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

№ 1 (січень)

Київ – 2020

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І.Вернадського. – К., 2020. – №1 (січень) . – 82с.

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

«Один из крупных украинских банков «засветил» в открытом доступе банковские данные своих клиентов. Данные доступны «благодаря» расшареной папке, обнаруженной через открытый всем желающим Wi-Fi с именем банка.

Об этом на своей странице в Facebook сообщил известный украинский эксперт по кибербезопасности, ведущий разработчик компании ИТ-Лаборатория Александр Галущенко…

На данный момент эксперт не опубликовал информацию о том, какой именно банк «засветил» данные, поскольку доступная информация, по его словам, оказалась «очень чувствительной».

– Информация ОЧЕНЬ чувствительная, поэтому пока ответов на вопросы «откуда, какой банк» не будет. Зато на вопрос «как получили» есть ответ: открытый Wi-Fi с именем банка, а там – расшаренная папка, – сообщил Галущенко. – Очень хочется получить ответ, что делать дальше: забыть, как бессмысленное направление, или добить эту финансовую организацию до конца. По опыту после публикаций в рамках #FRD обычно ничего не происходит: все «на морозе», с умным видом сообщают, что сами обнаружили, закрыли, а публикация – это так, ерунда от школьников. И, в то же время, пишут заявления куда только можно…

Как стало известно, о том, что данные банковской структуры находятся в открытом доступе, стало известно и сообщалось ещё год назад, но никакой реакции от финансового учреждения не последовало…». ***(Владимир Кондрашов. Один из крупнейших украинских банков слил в сеть персональные данные своих клиентов // Internetua (http://internetua.com/odin-iz-krupneishih-ukrainskih-bankov-slil-v-set-personalnye-dannye-svoih-klientov). 19.01.2020).***

***

«Открытые для чтения и записи папки с документами одного из подразделений регионального центра занятости были обнаружены хактивистами в открытом доступе. Всем желающим была открыта практически вся документация госструктуры за последние 9 лет, а диски как минимум несколько раз шифровали злоумышленники, требуя выкуп, но чиновников это ничему не научило. На одном устройстве, кроме, собственно, документов Центра занятости, также находится отчетность и рабочие данные компании, связанной с крупным ресторанным бизнесом.

Об этом в рамках флешмоба #fuckresponsibledisclosure, направленного на выявление и публичное оповещение об уязвимостях государственных информационных ресурсов, сообщил известный украинский эксперт по кибербезопасности, ведущий разработчик компании ИТ-Лаборатория Александр Галущенко.

Были обнаружены «проблемы» (если халатность можно так охарактеризовать) с безопасностью одного из подразделений Херсонского областного центра занятости.

– В диапазоне IP-адресов «Укртелекома» в районе часа дня увидели очень яркий хост с огромным количеством торчащих наружу расшаренных папок с

разрешением на запись. 11 всего и 7 на запись. На выходе имеем госструктуру и компанию, уверенно чувствующую себя в ресторанном бизнесе. Смотрите картинки. Одна даже есть с грифом «Для служебного пользования». На общем компе, – написал Александр Галущенко.

Как отметил эксперт, странным в ситуации выглядит не то, что данные госструктуры оказались в сети (за три года проведения флешмоба #fuckresponsibledisclosure, о котором мы неоднократно писали, это не редкость), а то, что рядом с этими данными хранится информация о частной компании:

– Мы часто находим расшаренные папки, открытые FTP, пароли в самих веб страницах и все такое. Но тут вариант несколько отличается. На одной машине находится практически вся документация с центра занятости с 2010 года и одной из серьезных коммерческих фирм. Непонятно: или админ сделал бэкап, или кто-то «подрезал» информацию, или в одном помещении, вместе и с озорным рвением работает госслужащий и он же – удачливый бизнесмен, – резюмирует Александр Галущенко.

Как именно и зачем эта информация оказалась вместе, а также почему позже «всплыла» в открытом доступе – неизвестно. К слову, Херсонский областной центр занятости не так давно искал «специалиста по информационным технологиям» на зарплату в 3800 гривен». ***(Владимир Кондрашов. Чиновников поймали на игнорировании правил информационной безопасности // Internetua (http://internetua.com/csinovnikov-poimali-na-ignorirovanii-pravil-informacionnoi-bezopasnosti). 09.01.2020).***

***

«В Раді національної безпеки і оборони України організували роботу щодо виявлення вразливостей, подолання її наслідків та забезпечення сталої роботи Єдиного порталу вакансій…

Вказано, що члени робочої групи розглянули питання щодо вразливості Єдиного порталу вакансій Національного агентства України з питань державної служби, що призвело до витоку частини персональних даних українських громадян….

Також у ході засідання було наголошено на важливості питань кібербезпеки у процесах цифрової трансформації держави та необхідності забезпечення органами державної влади належного кіберзахисту власних інформаційних систем…». ***(Дар'я Панченко. В РНБО налагодили роботу Єдиного порталу вакансій // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1847080-v-rnbo-nalagodili-robotu-yedinogo-portalu-vakansiy). 17.01.2020).***

***

«Для посилення безпеки планують змусити кожного користувача Інтернету авторизуватися

Спецслужби наголошують на наявності величезних проблем у сфері кібербезпеки держави. Тож вони поділилися думками, що планують робити, аби зберегти дані державних реєстрів у цілісності та безпеці.

Щодня ми користуємося банківськими картками, смартфонами та Інтернетом. Водночас законодавство, яке повинне створювати безпечні умови для користувачів, безмежно застаріло, адже було створене понад 10 років тому. Тож у Міністерстві цифрової трансформації вирішували, як захищати державу від хакерів.

У комітетських слуханнях узяли участь народні депутати з парламентських комітетів з питань національної безпеки та оборони, правоохоронної діяльності, гуманітарної та інформаційної політики, представники центральних органів державної влади, об'єднань громадян, бізнесу, неурядових організацій, провідні експерти та вчені.

Відкриваючи слухання, заступник голови комітету, голова підкомітету цифрової інфраструктури, електронних комунікацій та смарт-інфраструктури Олександр Федієнко зазначив, що актуальність проведення слухань викликана тим, що сьогодні кожен стикається з необхідністю користування інформаційними технологіями. Це стосується соціальних мереж, банкоматів, банківських рахунків, платіжних систем тощо. «В Україні вже багато років ведеться мова про реформи для покращення життя кожного з нас. Цифрова трансформація суспільства, проголошена одним із пріоритетів Президента, може, і повинна стати базовою умовою для такого покращення», — зазначив він…

Практичні кроки напрацьовує Рада національної безпеки та оборони. Водночас нормативні акти, які приймаються, — недоступні для пересічного користувача. Як висловилися під час слухання в комітеті, «щоб вороги не знали про наші кроки». Проте, як стало відомо, основні зміни націлені на покращення взаємодії між силовими структурами, які задіяні в убезпеченні державних інтересів і громадян від хакерів та міжнародної кіберзлочинності.

Натомість розв'язати всі наявні в державі проблеми неможливо, адже, як завжди, не вистачає коштів. Через це все більше уваги буде приділятися державно-приватному партнерству. Тож замість того, щоб на належному рівні фінансувати відповідні заходи, такий обов'язок перекладуть на приватний бізнес.

Наступною проблемою є відсутність належної термінології та законодавства. Адже, незважаючи на те, що проект закону «Про захист критичної інфраструктури» вже докрокував до парламенту, монобільшість не квапиться з прийняттям настільки важливих рішень. Замість цього планують покращити взаємодію з науковими установами та якісніше готувати фахівців.

Водночас правоохоронці скаржаться на постійний відплив кадрів. Адже приватні структури готові створювати і кращі умови, і платити адекватну зарплату. Через це фактично держава готує кваліфікований персонал «на виїзд»…

О.Федієнко також поінформував про прогнози експертів на 2020 рік. За його словами, все більше кіберзлочинців використовують штучний інтелект для масштабування своїх атак. «Особливо важливо те, що традиційні антивірусні рішення не працюють, тобто шкідливе навантаження може вільно спричинити хаос у цифрових системах. Наступного року ми побачимо нові спроби злочинців атакувати об'єкти з відкритим кодом. Буде зростати потреба в таких процесах, як фонові перевірки розробників та відкриті джерела розробників. На даний час середовище з відкритим кодом повністю базується на довірі. Організації, як правило, не верифікують попередніх проектів», — додав він.

Також представники силових відомств висловилися за необхідність проведення комплексного перегляду всього законодавства щодо питань інформаційної безпеки з метою створення системи узгодження та гармонізації в законах питань, які не суперечили б один одному та не залишали білих плям. Неможливо здійснювати масштабні та системні захисти в будь-якій сфері без знання її стану, без знання статистичних відповідних процесів. Тому в державі необхідно побудувати всеосяжну систему регулярної оцінки стану кібербезпеки, постійного моніторингу та спостереження кіберінцидентів на основі надійних даних.

Такі дані планують отримувати з усіх можливих джерел. Зокрема, на парламентському рівні обговорюються питання необхідності тотальної ідентифікації всіх абонентів інформаційних мереж. Для пересічного громадянина це може перетворитися на ще більше посилення контролю з боку держави. Зокрема, операторів зв'язку змусять продавати картки за паспортом, а неліцензоване програмне забезпечення хочуть поступово виводити з обігу.

Наразі не відомо, чи наберуться депутати сміливості йти так далеко у власних законодавчих ініціативах. Адже в Україні майже відсутні фахівці, які вміють та здатні знаходити вразливість безпеки в програмному забезпеченні. Як стверджують фахівці, єдиним адекватним кроком для забезпечення хоча б внутрішньодержавної безпеки є створення вітчизняного програмного забезпечення.

Зрозуміло, що через брак коштів українських операторів зв'язку планують змусити перебрати на себе ряд виключно державних функцій. Водночас викликає подив те, що компанії, які були замішані в шпигунських скандалах, відчувають себе в українському парламенті наче вдома…

Так, на нараду, яку проводило міністерство, були запрошені представники компанії Huawei, скандал навколо якої розгорівся навесні цього року. Зокрема, у Вашингтоні звинуватили гіганта в шпигунстві на користь Китайської Народної Республіки. Після цього Huawei потрапила до чорного списку компаній, з якими заборонено працювати.

Водночас китайська експансія на ринку була настільки всеосяжною до цього моменту, що відмовитися від співробітництва були здатні далеко не всі. Через це дію санкцій зупинили до лютого 2020 року. Натомість Сполучені Штати активно закликають інші держави припинити співробітництво з Huawei через величезні загрози національній безпеці. Підтримати власну державу в прийнятих рішеннях вирішила й корпорація Google, адже спеціального дозволу на співробітництво зі східним партнером вони вирішили не отримувати.

Водночас присутній на засіданні представник Huawei наголосив на зацікавленості в подальшому співробітництві з Україною. Він зазначив, що Китай є надійним партнером, який може поділитись і досвідом, і технологіями. Адже Україна є великим та потужним ринком.

Як зазначають фахівці з кібербезпеки, нині вже 2/3 обладнання, яке працює в системі спецзв'язку, має китайське походження. Водночас це створює великі ризики для обміну інформацією з країнами Європейського Союзу, які, хоч досі й тримають ноту мовчання, проте навряд чи будуть зацікавлені в тому, щоб давати доступ до власних даних країнам із закритим програмним кодом.

Представники українських операторів зв’язку зайвих витрат не злякались, адже вони й без того щорічно несуть величезні збитки. Перш за все їх турбує бездіяльність Національної поліції, яка поки що не здатна протидіяти крадіжкам обладнання та кабелів. Тому першим кроком у системі реального захисту повинна бути зміна законодавства та узгодження його з європейськими стандартами.

І це повинно бути наскрізною дією, адже одним підвищенням санкцій за злочини, скоєні проти кібербезпеки, докорінно ситуацію не змінити. Наступним кроком є ратифікація конвенцій та перехід від радянської кальки «забезпечення безпеки» до надання сервісних функцій. Зважаючи на швидкий розвиток онлайн-платежів та цифровізацію економіки, без адекватного законодавства ні бізнес-середовище, ні правоохоронці не зможуть убезпечити громадян від величезних ризиків.

Наприкінці засідання присутні погодилися з тим, що головна небезпека — між комп’ютером і стільцем, тож без навчання громадян основам цифрової гігієни «держава в смартфоні» стане найбільшим розчаруванням українців. Адже, доки ми не створимо вітчизняного програмного продукту належної якості, Україна так і залишиться буферною зоною, в якій одні будуть відпрацьовувати стратегію наступу, а європейські партнери — захисту. Громадяни ж залишаться пішаками на шаховій дошці, які не мають ні захисту, ні приватності». ***(Аміна БЕКМІРЗАЄВА. Зникла приватність // Закон і Бізнес (https://zib.com.ua/ua/140713-dlya_posilennya_bezpeki_planuyut_zmusiti_kozhnogo_koristuvac.html). 10.01.2020).***

***

«Зазначається, що кібератака відбулась 14 січня, але хакерам не вдалося отримати доступ до персональних даних користувачів.

Про це повідомляє пресслужба Української кіноакадемії.

«Інформуємо, що 14 січня 2020 року онлайн платформа DzygaMDB, на якій багато з вас мають профайли, зазнала хакерської атаки, внаслідок якої було пошкоджено базу даних сайту. Зловмисники хоч і втрутились в роботу сервісу, але їм не вдалося отримати доступ до персональних даних користувачів. Джерело атаки невідоме», - йдеться в повідомленні.

В Українській кіноакадемії додали, що спеціалістам DzygaMDB не вдалося повністю відновити втрачені дані за період з 8 грудня 2019 року по 14 січня 2020 року.

«Адміністрація DzygaMDB просить усіх користувачів платформи перевірити власні профілі та проєкти, що було внесено», - зазначили в пресслужбі». ***(Хакери пошкодили базу даних онлайн-платформи DzygaMDB // Інтернет-видання «Детектор медіа» (https://detector.media/infospace/article/173937/2020-01-15-khakeri-poshkodili-bazu-danikh-onlain-platformi-dzygamdb/). 15.01.2020)***.

***

«У Військовому інституті телекомунікацій та інформатизації імені Героїв Крут розпочались тримісячні курси з кіберзахисту для офіцерів підрозділів та частин військ зв'язку ЗСУ.

Тут готуватимуть молодших офіцерів задля зміцнення і розвитку системи кіберзахисту на тактичному й оперативно-тактичному рівні: від військової частини до оперативного угруповання, повідомляє АрміяInform.

