из корейских новостных порталов и представляет собой JavaScript-сценарий, загружаемый с подконтрольного киберпреступникам сервера.

Сценарий атаки Operation WizardOpium через 0-day в Chrome

Первоначальный загрузчик проверяет наличие на компьютере браузера Chrome и отправляет командному центру ряд AJAX-запросов на загрузку зашифрованных частей зловреда. Компоненты собираются в один файл на целевом устройстве и распаковываются при помощи RC4-ключа, также полученного с C&C-сервера. Итоговый код эксплойта представляет собой готовый к использованию обфусцированный скрипт на языке JavaScript.

Как выяснили эксперты «Лаборатории Касперского», зловред использует ошибку состояния гонки, вызванную недостаточной синхронизацией между двумя процессами в браузере. Из соображений безопасности они не называют уязвимую подсистему, но из бюллетеня безопасности Google понятно, что речь идет об одном из модулей, связанном с обработкой аудио. Эксплуатация недостатка приводит к состоянию use-after-free и возможности выполнения стороннего кода.

Вредоносная программа пытается определить указатели некоторых 64-разрядных адресов памяти и использовать эти сведения для обхода рандомизации

размещения адресного пространства (ASLR). Эксплойт выполняет многочисленные операции с памятью, что наряду с другими методами позволяет злоумышленникам получить произвольный примитив чтения/записи. В результате атакующие создают специальный объект для WebAssembly и FileReader в среде браузера, который запрашивает полезную нагрузку с командного сервера…

Разработчики Google выпустили внеочередную версию браузера, чтобы исправить уязвимость, зарегистрированную как CVE-2019-13720. ИБ-специалисты рекомендуют пользователям Chrome как можно быстрее обновить его до версии 78.0.3904.87.

Предыдущая сборка обозревателя увидела свет 22 октября этого года. Плановое обновление включало в себя патчи для 37 уязвимостей, а также новые функции безопасности, запущенные в тестовом режиме. Так, разработчики Chrome приступили к испытанию службы предупреждения о компрометации паролей Password Leak Detection.» ***(Egor Nashilov. Специалисты Kaspersky нашли 0day в Chrome // Threatpost (https://threatpost.ru/0day-in-chrome-wizardopium/34710/). 02.11.2019).***

***

«***5G оказалась еще опаснее, чем ее предшественницы.*** К такому выводу пришли исследователи в области безопасности университетов Айовы и Пердью. Ученые обнаружили около десятка уязвимостей, которые, по их словам, могут в режиме реального времени отследить геолокацию жертвы, подделать «аварийные» правительственные оповещения, вывести смартфон из строя или даже саму сеть в целом…

Хуже того! В совместном заявлении сказано, что некоторые из новых угроз также могут распространиться и на уже существующие 4G-сети, что до этого было невозможно. В ходе одной из атак ученые заявили, что им удалось получить как старые, так и новые временные сетевые идентификаторы телефонов «подопытных жертв», что позволило им выявить случай пейджинга, который можно использовать для отслеживания местоположения телефона или даже перехватить канал для трансляции поддельных оповещений о чрезвычайных ситуациях.

«Это может привести к искусственно созданной панике», - отмечено в пресс-релизе, - «подобно тому, как ранее, по ошибке, было отправлено аварийное оповещение, что над Гавайями летит ядерная баллистическая ракета, запущенная Северной Кореей».

Другая атака может быть использована для создания длительного отказа сотовой сети. В некоторых случаях уязвимости могут сократить радиус сотовой связи, что позволит правоохранительным органам и хакерам следить за гражданами и атаковать их гаджеты, используя специальное оборудование «скат» [Платформа, выполняющая в режиме реального времени контроль, управление и глубокий анализ трафика на уровне протоколов и приложений. Обеспечивает фильтрацию по «черным» и «белым» спискам, управление QoS, QoE].

Учитывая природу уязвимостей, исследователи заявили, что не планируют публично публиковать свой проверочный код эксплуатации. Однако, исследователи уведомили Ассоциацию GSM о своих выводах. Представитель ведомства Клэр Крэнтон заявила, что «Уязвимости были оценены как нулевые или

незначительные». GSM не отметил, будут ли они устранены и не указал график каких-либо исправлений. «Можем подчеркнуть, что отчет написан слишком неоднозначно», - сказала Крэнтон.

В зоне риска пользователи Android, в том числе Nexus 6P, Huawei и Samsung.» ***(5G оказалась еще опаснее, чем ее предшественницы // SecureNews (https://securenews.ru/5g-okazalas-esche-opasnee-chem-ee-predchestvenniki/). 14.11.2019).***

***

«Исследователи обнаружили утечку данных в программном обеспечении Asus Wi-Fi, которая дала бы хакерам беспрецедентный доступ к сетям пользователей и позволила бы взломать устройства умного дома, такие как Alexa и Amazon…

Уязвимость, обнаруженная vpnMentor, находится в AsusWRT, графическом веб-интерфейсе, который связывается с маршрутизаторами для настройки частных сетей Wi-Fi. Хотя приложение служит централизованной точкой доступа для пользовательских устройств, подключенных к Интернету, включая телефоны, планшеты, ноутбуки и другие устройства, оно также открывает пользователей для атаки хакеров.

Среди прочего, исследователи смогли выяснить IP-адреса, «имена пользователей», названия устройств, информацию об использовании и командах IFTTT, координаты долготы и широты, а также информацию о местоположении. Они, однако, упоминают, что никакая личная информация не была доступна для просмотра. Тем не менее, перекрестные ссылки на все просочившиеся данные могут легко позволить хакерам идентифицировать пользователя и его адрес. «Используя чьи-то координаты и IP-адрес, хакер может точно определить физический адрес пользователя», - объясняют vpnMentor.

Поскольку этот недостаток позволил взять под контроль незащищенные устройства в сетях AsusWRT, это также создало риск грабежей и мошенничества. «Хакеры могут использовать захваченные устройства, чтобы отслеживать поведение пользователей, находясь дома, заниматься спортом, когда в доме никого нет, и планировать грабежи с минимальным риском для воров», - добавили исследователи. «Если целевой пользователь AsusWRT имеет устройства с интеллектуальной блокировкой, хакеры могут получить к ним доступ, чтобы открыть двери через скомпрометированные устройства».

Исследователи отмечают, что, похоже, ранее эта уязвимость была замечена и другими ИТ-специалистами, но до сих пор не была раскрыта самой компанией. Остается неясным, смогли ли хакеры воспользоваться ею на практике.» ***(Плохие новости для пользователей Asus. Вас, скорее всего, уже взломали // SecureNews (https://securenews.ru/plohie-novosti-dlya-asus/). 08.11.2019).***

***

«Команда исследователей из компании Applied Risk обнаружила более 100 уязвимостей в различных системах управления зданиями (building management system, BMS) разных популярных брендов. Их эксплуатация

позволяет злоумышленнику осуществлять DoS-атаки, удаленно выполнять код и полностью скомпрометировать критические системы зданий.

Исследователи проанализировали системы управления зданиями различных поставщиков, в том числе Bosch, Nortek, Siemens, Schneider, Omron, Optergy, Trane, Tridium и пр. По результатам поисковых запросов Shodan, специалисты выявили около 19 тыс. уязвимых BMS, подключенных к Сети, большую часть из них составили BMS производства BACnet (7623 систем), Bosch (3239), Reliable Controls (3148) и Nortek (2582).

Каждая из данных систем доступна в Сети и может быть проэксплуатирована злоумышленником. BMS использовались в различных структурах, включая правительственные здания, банки, больницы или спальные районы, подвергая риску атак более 10 млн людей. Преступник может вызвать отказ отказ в обслуживании систем, подключенных к интернету, и перехватить контроль над помещениями у управляющих зданием.