"Офіцери, які пройдуть курс, мають отримати додаткові навички кіберзахисту і набути спроможностей з ефективного реагування на сучасні кіберінциденти та виклики. Курс має донести до слухачів результати досліджень та досвід європейських організацій, таких, як SANS, MITRE, NIST у забезпеченні кібербезпеки на об'єктах критичної інфраструктури держави, зміцненні у військах єдиного розуміння принципів побудови системи кібербезпеки і основ кіберзахисту", - розповів професор кафедри захисту інформації та кіберзахисту полковник Олег Мазулевський.

Цей курс - перший, спрямований на набуття практичних навичок з кіберзахисту, розроблений спеціально для офіцерів частин та підрозділів військ зв'язку.

"Курс враховує досвід європейських організацій, які готують фахівців кіберзахисту. Участь у розробці курсу брали науково-педагогічні працівники інституту та кафедри автоматизованих систем управління та кафедри комп'ютерних інформаційних технологій нашого інституту. Враховувалися напрями підготовки міжнародних інститутів, де готують не тільки цивільних фахівців, а й спеціалістів військових підрозділів, зокрема й для Збройних Сил США", - зазначив Мазулевський

Аудиторні заняття триватимуть один місяць. Це та частина, яка має відбуватися під наглядом викладачів. Потім передбачено два місяці роботи в пунктах постійної дислокації.» ***(Українських офіцерів вчать захищатись від хакерів // Багнет (http://www.bagnet.org/news/society/417145/ukrayinskih-ofitseriv-vchat-zahishchatis-vid-hakeriv). 28.01.2020).***

***

Національна система кібербезпеки

«Голова ЦВК Олег Діденко розповів, які кошти було витрачено на кібербезпеку інформаційних ресурсів ЦВК…

“На кінець 2018-го і протягом 2019-го року на підвищення рівня кіберзахисту інформаційних ресурсів ЦВК витрачено майже 30 мільйонів гривень”, – сказав він.

Крім того, за словами Діденка, було витрачено понад 9,5 мільйона гривень для посилення захисту автоматизованої системи “Державний реєстр виборців”. У наступному році на це планується витратити ще більш як сім мільйонів.

Також у 2020 році на підвищення рівня безпеки планується витратити ще більш як десять мільйонів гривень.

Водночас голова ЦВК заявив, що система кіберзахисту є “живим організмом”, який постійно вдосконалюється.

“Це нескінченний процес і у нас в цьому плані відбуваються постійні закупівлі та оновлення як апаратних засобів, тобто техніки, так і програмного забезпечення. Світ розвивається, технології розвиваються”, – пояснив він». ***(Глава***

ЦВК розповів, скільки витратили на кібербезпеку // Баба Клава дает добро (https://blin.mk.ua/news/118563). 11.01.2020).

***

«Секретар Ради національної безпеки і оборони Олексій Данілов вважає, що указ Президента про збільшення граничної чисельності працівників апарату РНБО дозволить суттєво посилити можливості Національного координаційного центру кібербезпеки. Про це повідомляє прес-служба РНБО.

"Указ президента України дозволить суттєво посилити можливості Національного координаційного центру кібербезпеки", - зазначив Данілов.

Так, згідно з Указом президента України від 28.01.2020 № 27/2020 "Про внесення змін до Указів президента України від 27 січня 2015 № 37 та від 7 червня 2016 № 242", граничну чисельність працівників Апарату Ради національної безпеки і оборони України збільшено на 30 осіб.

Згідно з указом Зеленського, тепер апарат РНБО може складатися з 190 співробітників.

Указом працівники Апарату Ради здійснюватимуть інформаційно-аналітичне, експертне, організаційне, матеріально-технічне та інше забезпечення діяльності Національного координаційного центру кібербезпеки.

"Враховуючи стратегічне значення, яке набувають питання кібербезпеки в системі національної безпеки України і в світі, діяльність Національного координаційного центру кібербезпеки стає одним з ключових у роботі РНБО України, і його завдання значно розширені відповідно до вимог часу", - прокоментував підписання Указу Данілов…» ***(Зеленський збільшив апарат РНБО до 190 осіб // Дзеркало тижня. Україна (https://dt.ua/POLITICS/zelenskiy-zbilshiv-aparat-rnbo-do-190-osib-336933_.html). 28.01.2020).***

***

Кібервійна проти України

«Служба безпеки України у межах реалізації комплексу заходів з протидії кіберзлочинності виявила та припинила діяльність хакерського угруповання, що здійснювало кібератаки на органи влади та управління України, об'єкти критичної інфраструктури України, банківські установи України та світу…

Під час проведення слідчих дій оперативники спецслужби затримали у Вінниці організатора угрупування, який з 2011 року надавав власне серверне обладнання для розміщення, адміністрування та розповсюдження членами угруповання та третіми особами шкідливого програмного забезпечення, бот-мереж та проведення кібератак, у тому числі DDoS-атак на стратегічні об'єкти на території України та банківські установи інших держав.

Зазначений "абузостійкий хостинг" був відомий в мережі Darknet під назвою ProHoster та Bulletproof.space.

Крім того стало відомо, що для безперешкодного провадження своєї діяльності члени угруповання налагодили корумповані зв'язки з окремими представниками правоохоронних органів та органів влади України. У ході проведення досудового розслідування було встановлено, що організатор хакерського угруповання свідомо надавав власне серверне обладнання для проведення кібератак на іноземні комерційні підприємства. Він також розміщував шахрайські ресурси, віруси-вимагачі, веб-ресурси, через які розповсюджувались вилучені з цивільного обігу об'єкти.

Наразі тривають невідкладні слідчі дії у межах кримінального провадження за ознаками злочину, передбаченого ч. 3 ст. 301 Кримінального кодексу України.Трьом особам оголошено про підозру у вчиненні вищезазначеного правопорушення.

Організатора протиправної діяльності затримано згідно зі ст. 208 Кримінального процесуального кодексу України та обрано запобіжний захід у вигляді тримання під вартою з можливістю внесення застави у розмірі 60 неоподаткованих мінімумів доходів громадян України.

Вилучене під час обшуків комп'ютерне обладнання направлено на проведення відповідних експертних досліджень…». ***(Валерія Гуржий. В Україні затримали групу хакерів, які атакували держоргани, об'єкти інфаструктури та банки // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1847024-v-ukrayini-zatrimali-grupu-khakeriv-yaki-atakuvali-derzhorgani-organi-infastrukturi-ta-banki). 17.01.2020).***

***

«У 2019 році фахівці Служби безпеки України нейтралізували пів тисячі кібератак на державні органи та критичну інфраструктуру.

Про це повідомляє пресслужба СБУ.

«Служба безпеки України комплексно та оперативно протидіє кіберзлочинності та гібридній агресії проти нашої країни через інтернет мережу. Так у 2019 році фахівці СБУ з інформаційної безпеки нейтралізували понад 480 кіберінцидентів та кібератак на органи державної влади та об'єкти критичної інфраструктури. За цей період також припинено функціонування більше ніж 1000 вебресурсів, що використовувались у злочинних цілях», – йдеться у повідомленні.

Також зазначається, що загалом у минулому році за напрямом контррозвідувального захисту інтересів держави у сфері інформаційної безпеки розпочато 339 кримінальних проваджень, серед них: 158 за злочини у сфері використання комп'ютерних систем (ст. 361, ст. 362 Кримінального кодексу України) та 34 за злочини проти основ національної безпеки (ст. 109, ст. 110 ККУ).

Крім того повідомляється, що фахівці СБУ ефективно співпрацюють із колегами з країн ЄС і НАТО для зміцнення колективної безпеки в інформаційному просторі та підвищення захищеності державних і фінансових структур щодо кіберзагроз.

«Так улітку 2019 року Служба спільно з партнерами зі США та Великої Британії припинила діяльність потужного хакерського угруповання, що сприяло протиправній діяльності в мережі Інтернет злочинцям по всьому світу.

Зловмисники, зокрема, забезпечували функціонування майже 40% російськомовного сегменту DarkNet», – зауважують у повідомленні.

У СБУ наголошують, що підрозділи контррозвідувального захисту інформаційної безпеки системно протидіють злочинній діяльності міжнародних хакерських угруповань, які спецслужби іноземних держав використовують на шкоду національній безпеці України. У минулому році Служба безпеки викрила 20 таких груп.

«На Дніпропетровщині СБУ припинила діяльність підконтрольного ФСБ РФ угруповання хакерів, яке напередодні парламентських виборів здійснювало масовані кібератаки на українські державні установи», – інформують в СБУ.

Згідно з повідомленням, спільно з Державною фіскальною службою СБУ викрила схему незаконного втручання до інформаційної бази даних Держаної податкової служби України. Скориставшись вразливостями системи зловмисники допомагали «конвертаційно-транзитним» групам ухилятись від сплати податків у особливо великих розмірах.

В СБУ наголошують, що комплексно протидіють несанкціонованим втручанням у роботу реєстрів Міністерства юстиції. Так у 2019 році було блоковано діяльність організованого угруповання чорних реєстраторів, яке сприяло рейдерським захопленням майна по всій Україні.

Фахівці СБУ із кібербезпеки також проводять заходи із виявлення та припинення деструктивної діяльності бот-мереж, підконтрольних іноземним спецслужбам. Ці ресурси використовують для інспірування конфліктів в середині країни та маніпулювання громадською думкою.

Зокрема, у грудні Служба безпеки блокувала роботу потужної »ботоферми», послугами якої користувались представники спецслужб РФ та бойовики терористичних «Л/ДНР». Через ресурс, зокрема, поширювали антиукраїнські матеріали та здійснювали спам-розсилку про фейкові мінування об’єктів у різних містах України.

СБУ викрила схему використання спецслужбами РФ псевдопатріотичних спільнот у соціальних мережах для розхитування внутрішньополітичної ситуації в Україні.

Загалом за минулий рік за матеріалами Служби безпеки 34 сепаратистські адміністратори соцмереж були притягнені до відповідальності за поширення антиукраїнської пропаганди та протиправного контенту. Набув законної сили 21 судовий вирок.

Крім того, майже 280 іноземцям, причетним до пропаганди сепаратизму в інтернеті, заборонено в’їзд в Україну». ***(СБУ торік нейтралізувала пів тисячі кібератак на державні органи // Українські медійні системи (https://glavcom.ua/country/incidents/sbu-torik-nejtralizuvala-piv-tisjachi-kiberatak-na-derzhavni-organi-655087.html). 25.01.2020).***

***

«У 2019 році урядова команда реагування на комп’ютерні надзвичайні події України зареєструвала 330 кіберінцидентів, пов’язаних з кібератаками на сайти органів державної влади України…

“За 2019 рік CERT-UA зареєструвала 330 кіберінцидентів, пов’язаних з кібератаками на сайти органів державної влади України”, — зауважили у Держспецзв’язку.

У пресслужбі зауважили водночас, що інформація щодо конкретного переліку міністерств та кількості зафіксованих кібератак на їх сайти становить інформацію з обмеженим доступом…». ***(На сайти органів влади України за рік було більше 300 кібератак // Рубрика (https://rubryka.com/2020/01/23/na-sajty-organiv-vlady-ukrayiny-za-rik-bulo-bilshe-300-kiberatak/). 23.01.2020).***

***

Боротьба з кіберзлочинністю в Україні

«Департамент кіберполіції Нацполіції розпочав кримінальне провадження після повідомлень в американський ЗМІ про те, що російські хакери намагалися зламали сайти кількох українських компаній, зокрема Burisma Holdings та студії «Квартал 95».

Про це повідомила пресслужба Міністерства внутрішніх справ…

Кримінальне провадження порушили за ч. 2 ст. 163 (порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції) і ч. 2 ст. 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України.

Українські поліцейські також звернулися до Федерального бюро розслідувань США та компанії Area1, що виявила ознаки хакерської атаки. Їх попросили надати опубліковані в американських ЗМІ матеріали. Нацполіція також ініціює створення спільної міжнародної слідчої групи, до якої запросять представників ФБР…». ***(Нацполіція відкрила кримінальне провадження щодо хакерської атаки на сайти Burisma і "Квартал 95" // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (https://day.kyiv.ua/uk/news/160120-nacpoliciya-vidkryla-kryminalne-provadzhennya-shchodo-hakerskoyi-ataky-na-sayty-burisma). 16.01.2020).***

***

«Служба безпеки України блокувала діяльність хакерського угруповання у Вінниці. Як повідомляє пресслужба СБУ, хакери спеціалізувалися на наданні послуг «абузостійкого» хостингу.

Їхнє серверне обладнання використовувалося членами групи та третіми особами для здійснення кібератак на органи влади України, об’єкти критичної інфраструктури, банківські установи України та світу.

У Вінниці затримано організатора угрупування, який з 2011 року надавав власне серверне обладнання для розміщення, адміністрування та розповсюдження шкідливого програмного забезпечення, бот-мереж та проведення кібератак, у тому числі DDoS-атак. Зазначений «абузостійкий хостинг» був відомий в мережі Darknet за назвами «ProHoster» та «Bulletproof.space».

Також відомо, що для безперешкодної діяльності група налагодила корумповані зв’язки з представниками правоохоронних органів та органів влади України.

Наразі тривають слідчі дії у межах кримінального провадження за ознаками злочину, передбаченого ч. 3 ст. 301 Кримінального кодексу України. Трьом особам оголошено про підозру у вчиненні вищезазначеного правопорушення.

Організатора помістили під варту з можливістю внесення застави у розмірі 60 неоподаткованих мінімумів доходів громадян України (близько тисячі гривень).

Вилучене під час обшуків комп’ютерне обладнання направлено на проведення відповідних експертних досліджень…». ***(У Вінниці хакери обслуговували кібератаки // iVin (http://i-vin.info/news/u-vinnytsi-khakery-obslugovuvaly-kiberataky-32548). 17.01.2020).***

***

«Понад 300 електронних адрес наркокрамниць заблокувала поліція за допомогою чат-боту "Стоп наркотик". Про це повідомили в МВС під час презентації цього додатку. Його розробили в харківському університеті внутрішніх справ. Це програма, яка дозволяє правоохоронцям систематизувати наркоадреси.

Діє чатбот через месенджер Telegram. Допомогти поліції блокувати наркоадреси можуть всі охочі. Для цього потрібно завантажити додаток на свій смартфон.

"На даний час інтернет мережу використовують як платформу для розповсюдження наркотиків. У зв'язку з цим факультетом кіберполіції Харківського університету внутрішніх справ створено безкоштовний чатбот "Стоп наркотик". Мрія для блокування телеграмм каналів через які здійснюється продаж наркотичних засобів", - говорить Олександр Гогілашвілі, Заступник міністра внутрішніх справ.

"Зараз, коли у нас уже 18,5 тисяч користувачів, які щоденно допомагають блокувати набагато більше, то на блокування однієї адреси уходить година-три години. І з такою швидкістю ми дуже швидко будемо блокувати наркоадреси", - говорить Денис Дацюк, курсант Харківського національного університету внутрішніх справ.» ***(МВС презентувало бота для полювання на наркокрамниці // ООО "Национальные информационные системы" (https://podrobnosti.ua/2334602-mvs-prezentuvalo-bota-dlja-poljuvannja-na-narkokramnits.html). 17.01.2020).***

***

«В Одесі затримали студента, який використовував вірус заради прихованого майнінгу криптовалюти…

Працівники кіберполіції в Одеській області спільно зі слідчими одеської поліції, за процесуального керівництва Одеської місцевої прокуратури №3, викрили в таких діях 20-річного студента одного з місцевих вишів.

Кіберполіція встановила: здобуваючи технічну освіту, молодик використовував отримані знання для вчинення протиправних дій. Будучи учасником хакерських форумів, він придбав шкідливе програмне забезпечення та модифікував його. Вірус призначався для прихованого майнінгу криптовалюти за

допомогою потужностей інфікованої комп'ютерної техніки. Надалі він збував це шкідливе програмне забезпечення на хакерських форумах.

Поліцейські провели обшук за місцем проживання одесита та вилучили комп'ютерну техніку. Її направлено на експертизу.

Кримінальне провадження розпочато за ст.361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) КК України. Наразі чоловіку вже оголошено про підозру. Санкція статті передбачає позбавлення волі на строк до п'яти років…». ***(Валерія Гуржий. В Одесі кіберполіція затримала хакера за розповсюдження шкідливого програмного забезпечення // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1848135-v-odesi-kiberpolitsiya-zatrimala-khakera-za-rozpovsyudzhennya-shkidlivogo-programnogo-zpbezpechennya). 23.01.2020).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Дональд Трамп, президент Сполучених Штатів Америки, планує обговорити кібератаки на сайт української компанії Burisma з президентом Росії Володимиром Путіним.

Питання хакерської атаки буде підняте, коли американський та російський президент розмовлятимуть найближчим часом. Про це 16 січня заявила радник Білого дому Келліан Конвей, повідомляє Reuters.

Президент США Дональд Трамп може обговорити інформацію про злом української енергетичної фірми Burisma в наступний раз, коли він буде розмовляти з президентом Росії Володимиром Путіним, — заявила Конвей…». ***(Трамп планує обговорити з Путіним кібератаки на сайт Burisma // Ракурс (https://racurs.ua/ua/n132184-tramp-planuie-obgovoryty-z-putinym-kiberataky-na-sayt-burisma-reuters.html). 16.01.2020).***

***

«Україна та НАТО домовилися про нові спільні військові навчання «Непорушна стійкість – 2020», що відбудуться 5-9 жовтня в акваторії Чорного моря.

Про це повідомили в інформаційному агентстві Міністерства оборони України АрміяІнформ.

Зазначається, що відповідну угоду вже підписали представники Північно-атлантичного альянсу та українського уряду у Брюсселі.

Участь у навчаннях «Непорушна стійкість – 2020» (Coherent Resilience 2020) візьмуть кілька тисяч військових країн-учасниць НАТО.

Разом із українськими армійцями вони відпрацюють аглоритм дій у кризових ситуаціях, які можуть виникнути в Чорноморському регіоні.

Загалом же до України має приїхати понад 200 інструкторів. Вони навчатимуть не лише, як протистояти збройній агресії, але й протидіяти кіберзагрозам.

Мета – злагоджено, вчасно і грамотно реагувати на кібератаки, напади на порти, захоплення транспортних шляхів та інші загрози…

Оцінюватиме взаємодію Вища морська школа США. За результатами навчань вони оцінять сильні і слабкі сторони взаємодії, а детальний аналіз і рекомендації нададуть на початку 2021 року…». ***(Україна та НАТО проведуть спільні військові навчання в акваторії Чорного моря // #ШоТам (https://shotam.info/ukraina-ta-nato-provedut-spil-ni-viys-kovi-navchannia-v-akvatorii-chornoho-moria/). 16.01.2020).***

***

«Україна і Японія провели консультації з кібербезпеки і обговорили практичні аспекти двосторонньої співпраці в цій галузі. Про це повідомляє прессслужба Ради національної безпеки і оборони України.

Згідно з повідомленням, сьогодні, 23 січня, у Токіо відбувся другий тур консультацій. До складу української делегації на чолі із заступником секретаря РНБО України Сергієм Демедюком увійшли представники МЗС України та СБУ.

Сторони розглянули питання огляду національних стратегій з кібербезпеки та обговорили останні інциденти у кіберпросторі.

"Це вже другий раунд українсько-японських консультацій з кібербезпеки. Таке двостороннє співробітництво сьогодні дає нам можливість побудувати більш чіткий план подальшого руху в напрямку покращення систем та заходів з реагування на майбутні загрози", - заявив заступник секретаря РНБО Сергій Демедюк.

На завершення першого дня консультацій сторони домовилися про взаємодію компетентних органів двох держав щодо побудови відкритого, операційно-сумісного, надійного та безпечного кіберпростору…». ***(Україна і Японія обговорили співпрацю у сфері кібербезпеки // Західна інформаційна корпорація (https://zik.ua/news/2020/01/23/ukraina_i_yaponiia_obhovoryly_spivpratsiu_u_sferi_kiberbezpeky_956384). 23.01.2020).***

***

«Топ-менеджмент американской компании McAfee 6 февраля приедет в Киев для проведения крупнейшего форума по кибербезопасности в Европе McAfee Cybersecurity Forum 2020. Локальную поддержку в проведении обеспечивает международная группа компаний БАКОТЕК - официальный дистрибьютор McAfee в Украине, Республике Беларусь, Азербайджане, Грузии, Армении.

Решения McAfee за годы работы компании успели выбрать такие клиенты, как Coca-Cola, Sony, General Motors, British American Tobacco, ФБР, ЦРУ, Лукойл, УкрТатНафта, Golden Telecom и многие другие.

Особенностью данного форума в Киеве станет всестороннее рассмотрение инструментов безопасности McAfee: как с точки зрения разработчика и интеграторов продуктов, так и со стороны тех украинских компаний-клиентов, которые уже внедрили решения в своих организациях.

Так, специалисты McAfee, БАКОТЕК, Softlist, Netwave, OptiData,ITIS раскроют технические нюансы защиты информации на всех этапах ее жизненного цикла, построения операционного центра безопасности в компании (SOC),

практике использования адаптивной защиты, примеры внедрения комплекса защиты рабочих станций корпоративной сети и многое другое. Специалисты ИБ из компаний-клиентов в свою очередь расскажут собственные кейсы внедрения решений McAfee у себя в организациях в ходе специального интервью после основной части докладов.

Посетители McAfee Cybersecurity Forum 2020 узнают о:

Решении класса “песочница” как ядре системы информационной безопасности по защите сетевого, почтового и веб-трафика

MVISION EDR — ключевом инструменте современного SOC для расследования инцидентов с возможностями мониторинга, обнаружения и реагирования на сложные угрозы на конечных точках

Построении архитектуры адаптивной безопасности для предотвращения сложных и целенаправленных атак согласно рекомендациям ведущих международных аналитических агентств (Gartner, Forrester и др.)

MVISION Cloud (CASB) — обеспечении защиты информации на всем пути от устройств к облаку (Device-to-Cloud Security)

Элементах и подходах по построению современного SOC, ядром которого является система управления событиями информационной безопасности (SIEM) с возможностью автоматического реагирования

McAfee MVISION — семействе облачных продуктов, обеспечивающих защиту данных и блокирующих угрозы безопасности на устройствах, в сетях, в облачных (IaaS, PaaS, SaaS) и локальных средах...» ***(Эволюция инструментов кибербезопасности в 2020: в Киеве пройдет крупный форум McAfee // PaySpace Magazine (https://psm7.com/security/evolyuciya-instrumentov-kiberbezopasnosti-v-2020-v-kieve-projdet-krupnyj-forum-mcafee.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Payspacemagazine+%28Payspacemagazine%29). 20.01.2020).***

***

Світові тенденції в галузі кібербезпеки

«ООН прийняла резолюцію, яку висунула Росія. Проти документу виступали Сполучені Штати Америки…

МЗС Росії пояснив, що резолюція, фактично, "закріплює цифровий суверенітет держав над своїм інформаційним простором і відкриває нову сторінку у історії глобального протистояння кіберзлочинності". Також, представник РФ при ООН Геннадій Кузьмін додав, що на основі резолюції буде створений спеціальний експертний спецкомітет, який "буде приймати до уваги результати роботи віденської групи експертів з кіберзлочинності", результати якого мають надійти у 2020 році.

Ціль створення цього спеціального органу, на думку Росії – розробка міжнародної конвенції протистояння злочинам у Всесвітній мережі. Під проєктом підписалося 47 країн-членів, серед них КНДР (яка, за останніми даними, отримує 2 млрд дол. тільки на хакерських атаках), Китай (який створює власний

цензурований Інтернет), Сирія, Куба, Венесуела, Білорусь, Іран (де Інтернет нещодавно повністю вимкнули під час масових протестів) та інші “сателіти” РФ.

"Росіяни дійсно зацікавлені у просуванні свого бачення, як має виглядати інтернет майбутнього. І це точно не про боротьбу з кіберзлочинами, а радше про кіберконтроль. Росія хоче припинити вільний витік інформації ", - заявив представник Держдепу США на брифінгу для медіа 19 грудня.

Глобально, ідея Росії має протистояти Конвенції Будапешту, за якою стоять США і де країни закликаються до міжнародної співпраці, щоб побороти злочини в Інтернеті. Вона була ратифікована ще у 2001 році, але Росія та Китай не голосували за неї. Сполучені Штати та Європа сумніваються, що російська ініціатива реально допоможе боротися з порушенням закону в мережі. Натомість, державні органи отримають додаткові повноваження для контролю за інформацією та блокування сайтів, на яких критикують уряд.

Росія багато років лобіювала таку резолюцію, відзначили США. Проблема у тому, що багато країн, які її підтримують, так чи інакше, не розуміють всієї складності системи. І от пояснити цим країнам, що насправді закладено у резолюцію трохи глибше, ніж "боротьба з кіберзлочинцями" – найскладніше завдання, вважають у Вашингтоні. Насправді, підкреслили у Держдепі, немає потреби у нових інструментах для цієї боротьби, вони вже наявні та активні. Це відповідає даним, що Росія не консультувалася з експертами у галузі, готуючи свою резолюцію.

Відкритий лист 36-ти організацій, які захищають права людини, назвав резолюцію такою, що "обмежить використання Інтернету для захисту прав людини та соціоекономічного розвитку". Такі закони можуть привести до вибіркових арештів, затримань та навіть до смерті людей, зазначено у листі…». ***(Анатолій Максимов. Кібербезпека, хакери, автономія: як Росія створює свій власний інтернет // Телеканал новин «24» (https://24tv.ua/rezolyutsiya_oon_po_kiberbezpetsi_do_chogo_tse_mozhe_prizvesti_n1255944). 02.01.2020).***

***

«LinkedIn - соцмережа для встановлення ділових контактів - вже третій рік поспіль складає щорічний звіт про найзатребуваніші професії - ТОП-15 спеціальностей. …дослідження було проведено в 11 країнах світу, серед яких США, Великобританія, Франція, Канада, Німеччина, Сінгапур та інші. Фахівці компанії провели аналіз, враховуючи професійні навички та особисті якості кандидатів, що претендують на найвищі зарплати. Серед основних трендів на 2020 рік LinkedIn назвав наступні…

Топ 15 найкращих спеціальностей за версією LinkedIn:

…10. Спеціаліст з кібербезпеки (Cybersecurity Specialist). За прогнозами, кібербезпека буде одним з найбільш швидко зростаючих напрямків інвестицій в IT в 2020 році. Спостерігається зростання попиту на фахівців з кібербезпеки та технічних фахівців, які мають досвід у цій галузі. Не секрет, що кібербезпека є першочерговою для кожної компанії. Зростання попиту на цю професію, ймовірно, продовжуватиметься, оскільки в звітах видно, що в 2019 році порушення даних збільшилося більше ніж на 50%...

Оскільки такі тенденції зберігатимуться впродовж 2020 року у провідних країнах світу, можна очікувати, що й в Україні описані спеціальності будуть у тренді на найближче майбутнє.» ***(LinkedIn склав рейтинг ТОП-15 професій майбутнього: цікаве буковинцям // Сайт міста Чернівці (https://www.0372.ua/news/2631454/linkedin-sklav-rejting-top-15-profesij-majbutnogo-cikave-bukovincam). 15.01.2020).***

***

«На цьогорічному Всесвітньому економічному форумі в Давосі… піднімали… соціально-значущі питання.

Ось топ-5 найважливіших:

…

5. Загрози кібербезпеки та скандал зі зламом телефонів через контакт з корон-принцом Саудівської Аравії

Згідно з доповіддю про глобальні ризики Всесвітнього економічного форуму за 2020 рік, кібератаки - на другому місці серед ризиків, які найбільше викликатимуть занепокоєння у бізнесу в усьому світі протягом наступних 10- ти років. Кібератаки на критичну інфраструктуру, оцінені п'ятим найбільшим ризиком у 2020 році, - стали новим нормальним явищем у таких галузях, як енергетика, охорона здоров'я та транспорт.

Тому кібербезпека була останні роки в порядку денному в Давосі, і ось цього року додався ще й особистий аспект.

У перший день форуму розгорівся скандал. Телефон Джеффа Безоса, засновника Amazon і одного з найбагатших людей світу, був зламаний корон-принцом Саудівської Аравії Мухаммедом бін Салманом.

Найцікавіше - багато з присутніх в Давосі ТОПів контактували з принцом Мухаммедом під час поїздки, коли він зустрівся з Безосом. Серед них: Стівен Мнучін, американський банкір, Тім Кук, CEO Apple, та Сатья Наделла, CEO Microsoft…» ***(Наталия Микольская. Пять важных выводов с Давоса // "Эксперт-Центр" (http://expert.org.ua/v-mire/2020/pyat-vazhnyh-vyvodov-s-davosa). 29.01.2020).***

***

«Йенс Столтенберг выступил с речью о кибербезопасности на Всемирном экономическом форме в Давосе.