Все исследованные BMS-системы содержат одни и те же уязвимости, среди которых наличие бэкдор-аккаунтов или консолей разработки, установки/конфигурации out-of-the box, установленные по умолчанию или встроенные учетные данные, отсутствие оценки безопасности прошивки, отсутствие статического анализа исходного кода, непроверенные входные параметры и недостаточная защита данных в сети и в хранилищах…» ***(В системах управления зданиями обнаружено более 100 уязвимостей // SecurityLab.ru (https://www.securitylab.ru/news/502662.php). 18.11.2019).***

***

«Исследователь проблем кибербезопасности Владимир Палант (Wladimir Palant) в этот понедельник рассказал в блоге о серии уязвимостей в компоненте онлайновой защиты, Kaspersky Web Protection, программных продуктов «Лаборатории Касперского», включая Kaspersky Internet Security 2019. Ошибки, обнаруженные им в декабре прошлого года, открывают внутренний прикладной программный интерфейс (API) этих продуктов для манипуляций со стороны вебсайтов.

Функции онлайновой защиты включают в себя сканирование результатов поиска для отсеивания потенциально вредоносных ссылок, блокировки рекламы и предотвращения отслеживания. Web Protection обменивается данными с основным приложением Kaspersky, и «секретная» подпись, которая теоретически должна быть неизвестна веб-доменам, призвана обеспечить безопасность этих коммуникаций. Однако, уязвимость позволяла веб-сайтам «достаточно легко», по словам Паланта, извлекать этот секретный ключ, «устанавливать соединение с приложением Kaspersky и отправлять команды так же, как это проделывает Web Protection».

Специалисты «Лаборатории» устранили ряд указанных недоработок, однако в апдейте Kaspersky Internet Security 2020, вышедшем в июле 2019 года, по словам Паланта, не только всё ещё остаются некоторые из них, но и появились новые…

«Лаборатория Касперского» сходу отмела претензии эксперта, ответив в блоге, что уже исправила все ошибки в компоненте веб-защиты своих продуктов и их расширений для Google Chrome. В то же время, компания признала, что: «Даже

самые тщательные превентивные меры не могут исключить просачивания мелких ошибок — ни один программный продукт в мире не может полностью избавиться от них на профилактической стадии».

Но даже мелкие ошибки в антивирусном ПО представляют особую опасность, отмечает Крэг Янг (Craig Young) из фирмы Tripwire: «Эти системы — желанная цель для вредоносного использования, потому что они, как правило, имеют максимальные права доступа и смогут обрабатывать опасные входные данные с минимальным вовлечением пользователей».

Новый патч уже разработан и будет доступен 28 ноября, но, учитывая упорное стремление разработчиков внедрять скрипты в веб-страницы, не полагаясь только на расширения браузеров, Палант не надеется, что проблемы будут полностью решены и в этот раз.» ***(ПО от Kaspersky Lab остаётся уязвимым для манипуляций веб-мастеров // Компьютерное Обозрение (https://ko.com.ua/po_ot_kaspersky_lab_ostayotsya_uyazvimym_dlya_manipulyacij_veb-masterov_131041). 27.11.2019).***

***

«В Google Play более 800 приложений оказались в зоне риска. Об этом составили отчет компания по обеспечению кибербезопасности Check Point, передают Podrobnosti.

Среди затронутых приложений оказались такие, которые люди используют очень часто: Facebook, WeChat, Messenger, Instagram, AliExpress, TuneIn и SHAREit. В этих приложениях есть множество "дыр" в безопасности, которые находятся в самих приложениях.

Facebook оправдывается и сообщает, что это не проблема, так как данные между клиентом и сервером шифруются, поэтому злоумышленники не в состоянии обойти защиту.

Google старается заставить разработчиков исправить приложения.» ***(В Google Play более 800 приложений в опасности // Багнет (http://www.bagnet.org/news/tech/412562/v-google-play-bolee-800-prilozheniy-v-opasnosti). 26.11.2019).***

***

«Специалисты, которые занимаются кибербезопасностью установили, что путем достаточно простых действий можно получать видео, фотографии, звукозаписи и даже ваше местоположение практически от любого смартфона.

Весь этот "букет" пользователь может подцепить, если разрешит приложению достаточно стандартный набор: доступ к хранилищу, камере, местонахождению и т.д. И уже тогда в опасности могут оказаться конфиденциальные документы, диктофонные записи или снимки, а также видео. Все это дает хакерам возможность шпионить за вами, когда им захочется.