Человечество пока даже не осознает, насколько новые технологии меняют природу современных боевых действий, и это ставит новые вызовы перед НАТО, которое постоянно адаптируется для эффективной защиты от таких угроз.

Об этом в четверг в рамках дискуссии на Всемирном экономическом форме в Давосе заявил генеральный секретарь НАТО Йенс Столтенберг.

"Я думаю, что для нас сейчас трудно даже представить последствия того, что мы видим вокруг. Когда вы читаете книги о первой мировой войне, одна из шокирующих вещей - это то, что они даже не представляли, какими могут быть последствия индустриальной революции для боевых действий. Я боюсь, что что-то подобное происходит сейчас, и мы, на самом деле, не понимаем, как сильно

технологии меняют также саму природу военного дела", - сказал руководитель Альянса.

Он отметил, что НАТО осознает, какие фундаментальные изменения произошли в самой природе военной борьбы. Это произошло не только вследствие появления кибернетических средств, но и вследствие развития искусственного интеллекта, автономных систем вооружения, систем распознавания лица и других. Если все эти технологии совместить, отметил Столтенберг, то можно представить себе системы вооружений, которые являются действительно очень страшными и разрушительными, если когда-нибудь будут использованы. В этих условиях по его мнению, гораздо труднее осуществлять контроль над вооружением, когда приходится не только считать боеголовки, но пытаться каким-то образом измерить алгоритмы и технологии, использование которых мир до этого не видел, по крайней мере, в военной сфере.

"Мы много инвестируем, чтобы оставаться на острие развития технологий, в частности, в кибернетической сфере. Мы (НАТО) приняли решение, что кибернетическая атака может быть причиной для применения статьи 5 (Вашингтонского договора, "нападение на одного является нападением на всех"). И это важное решение. Поэтому, если осуществляется кибернетическая атака на одного союзника, на нее может ответить весь Альянс. И после этого мы будем продолжать решать, каким именно образом реагировать на такую атаку", - отметил Столтенберг.

Он подчеркнул, что у стран-союзниц есть не только оборонительные, но и наступательные кибернетические технологии, и НАТО может координировать применение таких возможностей, как это уже произошло, например, в борьбе с ИГИЛ.

"Иногда люди не совсем понимают, в какой степени борьба против ИГИЛ представляла собой кибернетическую кампанию. Разрушая их кибернетические способности, закрывая их сайты, и все, что они делали в киберпространстве, включая рекрутинг, финансирование и пропаганду. Союзники по НАТО, используя кибернетические технологии, смогли разрушить эту систему", - сказал генеральный секретарь НАТО.

Он еще раз подчеркнул о том, что, в случае кибернетической атаки на одного из союзников, НАТО может применить статью 5 Вашингтонского договора.

"При этом ответ может быть как в кибернетическом пространстве, так и каким-либо другим. Мы никогда не будем давать предпочтение потенциальному агрессору, рассказывая о наших дальнейших шагах, о наших "красных линиях", и как мы собираемся отвечать. Мы осуществим все необходимые действия, чтобы ответить на такую атаку на все 360 градусов, включая кибернетические средства. При этом, если вы готовы сегодня, это не значит, что вы будете готовы завтра. Мы должны продолжать адаптироваться, и это тяжелая работа", - добавил Столтенберг.» ***(В НАТО заверили, что отреагируют на кибератаку в отношении любой страны Альянса // Телеграф (https://telegraf.com.ua/mir/europa/5318585-v-nato-zaverili-chto-otreagiruyut-na-kiberataku-v-otnoshenii-lyuboy-stranyi-alyansa.html). 23.01.2020).***

***

«За пять недель — в период между 9 октября и 15 ноября 2019 года — взломать системы армии США удалось 52 этичным хакерам. Представители Минобороны заявили, что такие мероприятия помогают усилить защиту вооружённых сил Америки. Специалисты атаковали армию США в рамках конкурса «Hack the Army», который проводится совместно с платформой HackerOne с 2016 года. Как нетрудно догадаться, основная задача инициативы «Hack the Army» — устранить все возможные уязвимости и лазейки, которые в теории могут использовать правительственные киберпреступники. Исходя из геополитической обстановки, США больше всего опасаются кибератак со стороны Ирана. За пять недель этичные хакеры должны были попробовать взломать 60 публично доступных онлайн-объектов армии США. Среди них были, например, домены army.mil и goarmy.com. 52 специалиста из США, Канады, Германии и Румынии сообщили о 146 обнаруженных уязвимостях. «Армия США выплатила хакерам более $275 000, сумма самого большого вознаграждения составила $20 000», — передаёт Business Wire». ***(Олег Иванов. За пять недель армию США взломали 52 этичных хакера // ООО «АМ-МЕДИА» (https://www.anti-malware.ru/news/2020-01-17-1447/31749). 17.01.2020).***

***

«В условиях растущих страховых требований по договорам киберстрахования страховщики США вынуждены повысить тарифы на 25%...

Сообщается, что минувший год ознаменовался рядом дорогостоящих кибернетических инцидентов с использованием вредоносного программного обеспечения, открывающего доступ к широкому спектру информации.

По данным компании-разработчика антивирусной защиты Malwarebytes Labs, в 2019 году зафиксировано на 6% меньше случаев кибернетического вымогательства по сравнению с 2018 годом, но степень ущерба и длительность технологических сбоев заметно усилилась. Хакерские атаки обычно сопровождаются вымогательством крупных денежных сумм, — в третьем квартале средняя сумма, которую требовали злоумышленники, составила более $41 тысяч.

Ранее сообщалось о результатах исследования, проведенного Федеральной резервной системой США (ФРС), что успешная кибератака на один или группу крупных банков США повлечет за собой системный сбой в работе финансового рынка». ***(Страховщики США повышают ставки на киберстрахование из-за растущих выплат // TRISTAR.com.ua (http://tristar.com.ua/1/news/strahovshiki_ssha_povyshaut_stavki_na_kiberstrahovanie_iz_za_rastushih_vyplat_12867.html). 29.01.2020).***

***

«Согласно проведенному исследованию Федеральной резервной системы США (ФРС), успешная кибератака на один или группу крупных банков США повлечет за собой системный сбой в работе финансового рынка.

Как выяснил интернет ресурс УкрСтрахование, авторы отчета провели моделирование хакерской атаки и оценили возможные последствия в условиях включения банков в глобальную платежную сеть. Таким образом, уязвимость одного банка может спровоцировать глобальный сбой в работе финансовой системы.

«Кибератака на любой из наиболее активных банков США, которая подрывает способность банков отправлять платежи, вероятно, окажет сильное влияние на ликвидность многих других банков в системе», — говорится в отчете…» ***(Последствия кибертатаки на крупный банк США будут фатальными для финансовой системы // УкрСтрахование (https://www.ukrstrahovanie.com.ua/news/posledstviya-kibertataki-na-krupnyj-bank-ssha-budut-fatalnymi-dlya-finansovoj-sistemy). 21.01.2020).***

***

Інші країни

«Президент Ірану Хасан Рухані звинуватив США у кібератаці, через яку війська збили український літак МАУ.

Іранські військові уточнили, що американці нібито вивели з ладу іранські радари, тому зенітники в Тегерані переплутали пасажирський лайнер МАУ з американською крилатою ракетою.

Існує також версія, що ймовірно, система ППО допустила помилку через заплутану структуру управління в країні. Адже в Ірані є дві майже незалежні армії, які іноді конфліктують одна з одною.

Одна з них – Корпус вартових ісламської революції і збила український літак…». ***(ППО Ірану могла випустити ракету в літак МАУ через внутрішній конфлікт двох армій // ФАКТИ. ICTV (https://fakty.com.ua/ua/svit/20200117-ppo-iranu-mogla-vypustyty-raketu-v-litak-mau-cherez-vnutrishnij-konflikt-dvoh-armij/). 17.01.2020).***

***

Протидія зовнішній кібернетичній агресії

«Федеральное бюро расследований США внесло изменения в свою политику по защите конфиденциальности и теперь начнет уведомлять государственных чиновников на уровне штата о взломах в локальных системах электронного голосования.

Ранее ведомство уведомляло об инцидентах только местные власти в обход руководства штатов. Изменение в политике является одной из правительственных мер, призванных пересмотреть процесс обмена информацией о киберугрозах. Новая политика поможет снизить беспокойство местных властей, которые ранее

неоднократно жаловались на отсутствие информации от федерального правительства.

По словам федеральных чиновников, цель заключается в более эффективном обмене информацией, что позволит передать данные о попытках вмешательства в выборы государственным чиновникам, обладающим ресурсами для устранения проблемы. Как отмечается, политика призвана обеспечить передачу информации от федерального правительства напрямую.

Политика ФБР не распространяется на стандартную киберактивность, такую как сканирование сетей на предмет уязвимостей, однако она будет расширена на сложные целевые фишинговые кампании, направленные на сбор учетных данных.

Новая политика предоставила обновленные и дополнительные указания по своевременному распространению уведомлений и сообщений об угрозах, защите информации и раскрытию информации о жертве, а также координации между ФБР и другими агентствами в отношении безопасности выборов.» ***(ФБР будет уведомлять власти штатов о взломах в ходе выборов // SecurityLab.ru (https://www.securitylab.ru/news/504214.php). 17.01.2020).***

***

«Группа анонимных исследователей безопасности, называющая себя Intrusion Truth, обнаружила 13 подставных компаний на острове Хайнань (Китай), через которые правительство Китая, предположительно, вербует киберпреступников.

Обнаруженные компании используют общие контактные данные, совместные офисы и размещают в интернете почти идентичные объявления о работе для найма подпольных специалистов. В данных объявлениях также указаны одинаковые почтовые адреса и контактные лица.

Фирмы практически не отличаются друг от друга, и каждая описывает себя как быстро растущую, высокотехнологичную компанию по информационной безопасности, которая стремится стать ведущим производителем продуктов и услуг информационной безопасности в Китае.

«В то время как компании подчеркивают свою приверженность информационной безопасности и киберзащите, размещенные ими технические требования говорят о поиске навыков проведения кибератак», — сообщили исследователи.

Эксперты из FireEye и «Лаборатории Касперского» связывают данные находки Intrusion Truth с финансируемой правительством КНР группировкой APT40, занимающейся кибершпионажем с 2013 года. Обычно она нацелена на страны, имеющие стратегическое значение для китайского проекта «Один пояс и один путь».

Некоторые из данных компаний специалисты связали с профессором кафедры информационной безопасности Гу Цзянь в университете Хайнаня. Фактически, одна из 13 подозреваемых фирм была размещена в библиотеке университета. По словам Intrusion Truth, Гу Цзянь также является бывшим военным китайской армии…» ***(Китайские киберпреступники скрываются за сетью подставных ИБ-компаний // SecurityLab.ru (https://www.securitylab.ru/news/504022.php). 14.01.2020).***

***

«Взлом Демократического национального комитета в 2016 году стал тревожным звонком для всех, кто беспокоится о международных кампаниях управляемого хаоса. В понедельник вечером появилась новая причина для беспокойства об избирательной кампании 2020 года. Нью-Йорк Таймс и компания по кибербезопасности Area1 поделились историей о новой кибератаке российских спецслужб, нацеленных на Burisma, украинскую газовую компанию, связанную с импичментом Трампа. В течение многих месяцев республиканские оперативники намекали на какую-то ужасную коррупцию внутри компании, и если российская разведка действительно взломала компанию, это открывает пугающие возможности.

В Конгрессе США уже предсказывают повторение сценария 2016-го, так член палаты представителей Адам Шифф комментирует: «Похоже, они снова надеются помочь этому президенту». Это вызывает опасения, учитывая отказ Трампа признать российский взлом в последний раз, нет никаких гарантий того, что Белый дом предпримет какие-нибудь шаги для пресечения подобных действий сейчас…

В то время как отчет о взломе показал ужасающую картину, доказательства взлома менее конкретны, чем может показаться. Существуют убедительные доказательства того, что Burisma была успешно атакована при помощи фишинга, но гораздо сложнее определить, кто за ней стоит. Есть веские основания полагать, что за взломом стоит ГРУ, однако прямых улик, выводящих на российский след нет. В результате дело против России выглядит разочаровывающе неполным и предполагает, что президентская компания в США стартует с большим количеством вопросов, чем ответов.

Большая часть доказательств Area1 изложена в восьмистраничном отчете, опубликованном в связи со статьей Times. Основным доказательством является схема атак, которые ранее были направлены против Института Хадсона и Джорджа Сороса, обычно с использованием одних и тех же регистраторов доменов и интернет-провайдеров. Самое очевидное, что во всех трех фишинговых кампаниях использовался один и тот же поставщик SSL и версии одного и того же URL-адреса, и все они маскировались под услугу под названием «My Sharepoint». С точки зрения Area1, это игровая схема ГРУ, а Burisma - только последняя, из долгой истории, цель.

Когда Кайл Эмке исследовал более ранние шаблоны того же паттерна для ThreatConnect, он пришел к более взвешенному выводу, оценив лишь с «умеренной уверенностью», что домены, с которых проводились атаки были связаны с APT28, сокращением используемым для ГРУ России.

Такая схема регистраций и фишинговых атак действительно выглядит как распространённая схема игры ГРУ, однако они не единственные, кто может управлять этим.

С практической точки зрения это означает, что операторы сетей должны поднимать тревогу каждый раз, когда они видят атаку, которая соответствует этому профилю, но сделать однозначный вывод по одному инциденту намного сложнее. Вся веб-инфраструктура, используемая в кампании, общедоступна и используется многими другими участниками, поэтому ни одна из них не может выступать

оружием в прямом смысле этого слова. Главной отличительной чертой, при этом, является термин «sharepoint», который исследователи видели только в URL-адресах, тесно связанных с ГРУ. Но любой может зарегистрировать URL со словом «sharepoint», так что связь является только косвенной…

«Это заметный набор согласований для поиска и потенциального использования для идентификации своей инфраструктуры», - сказал Эмке. «Но это не значит, что все, где были замечены эти совпадения, было и будет APT28».

Этот вид слабой атрибуции очень часто встречается в мире кибербезопасности, и он может вызвать реальные проблемы, когда страны изо всех сил пытаются выяснить международную дипломатию кибервойны. Фарзане Бадии, бывший исполнительный директор проекта по управлению интернетом в Georgia Tech, классифицирует слабую атрибуцию как «косвенные доказательства, которые могут быть подвергнуты техническому сомнению». Она рассматривает это как глобальную проблему и выступает за международные группы атрибуции, которые могут решить задачу, поэтому наблюдателям не нужно полагаться на частные компании или правительственные спецслужбы. Без этого проблема доверия может быть трудно решаема.

«Государства в основном финансируют кибератаки через индивидуальных подрядчиков и не осуществляют их самостоятельно», - говорит Бадии, затрудняя разграничение государственных субъектов и частных киберпреступников.

«Если вы обеспокоены вмешательством России в выборы 2020 года, ничто из этого не должно обнадеживать. ГРУ действительно взломал DNC в 2016 году, и нет никаких оснований думать, что они больше не попробуют совершить подобное, независимо от того, стояли ли они за конкретной фишинговой кампанией. Есть основания полагать, что ГРУ было замешано. Отсутствие прямых улик не обнадеживает - во всяком случае, это означает, что тот, кто это сделал, практически не оставил следов. Но если вы просто хотите узнать, действительно ли Россия взломала Burisma, то на этот вопрос пока нет ответа.» ***(Романов Роман. За хакерской атакой на украинскую газовую компанию Burisma могут стоять российские спецслужбы // Internetua (http://internetua.com/za-hakerskoi-atakoi-na-ukrainskuua-gazovuua-kompaniua-burisma-mogut-stoyat-rossiiskie-specslujby). 15.01.2020).***

***

«Представитель МИД Австрии Петер Гушельбауэр опроверг причастность России и Турции к кибератакам на внешнеполитическое ведомство…

Гушельбауэр подчеркнул, что сообщения о «российском следе» являются чистой спекуляцией…». ***(Антон Никитин. МИД Австрии ответил на сообщения о причастности России к кибератакам // Деловая газета «Взгляд» (https://vz.ru/news/2020/1/8/1017107.html). 08.01.2020).***

***

«В течение суток Иран будет пытаться использовать американское кибероружие против самих США», - предупреждал американский киберкомиссар еще при президенте Обаме, «потенциально нанося вред

энергетическим, финансовым и транспортным сетям Америки, используя взломанные и похищенные коды ЦРУ».

«Иран уже много лет активно проникает и внедряется в критически важные инфраструктуры по всей территории США», - утверждает Том Келлерман, который ранее занимался вопросами кибербезопасности Казначейства Всемирного банка. «Сейчас день траура [по иранскому генералу Кассима Сулеймани] подходит к концу и нам следует ожидать начала священной войны в киберпространстве. Честно говоря, мы довольно уязвимы».

Келлерманн также отметил, что Иран создал «элитные кибер-силы» за десятилетие, прошедшее после развертывания Stuxnet - компьютерного вируса, предположительно созданного Америкой и Израилем, который, в свое время, успешно дестабилизировал ядерную программу Ирана.

«Они могут нарушить работу систем управления воздушным транспортом в крупных аэропортах, что резко затруднит торговые отношения», - сказал Келлерманн. «Я очень обеспокоен энергетическим сектором. Я обеспокоен финансовым сектором. Реальность такова, что следующие 48 часов будут драматичными».

Келлерманн, который сейчас работает в фирме по кибербезопасности Carbon Black, предположил, что критически важная инфраструктура, от электростанций до финансовых учреждений, отреагировала на угрозу терроризма, разработав системы управления, которые можно было бы использовать дистанционно в случае физической атаки.

Но он сказал, что «большинство» таких систем были взломаны хакерами, использующими вирусы, которые находятся в состоянии покоя «как виртуальные спящие ячейки», ожидая пробуждения, чтобы контролировать или повредить их хосты.

Сила таких атак, была продемонстрирована в 2012-м, когда Иран нанес сокрушительный удар по нефтяной инфраструктуре своего регионального конкурента, Саудовской Аравии.

15 августа того же года вирус Shamoon стер данные с 3/4 всех компьютеров, принадлежащих саудовскому государственному нефтяному гиганту Aramco. То, что осталось, было изображением горящего американского флага. Две недели спустя аналогичная атака была направлена на производителя жидкого природного газа в Катаре, RasGas, и в сентябре несколько веб-сайтов американских банков были взломаны в результате третьего кибер-удара, приписанного Ирану.

Одним из признаков разрушительных последствий таких атак стал инцидент в 2015 году, когда российские хакеры отключили электричество на западе Украины. Платежные системы перестали работать, поезда перестали работать, связь была прервана.

По иронии судьбы любая иранская кибератака может использовать кибероружие, разработанное в США.

В 2016-м хакерская группа под названием Shadow Brokers похитила целый ряд хакерских инструментов США прямо из Агентства национальной безопасности (АНБ) США. В следующем году Wikileaks начал публиковать аналогичные хаки из «Убежища №7» ЦРУ, в котором содержались десятки сложных методов для

мониторинга, наблюдения и управления устройствами от смартфонов до автомобилей. Многие из украденных кодов были быстро приняты и адаптированы врагами США, в частности, EternalBlue, который, как многие считают, был разработан АНБ, ставший основой для глобальной кибератаки в 2017-м под названием NotPetya. Вирус затронул множество сфер: от нефти и судоходства до фармацевтических компаний. По оценкам экспертов ущерб нанесенный вирусом составил около $10 млрд. Россия остается ключевым подозреваемым по этому делу.

«Величайшим историческим событием в области кибербезопасности стало разграбление хранилища №7 и теневых брокеров», - говорит Келлерманн. «Величайшее оружие, разработанное США, было украдено Иранскими хакерами, а затем его усовершенствовали и модернизировали. Такова природа кибервойн и кибератак, ваше оружие будет использовано против вас».

Однако, это не просто кибер-оружие. Ведь, даже самое изощренное физическое оружие армии США не защищено от взлома. В 2011 году Иран захватил американский самолет-разведчик Sentinel RQ-170, взломав его системы наведения и приземлив возле Кашмера на северо-востоке Ирана.

Захваченный беспилотник впоследствии стал образцом для собственных дронов Ирана, один из которых, известный как Shahed 171, был перехвачен Израилем в 2018 году…

«Будущие войны действительно зависят от беспилотных, ракетных и авиационных боевых действий», - сказал Келлерманн. «Но всеми этими системами можно манипулировать и использовать их в своих целях, прибегая к кибератакам и кибервойнам».

Используя радиоэлектронные войны, все 3 сферы: беспилотники, ракеты и авиация, бывшие в числе военных приоритетов, которые Иран установил для пятилетнего плана модернизации, были запущены в июле 2017 года.

«В течение последних 20 лет у США было преимущество для сражений с противником, технологии которого отставали в развитии», - добавил Келлерманн. «Будь то Афганистан, Ирак или даже ИГИЛ. Сейчас Иран значительно усовершенствовал свои возможности по проведению кибератак, благодаря передаче технологий из России, и в результате они способны осуществлять разрушительные атаки на американскую инфраструктуру». ***(Роман Романов. Иран может применить против США их собственное оружие в «священной кибервойне» // Internetua (http://internetua.com/iran-mojet-primenit-protiv-ssha-ih-sobstvennoe-orujie-v-svyasxennoi-kibervoine-). 08.01.2020).***

***

«Невідомі зламали в суботу американський урядовий сайт, на якому публікується у відкритому доступі документація, і розмістили на його головній сторінці заяви в підтримку Ірану і проти американського лідера Дональда Трампа…

Увечері в суботу у американських користувачів при переході на портал FDLP (Federal Depository Library Program) відкривалася сторінка з написами англійською та перською мовами: “Це послання від Ісламської Республіки Іран. Ми не

припинимо надавати підтримку нашим друзям в регіоні — пригнобленим народам Палестини, Ємену, Бахрейну, народу і уряду Сирії та Іраку".

На сторінці також стверджується, що портал був "зламаний іранськими хакерами" нібито з "групи кібербезпеки Ірану". Невідомі розмістили на сторінці колаж, на якому зображений закривавлений після удару кулаком Трамп і запущені ракети.

Портал FDLP публікує для загального доступу урядову документацію.

В суботу Міністерство внутрішньої безпеки (МВБ) США повідомило, що Тегеран може організувати кібератаку на США після вбивства іранського генерала Касема Сулеймані…». ***(Ілля Нежигай. Невідомі під виглядом іранських хакерів зламали один з урядових сайтів США // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1844988-nevidomi-pid-viglyadom-iranskikh-khakeriv-zlamali-odin-z-uryadovikh-saytiv-ssha). 05.01.2020).***

***

«…Кібератака на комп'ютерну мережу МЗС Австрії триває вже третій день.

Про це заявив прес-секретар відомства Петер Гушельбауер у коментарі інформагентству APA в понеділок, 6 січня.

«Кібератака на IT-системи міністерства закордонних справ триває і в свято Трьох королів (6 січня, - ред.). Атаки продовжуються, як і технічні контрзаходи, до яких залучено також фахівці міністерства внутрішніх справ», - сказано в публікації.

У міністерстві поки не можуть оцінити, коли кібератака припиниться. За тактичними причинами технічні деталі кібернападу не розголошуються. Таким чином, поки що не зрозуміло, чи були якісь дані вкрадені або змінені.

Веб-сайт МЗС Австрії продовжує справно працювати, нападу піддалися внутрішні комп'ютерні мережі відомства…

Міністерство не виключає, що хакери могли діяти за завданням іноземної держави. Деталі у відомстві не розголошують, але уточнюють, що факт був швидко виявлений і усунутий». ***(Хакери третій день атакують МЗС Австрії // Українські медійні системи (https://glavcom.ua/news/hakeri-tretiy-den-atakuyut-mzs-avstriji-651047.html). 07.01.2020).***

***

«Глава МЗС Австрії Александр Шалленберг заявив у середу, що кібератаки проти його відомства, які почались на початку січня, продовжуються.

…про це міністр розповів, доповідаючи перед депутатами нижньої палати парламенту Австрії.

За словами Шалленберг, атака, що досі триває, є масивною, однак жодних витоків даних міністерства поки не виявлено.

Про кібернапад на МЗС Австрії було повідомлено 3 січня. Тоді мова йшла про можливе втручання іноземної держави. Однак зараз, за словами Шалленберга, немає достатніх доказів, щоб говорити про те, звідки надходить кібератака…». ***(Австрія заявила про продовження кібератак на своє МЗС // Європейська правда (https://www.eurointegration.com.ua/news/2020/01/22/7105458/). 22.01.2020).***

***

«По мере усиления гонки за Белый дом ФБР усиливает меры безопасности, чтобы государство могло лучше подготовиться к потенциальным кибератакам. В четверг федеральное правоохранительное агентство заявило, что расширит свои уведомления о взломах, затрагивающих избирательную инфраструктуру, и включит должностных лиц на уровне штата, а также местные и окружные власти.

Ранее ФБР уведомляло только пострадавшие округа, которые проводят выборы, а не должностных лиц ответственных за процедуры выборов. Это стало проблемой, потому что должностные лица государственных выборов подтверждают результаты и должны знать о кибератаках, если они происходят.

Безопасность на выборах является основной проблемой президентской кампании в США в 2020 году. Федеральное правительство стремится избежать кибератак, подобных тем, которые преследовали выборы 2016 года. Российские хакеры успешно проникли в государственные базы данных выборов, а также в базы данных избирателей в двух округах Флориды. Министерство внутренней безопасности пришло к выводу, что кибератаки не привели к изменению голосов.

Государственные чиновники во Флориде не узнали о нарушениях, пока не был публично опубликован доклад тогдашнего специального адвоката Роберта Мюллера о вмешательстве в выборы. В мае губернатор штата Флорида Рон ДеСантис заявил, что представители государственных органов были проинформированы ФБР только после выхода доклада.

Новые процедуры означают, что таких задержек можно избежать в будущем». ***(ФБР усиливает меры кибербезопасности перед выборами // SecureNews (https://securenews.ru/fbi-strengthens-cybersecurity-measures-before-elections/). 17.01.2020).***

***

«Представители корпорации Microsoft отметили всплеск фишинговых атак, нацеленных на представителей американского, японского и южнокорейского истеблишмента…

Эксперты корпорации предположили, что хакеры, входящие в состав группировки Thallium, действуют в интересах правительства Северной Кореи и базируются там же. Целями злоумышленников стали правительственные чиновники, члены преподавательского состава вузов и исследовательские организации. Интересовали хакеров разработки в области высоких технологий и тяжелой промышленности.

Для получения доступа к конфиденциальной информации хакерами использовался метод, известный как «целевое фишинг-мошенничество». Также использовались адреса электронной почты, которые выглядели вполне реально.» ***(Северокорейские хакеры терроризируют американцев // SecureNews (https://securenews.ru/severokoreyskie-hackeri-terroriziruyut-amerikantsev/). 08.01.2020).***

***

«Когда на прошлой неделе Израиль принимал у себя десятки мировых лидеров на Всемирном форуме по Холокосту, система киберзащиты страны отразила сотни кибератак, направленных против международного аэропорта страны и самолетов мировых лидеров.

Ссылаясь на Управление аэропортов, "Channel 12" рассказал, что по меньшей мере 800 разных кибератак были направлены на израильскую авиацию в четверг, в то время как мировые лидеры, включая вице-президента США Майка Пенса (Mike Pence) и президента России Владимира Путина (Vladimir Putin), приземлились в стране. Сообщается, что все атаки были успешно отбиты.

Отмечается, что нападения происходили из Ирана, Китая, Северной Кореи, России и Польши. Атаки "были направлены против аэропорта и самолетов, - говорится в сообщении, - и были направлены на то, чтобы нарушить траекторию полета более 60 самолетов с главами государств, королями и президентами".» ***(Самолеты лидеров, прилетевших в Израиль, подвергались кибератакам // ISRAland Online Ltd (http://www.isra.com/news/240724). 27.01.2020).***

***

«Масштабные вредоносные кампании, направленные против правительств и других организаций в Европе и на Ближнем Востоке в 2018 и 2019 годах, предположительно являются делом рук киберпреступников, действующих в интересах турецкого правительства. Об этом сообщили три высокопоставленных представителя западных служб безопасности…

Злоумышленники напали на по меньшей мере 30 организаций, включая правительственные министерства, посольства и службы безопасности, а также компании и другие предприятия. Целями преступников были службы электронной почты кипрского и греческого правительства, а также советник правительства Ирака по национальной безопасности.