Поверьте, что даже этого хватить жуликам для шантажа. Они могут атаковать пользователя с помощью социальной инженерии, а в некоторых случаях даже украсть ценную и важную финансовою информацию. Но специалисты в ходе своего расследования узнали, что существует уязвимость, которая расширяет масштаб хакера просто к сумасшедшим границам.

Работники Checkmarx сумели заставлять камеру на смартфоне делать снимки, даже когда пользователь выключил экран. Также телефон принудительно может записывать видео.

Оказалось, что для этого необходима определенная (неназванная в целях безопасности) последовательность действий и внутренних системных вызовов. Поэтому все, что нужно злоумышленнику просто скачать себе полученные в результате ролики и фотографии…» ***(Катерина Андриюк. В Сеть слили информацию, как проследить за кем угодно через камеру его смартфона // Hyser Media (https://hyser.com.ua/community/119721-v-set-slili-informaciyu-kak-prosledit-za-kem-ugodno-cherez-kameru-ego-smartfona). 26.11.2019).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Дослідники з Наньянського технологічного університету (Nanyang Technological University, NTU Singapore) розробили квантовий чип, який у 1000 разів менший за сучасні, але пропонує таку ж квантову технологію підвищеної безпеки. Більшість провідних стандартів безпеки, які використовуються в методах безпечного зв'язку – від зняття готівки в банкоматі до покупки товарів через інтернет на смартфоні, – не використовують квантову технологію. Електронна передача персонального ідентифікаційного номера (ПІН) або пароля може бути перехоплена, що створює загрозу безпеці.

Цей квантовий чип завбільшки 3 мм використовує квантові алгоритми зв'язку для забезпечення підвищеної безпеки в порівнянні з існуючими стандартами. Це досягається шляхом інтеграції паролів в передану інформацію, утворюючи безпечний квантовий ключ. Після отримання інформації вона знищується разом з ключем, що робить її надзвичайно безпечною формою зв'язку.

Крихітний квантовий чип для безпечних комунікаційних технологій

Для цього також потрібно у 1000 разів менше місця, ніж для сучасних систем квантової зв'язку, які можуть бути такими ж великими, як холодильник або навіть займати простір цілої кімнати чи офісного поверху. Це відкриває двері для більш безпечних комунікаційних технологій, які можуть бути розгорнуті на компактних пристроях, таких як смартфони, планшети і розумні годинники. Це також закладає основу для кращих методів шифрування для онлайн-транзакцій і електронних комунікацій.

У сучасному світі кібербезпека дуже важлива, оскільки велика частина наших даних зберігається і передається в цифровому вигляді. Майже всі цифрові платформи і сховища вимагають, щоб користувачі вводили свої паролі і біометричні дані. І поки це так, їх можна підслуховувати або розшифровувати. Квантова технологія усуває це, оскільки і пароль, і інформація інтегруються у відправлені повідомлення, утворюючи квантовий ключ». - Професор Лю (Liu) зі Школи електротехніки та електроніки NTU

Квантовий зв'язок працює з використанням рандомізованих рядків коду для шифрування інформації, яку може відкрити тільки передбачуваний одержувач з правильним ключем. Немає необхідності передавати додаткові паролі або біометричні дані, що є стандартною практикою в сучасних формах зв'язку.

Найбільші світові технологічні компанії, в тому числі Google та IBM, прагнуть розробити квантові суперкомп'ютери, які б здійснили революцію в обчислювальній техніці на швидкостях, що зараз просто немислимі. Одна з очікуваних сил квантової технології полягає в криптографії – мистецтві секретного спілкування.

Квантова технологія безпечніша за класичні канали

З поширенням інтернет-сервісів платформи електронної пошти і месенджери, такі як WhatsApp, Facebook, Skype, Snapchat, Telegram тощо, створили свої власні захищені канали зв'язку – так звані «класичні канали». На відміну від квантових каналів, які несуть інформацію, є протоколи безпеки, які інтегровані в зашифровані дані. Кожен канал унікально відрізняється один від одного, знижуючи або навіть виключаючи ризик перехоплення або витоку інформації під час передачі.