Атаки включали перехват интернет-трафика, потенциально позволяя преступникам получить несанкционированный доступ к сетям государственных органов и других организаций. По словам западных чиновников и частных экспертов по кибербезопасности, преступники использовали метод, известный как отравление кэша DNS (или DNS-спуфинг). Во время DNS-спуфинга происходит изменение записей на DNS-сервере с целью перенаправления трафика. Поменяв конфигурацию данной системы, злоумышленники смогли перенаправлять пользователей на мошеннические сайты и похищать учетные данные. Как сообщает информагентство, подобные атаки впервые были зафиксированы в начале 2018 года. По словам двух британских и одного американского чиновника, данная кибершпионская активность имеет характерные черты кампании, спонсируемой государством Турции.

Данный вывод основан на трех факторах: личностях и местонахождении жертв преступников, в том числе правительства геополитически значимых для Турции стран; сходстве с предыдущими атаками, в ходе которых использовалась зарегистрированная в Турции инфраструктура; и информации разведслужб.

Министерство внутренних дел Турции не прокомментировало данную ситуацию. Высокопоставленный турецкий чиновник не ответил напрямую на вопросы о данной кампании, но сообщил, что Турция сама часто становится

жертвой кибератак.» ***(Турецкие преступники заподозрены в атаках на более чем 30 организаций по всему миру // SecurityLab.ru (https://www.securitylab.ru/news/504445.php). 27.01.2020).***

***

Створення та функціонування кібервійськ

«Кибер-войска были созданы в 2013 году и насчитывают примерно 6200 военных из разных служб. Накануне специальная комиссия при Национальном Конгрессе США приняла решение об увеличении бюджета и численности американских ИТ-войск…

“Стоит отметить, что положение сил в современном кибер-пространстве очевидно-неадекватно”, - заявил член палаты представителей Майк Галлагер. Именно в соответствии с “новым восприятием кибер-реальности”, Галлагер и другие члены комиссии заявили, что Пентагон должен быть способен противостоять растущим вызовам со стороны зло-действующих лиц». ***(Конгресс США намерен увеличить субсидирование кибервооружения // SecureNews (https://securenews.ru/kongress-usa-uvelichil-subsidirovaniye/). 09.01.2020).***

***

«Кибернетическое командование США оказалось не готовым к большим объемам данных, полученных в результате взлома информационной инфраструктуры террористической организации ДАИШ (является запрещенной в РФ). Хотя операция по взлому учетных записей и серверов ДАИШ прошла успешно, у Киберкомандования не хватило места для хранения извлеченных материалов. Об этом говорится в документах, опубликованных в рамках закона США «О свободе информации» (FOIA) на сайте Архива национальной безопасности при Университете Джорджа Вашингтона.

Шесть опубликованных на сайте сильно отредактированных документов подводят итоги 120-дневной оценки данных, проведенной Киберкомандованием по завершении операции «Светящаяся симфония» (Glowing Symphony).

Засекреченная наступательная кибероперация проводилась в ноябре 2016 года Объединенной тактической группой Ares (JTF-Ares). Ее целью была блокировка распространения пропаганды в интернете путем взлома принадлежавших ДАИШ учетных записей в соцсетях, сайтов и серверов.

Как выяснилось в ходе анализа результатов кибероперации, Киберкомандование недооценило объемы данных, с которым ему пришлось столкнуться. Вопрос, где хранить извлеченные из взломанной инфраструктуры материалы, стал самым главным.

Во избежание возникновения подобных проблем в будущем Киберкомандование рекомендовало своей Группе развития возможностей (CDG) разработать новое решение для хранения данных». ***(У Киберкомандования США закончилось место для хранения взломанных данных // SecurityLab.ru (https://www.securitylab.ru/news/504321.php). 22.01.2020).***

***

«Главный игрок на японском рынке оборонных и промышленных технологий Mitsubishi Electric повергся кибератаке, в результате которой могла произойти утечка информации, принадлежащей партнерам компании и правительственным службам.

…злоумышленники могли скомпрометировать переписку Mitsubishi Electric с представителями Министерства обороны и Агентства по ядерному регулированию, а также документы, относящиеся к совместным проектам с частными фирмами, в том числе с коммунальными предприятиями, железнодорожными операторами, автопроизводителями и операторами связи. Высокочувствительная информация, связанная с работой критической инфраструктуры и оборонными технологиями, скомпрометирована не была, уверяют в Mitsubishi Electric.

В июне прошлого года специалисты компании зафиксировали подозрительную активность на одном из своих устройств, находящихся в Японии. В ходе внутреннего расследования они обнаружили неавторизованный доступ к системам отделов менеджмента в главном и других офисах Mitsubishi Electric. Как считают в компании, за инцидентом стоят китайские киберпреступники.» ***(Компания Mitsubishi Electric подверглась кибератаке // SecurityLab.ru (https://www.securitylab.ru/news/504228.php). 20.01.2020).***

***

«Специалисты из компании ImmuniWeb провели анализ уровня кибербезопасности 100 крупнейших в мире аэропортов (Азии, Европы, Северной Америки, Австралии, Африки и Южной Америки). По результатам исследования, 97 из 100 крупнейших аэропортов мира подвержены угрозам безопасности, связанным с уязвимыми web-приложениями и мобильными программами, неправильно настроенным публичным облачным сервисом или утечками данных.

97% сайтов аэропортов работают на устаревшем ПО, 24% — содержат известные и эксплуатируемые уязвимости, 76% и 73% web-сайтов не соответствуют стандартам GDPR и PCI DSS соответственно, а у 24% отсутствует SSL-шифрование или используется устаревший SSLv3-протокол.

Оценивая уровень безопасности главных web-сайтов, специалисты присвоили максимальную оценку A+ (не обнаружено ни одной проблемы) только трем, 15 получили оценку A (несколько небольших проблем), 11 — B (ряд небольших проблем), 47 — C (уязвимости и серьезные проблемы) и 24 — F (наличие известных и эксплуатируемых уязвимостей). 53 сайта работали на устаревшем ПО, 38 содержали уязвимые компоненты, 10 использовали устаревшую систему управления содержимым, а 6 — уязвимую CMS.

Что касается межсетевых экранов web-приложений (WAF), только 55% основных web-сайтов и 40% поддоменов крупнейших аэропортов мира защищены WAF.

Сканирование облачных сервисов выявило использование общедоступного облачного хранилища Amazon Web Services S3 в 12 аэропортах. Три аэропорта использовали незащищенные бакеты, которые содержали значительный объем конфиденциальных данных. В ходе исследования специалисты определили 3 самых безопасных международных аэропорта, которые успешно прошли все проверки: Амстердамский аэропорт Схипхол, аэропорт Хельсинки-Вантаа и Дублинский аэропорт.» ***(97 из 100 крупнейших аэропортов используют уязвимые сайты и web-приложения // SecurityLab.ru (https://www.securitylab.ru/news/504519.php). 29.01.2020).***

***

«Специалисты из компании Dragos зафиксировали растущее число киберпреступных группировок, нацеленных на энергетические компании в Северной Америке.

«По мере того, как злоумышленники вкладывают больше усилий и денег на приобретение новых возможностей, риск разрушительного нападения на электроэнергетический сектор значительно возрастает», — сообщается в отчете North American Electric Cyber Threat Perspective.

Эксперты обнаружили в общей сложности 11 группировок, нацеленных на АСУ ТП, семь из которых ранее уже осуществляли атаки на электрические сети в Северной Америке — PARISITE, XENOTIME, MAGNALLIUM, DYMALLOY, RASPITE, ALLANITE и COVELLITE.

Операторы вредоносного ПО Triton/Trisis из группировки XENOTIME в 2017 году напали на нефтехимический завод в Саудовской Аравии, а теперь нацелились на электрические сети в США и Азиатско-Тихоокеанском регионе.

Спонсируемая иранским правительством киберпреступная группировка APT33, также известная как Elfin, MAGNALLIUM или Refined Kitten также переключилась на электроэнергетический сектор в США осенью 2019 года.

Специалисты также рассказали в отчете о группировке PARISITE, связанной с MAGNALLIUM, которая ориентирована на коммунальные, аэрокосмические и нефтегазовые компании в Северной Америке, Европе и на Ближнем Востоке. Злоумышленники используют инструменты с открытым исходным кодом для компрометации инфраструктуры цели и эксплуатируют уязвимости в VPN для получения доступа к сетям жертв.

Другая обнаруженная группировка — WASSONITE предположительно связанна с COVELLITE. Вредоносные программы и инфраструктура COVELLITE аналогичны тем, что применяет предположительно спонсируемая государством Северной Кореи Lazarus Group.

WASSONITE существует примерно с 2018 года и нацелена на электроэнергетический и атомный секторы, производственные и исследовательские предприятия в Индии, а также, вероятно, в Южной Корее и Японии. Преступники использовали известный «шпионский инструмент» DTrack для сбора учетных данных.

Как отметили эксперты, только группировки XENOTIME и ELECTRUM обладают возможностями и инструментами, необходимыми для атак на АСУ ТП. ELECTRUM — группировка, стоящая за атакой в 2016 году на энергосистему Украины, в ходе которой применялось вредоносное ПО CrashOverRide

В отчете описаны шесть возможных сценариев атак на сектор электроэнергетики Северной Америки, в том числе разрушительные события, приводящие к перебоям в электроснабжении, атаки через сторонних производителей и производителей оригинального оборудования, на объекты в цепочке поставок электроэнергии, а также через сотовую связь или спутниковые соединения.» **(Киберпреступники нацелились на энергетические компании в Северной Америке // SecurityLab.ru (https://www.securitylab.ru/news/503949.php). 13.01.2020).**

***

«Юваль Штайниц (Yuval Steinitz) заявил в среду на конференции по кибербезопасности в Тель-Авиве, что несколько месяцев назад нация "обнаружила и нейтрализовала" серьезную и изощренную кибератаку, целью которой было парализовать и контролировать одну из главных электростанций страны и другие объекты.

Страны, враждебные Израилю, такие как Иран, могут создать хаос, если они нацелены на такую критически важную инфраструктуру, как транспорт, здравоохранение или системы связи, сказал господин Штайниц. Но самой чувствительной, по его словам, инфраструктурой является энергетический сектор. Министр не указал, какая конкретно электростанция подверглась атаки.

Как сообщил Йосси Шнек (Yossi Shneck), глава кибербезопасности на коммунальном предприятии, это не был один из объектов Израильской электрической корпорация, системы которой, тем не менее, в прошлом году претерпевали в среднем 11 000 подозрительных кибер-событий в секунду, что делает ее одной из самых атакуемых в цифровом пространстве организаций в мире». ***(Министр энергетики: Израиль предотвратил "серьезную" атаку на электростанцию // ISRAland Online Ltd (http://www.isra.com/news/240853). 29.01.2020).***

***

Захист персональних даних

«Европейские регуляторы присудили 114 миллионов евро штрафа нарушителям Общего регламента защиты данных (GDPR) с тех пор как закон вступил в силу в середине 2018 года, причем подход к наказанию за нарушения Регламента варьируется от страны к стране…

Это стало ясно из отчёта юридической фирмы DLA Piper, которая также выяснила, что Франция выписала пока рекордный штраф за нарушение Регламента — 50 миллионов евро государство получит от компании Google. В то же время

Великобритания, Германия и Нидерланды лидировали по количеству нарушений за отчетный период.

Соблюдение закона обеспечивается совместными усилиями национальных регуляторов по защите данных в каждой стране Евросоюза, но самую большую ответственность несёт Ирландия, где располагаются крупные офисы гигантов из Силиконовой долины, вроде Facebook.

Партнёр компании DLA Piper прогнозирует, что штрафы будут расти, потому что появилась практика судебного разбирательства по вопросам защиты данных, и из-за того, что случаи тщательно рассматриваются в суде и появляются новые правовые прецеденты, штрафы постепенно возрастут.

В то же время штрафы не могут вырасти слишком быстро: сейчас регуляторы вправе потребовать штраф от двух до четырёх процентов мирового оборота компании, однако слишком высокий штраф может привести к провалу в суде, а в случае нескольких провалов регулятор потеряет свой авторитет, поэтому движение будет постепенным.

Самый большой штраф, который до сих пор находится под вопросом, это штраф британского регулятора к компании British Airways на 183 миллиона фунтов за кражу хакерами данных полумиллиона клиентов с сайта компании.» ***(Евросоюз оштрафовал нарушителей GDPR на 114 миллионов евро за полтора года // РосКомСвобода (https://roskomsvoboda.org/54625/). 20.01.2020).***

***

«За последние 18 месяцев, прошедших с момента вступления в силу Общего регламента защиты данных (The General Data Protection Regulation, GDPR), было зафиксировано более 160 тыс. уведомлений об утечках данных, и данное число продолжает расти с каждым днем.

По словам специалистов из юридической фирмы DLA Piper, после вступления в силу новых европейских правил о конфиденциальности в первые восемь месяцев в среднем поступало 247 уведомлений об утечках данных в день. С тех пор это число возросло до 278 уведомлений в день.

«Количество уведомлений об утечках данных увеличилось более чем на 12% по сравнению с прошлым годом, и регуляторные органы были заняты тестированием новых полномочий по санкциям и штрафам организаций», — отметили эксперты.

По оценкам специалистов, общая сумма выплаченных на сегодняшний день штрафов составляет €114 млн. Национальная комиссия по информатике и свободам (Commission nationale de l'informatique et des libertés, CNIL) Франции в 2019 году оштрафовала компанию Google на максимальную сумму в €50 млн за нарушение правил Общего регламента по защите данных касательно прозрачности при получении согласия на обработку и использование персональной информации пользователей…» ***(За последние 18 месяцев зафиксировано 160 тыс. утечек данных // SecurityLab.ru (https://www.securitylab.ru/news/504271.php). 21.01.2020).***

***

«В социальной сети Facebook запущена новая функция, отправляющая пользователям уведомление в случае, когда учетная запись используется для авторизации в стороннем приложении.

Функция не только будет служить дополнительным уровнем защиты, уведомляющем о несанкционированном доступе к учетной записи, но также предоставит больший контроль над конфиденциальной информацией.

Уведомление будет отправляться по электронной почте и в приложении Facebook, показывая, какие сведения социальная сеть предоставила сторонней программе или web-сайту. Через электронное письмо можно будет зайти в настройки и удалить разрешение приложению на доступ к пользовательским данным.

Пользователь получит уведомление в первый раз во время авторизации в приложении и когда будет использовать его повторно после истечения срока доступа данной программы к информации. Также можно просмотреть все приложения, которые в настоящее время имеют доступ к авторизации в системе и отменить его в случае необходимости…» ***(Facebook будет уведомлять об авторизации в сторонних приложениях // SecurityLab.ru (https://www.securitylab.ru/news/504100.php). 15.01.2020).***

***

«Операторы вымогательского ПО Nemty планируют разработать блог, в котором будут публиковаться похищенные данные жертв, отказавшихся платить выкуп злоумышленникам.

Новая практика, начатая операторами Maze и теперь также используемая Sodinokibi, заключается в краже файлов у компаний перед их шифрованием. Если жертва не платит выкуп, часть украденных данных будет публиковаться в Сети, пока не будет произведена оплата.

В партнерской панели Nemty разработчики вымогателя разместили новостную ленту, в которой они сообщают о будущих планах, исправлениях ошибок и предстоящих изменениях, касающиеся схемы RaaS (Ransomware-as-a-Service, вымогательское ПО-как-услуга).

Как сообщил ресурс BleepingComputer, Nemty уже настроен для сетевых атак в режиме компоновщика. Он используется для создания исполняемых файлов, предназначенных для всей сети, а не для отдельных компьютеров. Созданные исполняемые файлы вымогателей предназначены «только для корпораций», и будет один ключ для дешифрования всех устройств в сети…» ***(Вслед за Maze и Sodinokibi операторы Nemty начнут публиковать украденные данные // SecurityLab.ru (https://www.securitylab.ru/news/504023.php). 14.01.2020).***

***

«Операторы вредоносного ПО Sodinokibi, также известного как REvil, решили последовать примеру Maze и начали публиковать похищенные данные жертв, которые отказались заплатить выкуп. Злоумышленники разместили ссылки на около 337 МБ предположительно украденных файлов жертв на одном из подпольных форумов. Как утверждают преступники, данные принадлежат компании Artech Information Systems.

«Это небольшая часть того, что у нас есть. Если не будет никаких движений, мы продадим оставшиеся, более важные и интересные коммерческие и личные данные третьим сторонам, в том числе финансовую информацию», — сообщили преступники.

В настоящее время сайт Artech недоступен, и неизвестно, связано ли это с действиями преступников. Представители компании пока не прокомментировали данную ситуацию, сообщил ресурс BleepingComputer…» **(Операторы Sodinokibi впервые опубликовали в Сети похищенные данные // SecurityLab.ru (https://www.securitylab.ru/news/503973.php). 13.01.2020).**

***

«В течение нескольких лет Microsoft прослушивала и обрабатывала голоса пользователей Skype и Cortana без каких-либо мер безопасности. Об этом изданию The Guardian рассказал бывший подрядчик компании, в течение двух лет занимавшийся обработкой голосов пользователей с помощью личного ноутбука у себя дома в Пекине.

По словам подрядчика, работники получали доступ к записям команд голосовому помощнику Cortana и некоторых телефонных звонков в Skype через web-приложение, запущенное в браузере Google Chrome на их персональных ноутбуках с использованием китайского интернета. При этом им не оказывалась никакая помощь по защите данных от вмешательства киберпреступников или правительств. Более того, согласно инструкциям от Microsoft, для большего удобства у всех работников был один и тот же пароль, а проверка благонадежности самих работников и вовсе отсутствовала.

«Я анализировал записи на британском английском языке (я британец), поэтому прослушивал людей, установивших в настройках своих устройств Microsoft британский английский, и имел доступ к ним через свой домашний ноутбук с помощью одного лишь пароля», – сообщил бывший работник, занимавшийся анализом образцов речи пользователей. Свой логин и пароль он получил от Microsoft по электронной почте в незашифрованном виде, причем логин был очень простым, а пароль – одним для всех.

Впервые о прослушке разговоров, ведущихся через переводчик в Skype, стало известно в августе прошлого года. Как сообщалось, приложение Skype собирало и использовало записи разговоров пользователей для улучшения продуктов Microsoft, а также для развития технологии перевода и распознавания речи.

Согласно заявлению Microsoft, с тех пор компания закрыла программу обработки речи пользователей Skype и Cortana для Xbox, и перевела остальных сотрудников, занимающихся анализом образцов речи, в защищенные офисы, расположенные за пределами Китая». **(Подрядчики Microsoft прослушивали разговоры в Skype без каких-либо мер безопасности // SecurityLab.ru (https://www.securitylab.ru/news/503948.php). 13.01.2020).**

***

«Смартфоны и планшеты производства компании Samsung предположительно поставляются с предустановленным “шпионским” ПО, которое регулярно обращается к расположенным в Китае серверам. Речь идет

о функции под названием Device Care, реализованной на всех смартфонах и планшетах южнокорейского производителя.

На проблемму обратил внимание один из пользователей форума Reddit, заметивший, что данная функция имеет отношение к китайской компании Qihoo 360, ранее неоднократно фигурировавшей в скандалах, связанных со скрытым сбором данных. В то время как Samsung сама подтвердила, что модуль Storage функции Device Care работает на ПО Qihoo, компания не предоставила никакой информации относительно того, почему он отправляет данные в Китай.

“Сканнер Storage на вашем телефоне имеет полный доступ ко всем персональным данным (так как он является частью системы) и по китайским законам будет отправлять данные при соответствующих запросах”, - поясняет пользователь.

Как оказалось, при запуске функция коммуницирует с несколькими китайскими серверами, хотя в настоящее время неизвестно, какие данные передаются…

В компании Samsung пока не прокомментировали ситуацию. Тем временем, ряд пользователей ее устройств уже запустили петицию с просьбой удалить программное обеспечение Qihoo 360 со смартфонов». ***(Смартфоны Samsung заподозрили в скрытой отправке данных в Китай // SecurityLab.ru (https://www.securitylab.ru/news/503845.php). 08.01.2020).***

***

«…Конфиденциальные сведенья о знаменитостях, номинированных на специальные награды Соединенного Королевства за деятельностью на пользу стране и всей нации, пробыли в открытом доступе на протяжении нескольких часов. Список пострадавших от непонятной ошибки довольно длинный. Присутствуют в перечне и весьма знакомые имена. Легенда мировой сцены Элтон Джон, музыкант группы Queen Роджер Тейлор, кинематографисты Сэм Мендес и Стив Маккуин, бывший глава британских «Консерваторов» Иэн Данкан Смит и многие другие.

Представитель Кабинета министров Великобритании принес публичные извинения всем выдающимся людям страны, которые были удостоены знаковых наград, но пострадали от произошедшей ошибки. Сообщается также, что в связи с утечкой секретной частной информации в общий доступ, инициировано расследование. Правоохранители намерены выяснить, по каким причинам и с участием каких лиц стала вообще возможной подобная неприятная ситуация.» ***(Сайт правительства Великобритании «слил» персональную информацию английских знаменитостей // SecureNews (https://securenews.ru/sayt-pravitelstva-slil-konfidencialnie-dannie/). 02.01.2020).***

***

«…Эксперты компьютерных технологий из Техасского Университета в Сан-Антонио (UTSA) опубликовали первый обзор рисков приватности и безопасности, создаваемых электросамокатами, сопутствующими программными сервисами и приложениями.

Согласно этому обзору, который вскоре выйдет в бюллетене второго семинара ACM по автомобильной и авиационной безопасности (AutoSec 2020), хакеры имеют возможность организовывать прослушку Bluetooth-коммуникаций пользователя с электроскутером или даже вмешиваться в работу систем GPS-навигации.

Провайдеры сервисов проката электросамокатов могут подвергаться атакам типа «отказ в обслуживании». Кроме того, они часто хранят не только историю платежей подписчиков, но и их индивидуальные профили, откуда взломщик может извлечь сведения о координатах дома и работы пользователя, его предпочтениях и излюбленных маршрутах.

«Мы идентифицировали и обрисовали в общих чертах различные слабые звенья или поверхности атаки в современной экосистеме совместных поездок или микромобильности, которые потенциально могут быть использованы злоумышленниками, начиная с вывода личных данных водителей и заканчивая экономическими потерями для поставщиков услуг, дистанционным контролем за работой транспортных средств», — заявил руководитель этого исследования Муртуза Джадливала (Murtuza Jadliwala), доцент кафедры компьютерных наук UTSA.

Для гарантирования дальнейшей жизнеспособности индустрии микромобильности, по мнению автора, работающие на этом рынке компании должны задуматься не только о физической безопасности ездоков и пешеходов, но и о том как защитить себя и потребителей от серьёзных угроз кибербезопасности и конфиденциальности, привносимых этой новой технологией.» ***(Вышел первый обзор киберугроз, связанных с электросамокатами // Компьютерное Обозрение (https://ko.com.ua/vyshel_pervyj_obzor_kiberugroz_svyazannyh_s_jelektrosamokatami_131711). 29.01.2020).***

***

«Компания Comparitech, работающая в сфере информационной безопасности, объявила о том, что в конце прошлого года исследователям удалось обнаружить в открытом доступе 250 млн записей, связанных с клиентами службы поддержки Microsoft. Идентичные базы данных размещались на пяти незащищённых серверах Elasticsearch.

В сообщении говорится о том, что в БД находились записи за 14-летний период с 2005 по 2019 годы. Записи содержали переговоры сотрудников службы поддержки корпорации Microsoft с клиентами из разных стран мира. Отмечается, что все данные хранились в незащищённом виде, а доступ к ним мог получить любой пользователь сети Интернет, используя для этого свой веб-браузер.

Базы данных находились в открытом доступе около двух дней, после чего они попали в поле зрения исследователей, которые незамедлительно уведомили об инциденте Microsoft. Поисковая система BinaryEdge проиндексировала БД 28 декабря, а уже на следующий день они были обнаружены специалистом по кибербезопасности Бобом Дьяченко (Bob Diachenko). Получив уведомление, Microsoft закрыла доступ к данным 30-31 декабря, затем началось расследование инцидента, после проведения которого о нём было объявлено публично.

«Я немедленно сообщил о своей находке в Microsoft, и в течение 24 часов доступ к серверам был заблокирован. Я рад, что команда Microsoft нашла оперативное и быстрое решение этой проблемы, несмотря на то, что инцидент произошёл в канун Нового года», — сказал Боб Дьяченко.

Большая часть персональных данных клиентов была удалена из записей, попавших в открытый доступ. Однако опубликованные данные говорят о том, что в БД содержались электронные адреса, IP-адреса клиентов, поступающие от службы поддержки сообщения и др.» ***(Данные 250 млн клиентов службы поддержки Microsoft обнаружены в открытом доступе // SmartPhone.ua (http://www.smartphone.ua/news/dannye_250_mln_klientov_slujby_podderjki_microsoft_obnarujeny_v_otkrytom_dostupe_63453.html). 23.01.2020).***

***

«В прошлом месяце компания Wawa сообщила о заражении своих PoS-терминалов вредоносным ПО, а теперь данные продается на черном рынке.

На этой неделе киберпреступники выставили на продажу на крупнейшем кардинговом форуме Joker's Stash платежные данные 30 млн американцев и более 1 млн иностранцев. Массив данных продается под названием BIGBADABOOM-III. Как сообщают специалисты ИБ-компании Gemini Advisory, данные были похищены в результате взлома американской сети магазинов и автозаправочных станций Wawa. Сама сеть подтверждает этот факт.

В прошлом месяце компания Wawa сообщила о масштабной утечке данных, произошедшей в результате заражения ее PoS-терминалов вредоносным ПО. По словам представителей Wawa, вредоносная программа похитила данные всех кредитных и дебетовых карт, с помощью которых покупатели рассчитывались в их магазинах и на АЗС. Вредоносное ПО находилось в PoS-терминалах с 4 марта по 12 декабря 2019 года. Инцидент затронул все 860 магазинов Wawa (600 из них совмещены с АЗС).

По словам специалистов Gemini Advisory, инцидент является одной из крупнейших утечек платежных данных не только в 2019 году, но и за все время. По своим масштабам утечка сопоставима со взломом торговых сетей Home Depot в 2014 году (были похищены данные более 50 млн банковских карт) и Target в 2013 году (были похищены данные 40 млн банковских карт).

Как уверяют представители Wawa, злоумышленники похитили только платежную информацию, а PIN-коды, номера CVV2 и персональные данные держателей карт скомпрометированы не были. Однако в изученных журналистами ZDNet образцах похищенных данных номера CVV2 все же встречаются.

Как сообщают специалисты Gemini Advisory, стоимость данных на Joker's Stash составляет в среднем $17 за одну карту, выпущенную в США, и $210 за одну карту, выпущенную за рубежом. По их словам, выставлять данные на продажу только после того, как об утечке станет известно широкой общественности, является стандартной практикой для Joker's Stash. Операторы форума пользуются шумихой в прессе, чтобы укрепить свое положение самого известного продавца скомпрометированных платежных карт.» ***(На черном рынке выставлены на продажу данные 30 млн клиентов сети Wawa // SecurityLab.ru (https://www.securitylab.ru/news/504523.php). 29.01.2020).***

***

«Во вторник, 28 января, компания Facebook представила новую функцию «Действия вне Facebook» (Off-Facebook Activity), которая не только позволяет пользователям очищать свою историю активности за пределами соцсети, но также свидетельствует о том, что Facebook следит за ними, даже если приложение выключено.

Для подбора релевантной рекламы Facebook и принадлежащим ей Instagram и Messenger вовсе не нужно подслушивать и подглядывать за пользователями через камеры и микрофоны на их устройствах – у компании для этого есть другие инструменты. Facebook знает, когда пользователь посетил сайт поддерживаемого им политика, прочитал новость в газете, купил что-то в интернет-магазине или открыл «умный» замок с помощью приложения.

Теперь благодаря функции «Действия вне Facebook» пользователь может узнать, какие сайты и приложения отправили Facebook информацию о нем в течение последних 180 дней.

«Действия вне Facebook включают ваше взаимодействие с компаниями и организациями, о котором они нам сообщают. Например, когда вы посещаете их сайты через Facebook. […] Компании и организации, которые используют наши инструменты для бизнеса, могут передавать нам информацию о действиях на их сайтах или в приложениях. Это позволяет нам персонализировать контент, например, подбирать для вас наиболее актуальную рекламу. В соответствии с нашими требованиями компании и организации должны заранее уведомлять пользователей о том, что будут применять наши инструменты для бизнеса», - говорится в описании функции.

Функция скрыта в «Настройках» приложения и носит, скорее, информативный характер. Она действительно позволяет удалять историю активности за пределами соцсети, но это никак не повлияет ни на количество отображаемой рекламы, ни на дальнейший сбор информации, ни на подбор рекламы». ***(Facebook собирает данные об активности пользователей за пределами соцсети // SecurityLab.ru (https://www.securitylab.ru/news/504505.php). 29.01.2020).***

***

«Производитель решений безопасности Avast продает данные своих пользователей крупнейшим в мире компаниям, в том числе Google и Microsoft. Об этом узнали журналисты изданий Motherboard и PCMag в ходе совместного расследования.