Простіше кажучи, квантова технологія не вимагає додаткової передачі паролів або біометричних даних, які необхідні в «класичних каналах». Це виключає ризик перехоплення або витоку інформації, створюючи майже нерозривне шифрування. Квантовий комунікаційний чип, розроблений дослідниками NTU, буде економічно ефективним, оскільки він використовує стандартні промислові матеріали, такі як кремній, що також полегшує його виробництво.

Наразі, команда NTU прагне розробити гібридну мережу традиційних систем оптичного зв'язку і квантових систем зв'язку. Це поліпшить сумісність квантових технологій, які можуть бути використані в більш широкому діапазоні додатків, таких як підключення до інтернету.» ***Грицина Вікторія. Крихітний квантовий чип підвищить кібербезпеку смартфонів // Pingvin.pro (https://pingvin.pro/gadgets/news-gadgets/kryhitnyj-kvantovyj-chyp-pidvyshhyt-kiberbezpeku-smartfoniv.html). 04.11.2019).***

***

«Elcore Distribution объявляет о расширении сотрудничества с Trend Micro. В начале года компании анонсировали партнерство в Грузии, Казахстане, Молдове и Украине. Теперь полный спектр решений кибербезопасности японского разработчика будет доступен партнерам Elcore еще в восьми странах СНГ: в Азербайджане, Армении, Беларуси, Кыргызстане, Монголии, Таджикистане, Туркменистане и Узбекистане.

«Опыт взаимодействия в Украине, Казахстане, Молдове и Грузии показал высокую эффективность партнерства с Elcore Distribution в реализации проектов в области информационной безопасности. Поэтому мы последовательно расширяем масштабы нашего сотрудничества – рассказывает Герман Позанков, региональный директор Trend Micro в России, СНГ, Монголии. – Мы рады, что теперь наши решения станут еще ближе партнерам и заказчикам в странах СНГ. Совместно с Elcore Distribution мы, также, будем проводить обучение сотрудников коммерческих организаций и государственных учреждений и всеми возможными способами способствовать росту знаний в сфере ИБ и усилению защищенности

критически важных объектов инфраструктуры». ***(Решения Trend Micro будут доступны партнерам Elcore в 12 странах // Компьютерное Обозрение (https://ko.com.ua/resheniya_trend_micro_budut_dostupny_partneram_elcore_v_12_stranah_130789). 07.11.2019).***

***

«Польский исследователь безопасности создал инструмент сбора данных с открытым исходным кодом (OSINT), который индексирует информацию о чувствительных устройствах, подключенных к Интернету, и отображает их приблизительное местоположение на карте…

Исследователь говорит, что он создал инструмент как способ позволить организациям сканировать свои сети и идентифицировать уязвимое оборудование, но у инструмента также есть и темная сторона, так как он может использоваться злоумышленниками для нацеливания на организации с меньшими усилиями.

Названный Kamerka («камера» на польском языке), инструмент был выпущен в прошлом году. Инструмент работает на пользовательских поисковых запросах. Kamerka принимает эти запросы и использует поисковые системы, такие как Shodan и BinaryEdge, для поиска общих брендов определенного устройства и отображения результатов на карте Google.

В то время как в своей первоначальной версии Kamerka сканировала только камеры слежения (отсюда и название), инструмент получил несколько обновлений. Текущие версии могут сканировать и идентифицировать: камеры безопасности; принтеры; промышленное оборудование ICS / SCADA, подключенное к Интернету; системы и датчики, которые работают поверх протокола MQTT; устройства, которые транслируют потоковое видео на основе RTSP; твиты, посты в Instagram и изображения Flicker, которые содержат сведения о геолокации. Kamerka собирает эту информацию в базе Elasticsearch и затем наносит ее на карту Google.» ***(Почувствуйте себя хакером. Польский программист создал «карту критической инфраструктуры» // SecureNews (https://securenews.ru/pochuvstvuyte-sebya-hakerom/). 08.11.2019).***

***

«В честь 15-летия своего браузера Firefox компания Mozilla решила расширить свою программу вознаграждения исследователей безопасности за обнаруженные уязвимости (bug bounty) и увеличить максимальную сумму вознаграждения в три раза. Так, отныне за уязвимости удаленного выполнения кода в Firefox или других менее известных сервисах Mozilla (VPN, локализация, инструменты для управления кодом, распознавание речи и пр.) исследователь может получить $15 тыс. За другие уязвимости компания готова заплатить от $1 тыс. до $6 тыс.

Решение утроить сумму вознаграждения поставило Mozilla в один ряд с другими технологическими компаниями, у которых также есть программы bug bounty, правда, в самый конец этого ряда. К примеру, Yahoo! и Snapchat платят исследователям $15 тыс. за любую уязвимость в своих сервисах. $15 тыс. – минимальная сумма вознаграждения, которую предлагает Microsoft, тогда как максимальная составляет $300 тыс. Также для сравнения, максимальная сумма

вознаграждения в рамках bug bounty составляет $100 тыс. у Intel, $33 тыс. у Dropbox, $20 тыс. у Twitter и $150 тыс. у Google за уязвимости в ChromeOS.

Свою программу bug bounty также запустила компания Huawei. Она готова платить $220 тыс. за критические уязвимости в своих Android-устройствах (Mate, P, Nova, Y9 и Honor) и $110 тыс. за опасные уязвимости. К слову, за эти же уязвимости Google предлагает меньшие суммы – $200 тыс. и $100 тыс. соответственно.

Самое высокое вознаграждение предлагает компания Apple, в нынешнем году увеличившая сумму с $200 тыс. до $1 млн.» ***(Mozilla утроила сумму вознаграждения в рамках bug bounty // SecurityLab.ru (https://www.securitylab.ru/news/502715.php). 20.11.2019).***

***

«Поставщик решений в области кибербезопасности по всему миру, объявила о новой технологии безопасности Интернета вещей. Check Point Software Technologies первой из компаний предложила консолидированное решение для обеспечения безопасности, которое укрепляет и защищает программно-аппаратное обеспечение IoT-устройств и обеспечивает их защиту от продвинутых атак. Технология будет интегрирована в архитектуру Check Point Infinity благодаря приобретению стартапа Cymplify, базирующегося в Тель-Авиве…» ***(Check Point Software Technologies переворачивает подход к кибербезопасности устройств Интернета вещей // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5625105-Check-Point-Software-Technologies.html). 19.11.2019).***

***

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

Баймуратов М. О. Безпека інформаційних систем. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року : наук.-практ. комент. / Михайло Баймуратов, Борис Кофман, Олександр Старинець. - Київ, 2019. - 230 с.

Шифр зберігання НБУВ: ВА836870

***

Бойко В. Д. Кібербезпека та захист персональних даних в ЄС: проблеми цифрового суспільства / В. Д. Бойко, М. Д. Василенко // Наукові праці Національного університету «Одеська юридична академія». - 2019. - Т. 23. - С. 34-47.

Досліджено реформу ЄС щодо захисту персональних даних через призму кібербезпеки в умовах цифрового суспільства. Розглянуто новації, розбіжності та протиріччя між чинним законодавством та технічним вирішенням питань захисту персональних даних.

Шифр зберігання НБУВ: Ж72103

***

Демченко П. С. Правовий моніторинг вітчизняного законодавства в сфері реалізації Стратегії кібернетичної безпеки України / П. С. Демченко // Альманах права. - 2019. - Вип. 10. - С. 298-303.

Досліджено роль правового моніторингу як засобу дослідження нормативно-правових актів в сфері кібернетичної безпеки України. Розкрито загальні сутність та ознаки поняття «правовий моніторинг», роль правового моніторингу як методу дослідження та оцінки законодавства України як на стадії розробки,так й при характеристиці вже діючих правових норм. Піднято проблематику наявності деяких законодавчих прогалин в Законі України «Про основні засади кібербезпеки України» від 07.10.2017 року, в основі котрих полягає відсутність єдності юридичної техніки формулювання категоріального апарату, заснованого на технічній термінології, на котрою апелює сфера кібернетики та інформатики. Наведено підходи щодо проведення правового моніторингу, націленого на виявлення та усунення неточностей у системі нормативно-правових актів в сфері забезпечення кібернетичної безпеки в Україні.

Шифр зберігання НБУВ: Ж74094

***

Джулій В. М. Моделі та алгоритми виявлення атак в бездротових мережах передачі даних / В. М. Джулій, О. С. Лєнков, Л. О. Ряба // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. - 2018. - Вип. 59. - С. 76-86.

Запропоновано комплекс системних моделей процесу функціонування виявлення атак в складі інформаційної системи, заснованих на методології IDEF0 і IDEF1X, що дозволяють деталізувати процес виявлення атак в бездротових мережах і інтегрувати систему виявлення атак з компонентами інтегрованої системи захисту інформації в організації з урахуванням вимог нормативних документів. Представлено алгоритми виявлення атак на основі класифікуючої моделі з використанням методів інтелектуального аналізу даних, які на відміну від існуючих алгоритмів дозволяють підвищити точність виявлення атак і знизити кількість помилкових спрацьовувань за рахунок попереднього навчання і донавчання системи на даних реального мережевого трафіку. Обгрунтовано архітектуру інтелектуальної системи виявлення бездротових атак, яка функціонує на основі розроблених алгоритмів виявлення атак і їх об'єднання в ансамбль, застосування яких дозволяє з більш високою точністю і повнотою виявляти і блокувати атаки на бездротовий компонент інформаційної системи.

Шифр зберігання НБУВ: Ж73166

***

Інтелектуальні системи та інформаційні технології = Intellectual systems and information technologies : пр. міжнар. наук.-практ. конф., 19-24 серп. 2019 р., Одеса, Україна. - Одеса : ТЕС, 2019. - 268 с.

Зі змісту:

- Хорошко В., Хохлачова Ю., Ахмад Аясрах Расмі Алі. Забезпечення безпеки в кібернетичному просторі;
- Милов А., Евсеев С. Имитационное моделирование распределения инвестиций в системах кибербезопасности.

Шифр зберігання НБУВ: СО36861

***

Муляр І. В. Захист від прихованих загроз в середовищі хмарних обчислень / І. В. Муляр, О. В. Мірошніченко, А. В. Краснік, Л. В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. - 2018. - Вип. 59. - С. 115-126.

Розроблено модель прихованих загроз інформаційній безпеці в середовищі хмарних обчислень, що враховує активний характер суб'єктів і об'єктів інформаційної взаємодії. Запропоновано модель операцій, що відбуваються з даними при їх обробці в середовищі хмарних обчислень, що дозволяє формалізувати опис інформаційних процесів у вигляді мультиграфа транзакцій

Шифр зберігання НБУВ: Ж73166

***

Національна безпека: моніторинг реалізації законодавства України . - Київ, 2018. - 374 с.

Зі змісту:

- Анісімова М. Міжнародне партнерство – інструмент забезпечення національної кібербезпеки України.

Шифр зберігання НБУВ: ВА836868

***

Самойленко О. А. Типові слідчі ситуації наступного етапу розслідування злочинів, скоєних у кіберпросторі / О. А. Самойленко // Актуальні проблеми держави і права. - 2019. - Вип. 82. - С. 188-194.

Визначено типові слідчі ситуації наступного етапу розслідування злочинів, скоєних у кіберпросторі. На підставі узагальнення матеріалів кримінальних проваджень про такі злочини констатовано про наявність слідчої та слідчо-розшукової моделі таких ситуацій розслідування. Встановлено критерії, що покладаються в основу типізації таких ситуацій.

Шифр зберігання НБУВ: Ж69995

***

Самойленко О. А. Типові слідчі ситуації початкового етапу розслідування злочинів, вчинених у кібепросторі / О. А. Самойленко // Наукові праці Національного університету «Одеська юридична академія». - 2019. - Т. 23. - С. 121-128.

Запропоновано типові слідчі ситуації, що характеризуються наявністю персоналізованих відомостей про користувача як злочинця. Їх розглянуто на прикладі конкретних кримінальних проваджень у комплексі з тактичними завданнями та засобами їх вирішення.

Шифр зберігання НБУВ: Ж72103