Во время расследования журналисты изучили большое количество контрактов и принадлежащих другим компаниям документов, проливающих свет на то, как Avast торгует историями браузеров своих пользователей.

Судя по документам принадлежащей Avast дочерней компании Jumpshot, установленное на компьютере пользователя антивирусное ПО Avast собирает его данные, а Jumpshot «упаковывает» их в различные продукты и продает крупнейшим мировым корпорациям. В число бывших, настоящих и потенциальных покупателей входят Google, Yelp, Microsoft, McKinsey, Pepsi, Sephora, Home Depot,

Condé Nast, Intuit и пр. За продукты, содержащие «все клики» пользователя, некоторые клиенты платили миллионы долларов. Опция «все клики» позволяет клиентам с большой точностью отслеживать активность пользователей в интернете, их клики и передвижения внутри сайтов.

По данным компании Avast, число пользователей ее антивирусного ПО достигает 435 млн в месяц. Согласно документам Jumpshot, «дочка» владеет данными со 100 млн устройств. Avast утверждает, что собирает данные только пользователей, давших свое согласие, однако опрошенные журналистами пользователи не знают о продаже своих данных третьим сторонам.

Полученные Motherboard и PCMag данные включали историю поиска в Google, поиски местоположения и GPS-координаты на «Картах Google», а также сведения о том, какие сайты и когда посещал пользователь. Журналисты даже могли определить, какие порнографические ресурсы посещал пользователь, какие поисковые запросы вводил на этих сайтах и какие видео смотрел.

Хотя данные являются анонимными и не содержат имен, по словам экспертов, их вполне достаточно для деанонимизации того или иного пользователя.

Как стало известно в прошлом месяце, расширения для браузеров от Avast собирали данные об активности пользователей в интернете. Впоследствии компания была вынуждена прекратить эту практику, однако быстро нашла выход из сложившейся ситуации и стала собирать данные непосредственно через свои антивирусы.

Согласно документам Jumpshot, на прошлой неделе Avast стала запрашивать у пользователей своего бесплатного антивируса разрешение на сбор их данных. Запрос отображается в всплывающем окне, однако, как показал проведенный журналистами опрос, пользователи не знают, что речь идет о продаже их данных третьим сторонам». ***(Avast продает историю браузеров своих пользователей // SecurityLab.ru (https://www.securitylab.ru/news/504458.php). 28.01.2020).***

***

«За последние 18 месяцев, прошедших с момента вступления в силу Общего регламента защиты данных (The General Data Protection Regulation, GDPR), было зафиксировано более 160 тыс. уведомлений об утечках данных, и данное число продолжает расти с каждым днем.

По словам специалистов из юридической фирмы DLA Piper, после вступления в силу новых европейских правил о конфиденциальности в первые восемь месяцев в среднем поступало 247 уведомлений об утечках данных в день. С тех пор это число возросло до 278 уведомлений в день.

«Количество уведомлений об утечках данных увеличилось более чем на 12% по сравнению с прошлым годом, и регуляторные органы были заняты тестированием новых полномочий по санкциям и штрафам организаций», — отметили эксперты.

По оценкам специалистов, общая сумма выплаченных на сегодняшний день штрафов составляет €114 млн. Национальная комиссия по информатике и свободам (Commission nationale de l'informatique et des libertés, CNIL) Франции в 2019 году оштрафовала компанию Google на максимальную сумму в €50 млн за нарушение правил Общего регламента по защите данных касательно прозрачности при

получении согласия на обработку и использование персональной информации пользователей…» ***(За последние 18 месяцев зафиксировано 160 тыс. утечек данных // SecurityLab.ru (https://www.securitylab.ru/news/504271.php). 21.01.2020).***

***

Кібербезпека Інтернету речей

«Киберпреступник выложил в открытый доступ списки учетных данных Telnet для более 515 тыс. серверов, домашних маршрутизаторов и IoT-устройств. Как сообщает ZDNet, списки были опубликованы на популярном хакерском форуме. В них содержатся IP-адреса, логины и пароли для сервиса Telnet – протокола для удаленного доступа, позволяющего контролировать устройства через интернет.

Составляя списки, киберпреступник сканировал интернет в поисках устройств с открытыми Telnet-портами, а затем подбирал учетные данные путем подстановки заводских паролей и логинов или придуманных, но очень простых и ненадежных.

Такие списки часто называют списками ботов, поскольку они часто используются операторами IoT-ботнетов. Сначала преступники сканируют интернет, составляя список ботов, а затем используют его для подключения к устройствам и заражения их вредоносным ПО.

Как правило, подобные перечни держатся в секрете, но на этот раз список был опубликован online оператором одного из сервисов, осуществляющих заказные DDoS-атаки. По словам оператора, ботнет ему больше не нужен, поскольку он перешел на новую бизнес-модель и теперь арендует мощные серверы у облачных провайдеров.

Указанные в списках данные датируются октябрем-ноябрем 2019 года. Хотя некоторые IP-адреса и пароли с тех пор могли поменяться, списки все равно представляют большой интерес для киберпреступников.» ***(В Сети опубликованы пароли для 515 тыс. IoT-устройств // SecurityLab.ru (https://www.securitylab.ru/news/504223.php). 20.01.2020).***

***

«Правительство Великобритании обнародовало законопроект, направленный на защиту IoT-устройств.

Законопроект содержит три основных требования для производителей «умных» устройств. В частности, все пароли пользовательских IoT-устройств должны быть уникальными и без возможности сбросить их до «универсальных» заводских настроек; производители должны предоставить общедоступную точку контакта, чтобы каждый мог сообщить об уязвимости и рассчитывать на «своевременное принятие мер»; производители обязаны четко указать минимальный период времени, в течение которого устройства будут получать обновления безопасности в местах продаж

«Наш новый законопроект обязывает фирмы, производящие и продающие подключенные к интернету устройства, учитывать и пресекать действия хакеров, угрожающих конфиденциальности и безопасности людей. Это будет означать, что надежные стандарты безопасности будут внедряться на этапе проектирования, а не применяться в качестве запасного плана», — сообщил министр по цифровым и широкополосным технологиям Великобритании Мэтт Уормен (Matt Warman).

Норма была разработана Министерством по делам культуры, СМИ и спорта Великобритании после продолжительного периода консультаций, которые начались в мае 2019 года.

Как сообщили в правительстве Великобритании, законопроект планируется принять «как можно скорее». ***(Великобритания готовит закон по защите IoT-устройств // SecurityLab.ru (https://www.securitylab.ru/news/504485.php). 28.01.2020).***

***

Кіберзлочинність та кібертероризм

«Организации все чаще становятся жертвами спонсируемых правительствами киберпреступников. 25% компаний связывают атаки на их бизнес с кибервойной или действиями других государств, показали результаты опроса, проведенного специалистами из компании Radware.

В 2018 году только 19% организаций связывают в кибератаках другие государства, но в 2019 году эта цифра увеличилась до 27%. Что интересно, предприятия в Северной Америке чаще склонны связывать атаки с правительственными киберпреступниками (36%).

«Кибератаки со стороны спонсируемых правительствами преступников являются одними из самых сложных для нейтрализации, поскольку их организаторы часто располагают значительными ресурсами, знаниями об уязвимостях нулевого дня и терпением для планирования и выполнения данных операций. Подобные атаки могут привести к потере конфиденциальных, торговых, технологических или других данных», — отметили специалисты.

Как показали результаты опроса, 22% опрошенных даже не знали, были ли они атакованы, а 27% пострадавших не догадывались о мотивах преступников. 38% компаний не уверены, подвергались ли их сети атакам IoT-ботнетов, а 46% не уверены, что подверглись зашифрованным DDoS-атакам.

Хотя технологии мобильной связи 5-го поколения (5G) предоставляют прекрасную возможность для обеспечения безопасности в сетях, только 26% опрошенных подтвердили готовность к развертыванию 5G, а 32% — лишь частично подготовлены.» ***(Проправительственные кибергруппировки стали чаще атаковать компании // SecurityLab.ru (https://www.securitylab.ru/news/504224.php). 20.01.2020).***

***

«Киберпреступники начали использовать новую технику фишинга, чтобы обманом заставить сотрудников компаний устанавливать вредоносные программы, переводить деньги или передавать свои учетные данные.

Злоумышленники проникают в бизнес-каналы электронной почты, используя ранее скомпрометированные учетные данные (приобретенные на подпольных форумах, украденные или полученные путем брутфорса), и присоединяются к диалогу под видом одной из групп…

Идея заключается в том, что злоумышленник эксплуатирует реальную личность, от ее имени осуществляя фишинговые атаки, которые жертва будет расценивать как сообщения, исходящие от доверенного источника.

Как отметили специалисты, киберпреступники активно используют данную технику атаки для компрометации компаний. В ходе анализа 500 тыс. электронных писем эксперты обнаружили, что перехват переписок вырос более чем на 400% в период с июля по ноябрь прошлого года. В большинстве случаев злоумышленники не используют скомпрометированную учетную запись для отправки фишингового сообщения, поскольку владелец аккаунта может обнаружить среди исходящих почтовых сообщений подозрительное письмо.

Вместо этого преступники используют домены, отличающиеся от оригинальных и доверенных URL-адресов одним или двумя символами. Преступники полагаются на то, что жертва не заметит изменения в домене и не заподозрит в обмане коллегу, клиента или партнера. Эксперты сообщили о случаях, когда злоумышленники неделями общались со своими предполагаемыми жертвами, чтобы обеспечить высокий уровень доверия.» ***(Эксперты предупредили о новом виде фишинговых атак // SecurityLab.ru (https://www.securitylab.ru/news/504177.php). 17.01.2020).***

***

«Операторы вымогательского ПО REvil (также известного как Sodinokibi) в канун Нового года атаковали компьютерные системы биржевого провайдера Travelex, в результате чего британские банки Lloyds, Barclays, HSBC и Royal Bank of Scotland, не смогли обрабатывать транзакции.

Изначально киберпреступники требовали выкуп в размере $3 млн. в обмен на зашифрованные данные клиентов, однако теперь сумма увеличилась вдвое и составляет $6 млн. По словам представителей Travelex, система безопасности заблокировала данные в качестве «меры предосторожности» сразу после обнаружения вируса, а данные клиентов не были скомпрометированы.

«В настоящее время мы блокируем вирус и работаем над восстановлением своих систем для возобновления нормальной работы в кратчайшие сроки. Сеть Travelex продолжает предоставлять услуги по обмену валюты наличными вручную», — сообщила Travelex.

Как сообщила BBC со ссылкой на сообщение от преступников, злоумышленники скачали 5 ГБ данных о клиентах биржи и планируют продать их через шесть дней, если биржа не заплатит выкуп.

Travelex сотрудничает с Национальным криминальным агентством Великобритании (NCA) и столичной полицией Лондона, которые проводят уголовное расследование инцидента». ***(Операторы Sodinokibi требуют от***

валютной биржи Travelex $6 млн // SecurityLab.ru (https://www.securitylab.ru/news/503937.php). 10.01.2020).

***

«Киберпреступники организовали масштабную кампанию по взлому смартфонов Samsung в Южной Корее. Злоумышленники нацелены в первую очередь на знаменитостей и вымогают со своих жертв деньги, угрожая опубликовать в Сети их персональные данные.

…среди жертв есть знаменитые актеры, режиссеры, музыканты, поп-идолы, шеф-повары и пр. С каждого пострадавшего киберпреступники требуют выкуп в размере от $43 тыс. до $860 тыс.

Злоумышленники получили доступ к фотографиям, видеороликам, текстовым сообщениям и другой персональной информации многих знаменитостей. В случае отказа выплачивать выкуп, вымогатели грозят опубликовать все похищенные данные в свободном доступе. Как сообщил ресурс, пока был зафиксирован лишь один случай удовлетворения требований вымогателей – популярный певец, пожелавший остаться неизвестным, заплатил требуемую сумму для предотвращения утечки.

Однако другой известный южнокорейский актер Чжу Чженмо отказался выполнять требования преступников, в результате чего его данные незамедлительно оказались в Сети.

Компания Samsung пока что не прокомментировала данный инцидент…». **(Вымогатели взломали смартфоны Samsung южнокорейских знаменитостей // SecurityLab.ru (https://www.securitylab.ru/news/503916.php). 10.01.2020).**

***

«Американский бизнесмен, соучредитель компании по кибербезопасности, признался, что нанимал преступников для совершения кибератак на других.

Такер Престон из Мейкона, штат Джорджия, признался, что заплатил киберпреступникам за запуск серии распределенных атак типа «отказ в обслуживании» (DDoS) в период с декабря 2015 года по февраль 2016 года.

DDoS-атаки препятствуют функционированию веб-сайта, бомбардируя его таким большим количеством нежелательного интернет-трафика, что он не может обрабатывать посещения настоящих пользователей.

На прошлой неделе в суде Нью-Джерси 22-летний Престон признал себя виновным в одном из обвинений в повреждении защищенных компьютеров при передаче программы, кода или команды. Престон признался, что нанес бизнесу, на который совершались отаки, ущерб как минимум в 5000 долларов.

Обвинение, по которому Престон признал себя виновным, наказывается максимальным наказанием в виде 10 лет лишения свободы и штрафом в размере до 250 000 долларов США.

Престон является соучредителем компании BackConnect Security LLC, специализирующейся на облачной безопасности и производительности в Интернете, которая претендует на звание «нового отраслевого стандарта в области предотвращения DDoS» и в настоящее время размещается в сети с использованием

недействительного сертификата». ***(Соучредитель компании по кибербезопасности платил за DDoS атаки на конкурентов // SecureNews (https://securenews.ru/ddos-attacks-on-competitors/). 22.01.2020).***

***

«Веб-сайт, созданный для приема пожертвований жертвам разрушительного австралийского лесного пожара, сам стал жертвой цифрового кода скимминга, предназначенного для сбора информации о платежных картах.

Аналитики из Malwarebytes сообщили в Twitter о проблемах, с которыми столкнулся сайт анонимных пожертвований, который собирал деньги для тех, кто пострадал от пожаров в озере Конжола, где было разрушено множество домов.

В таких атаках в стиле Magecart хакеры, как правило, внедряют вредоносный JavaScript в страницы платежей для сбора данных пользователей и их карт. Затем он отправляется на внешний домен, который находится под контролем злоумышленников.

В этом инциденте вредоносный код был идентифицирован как «ATMZOW», а вредоносный домен, на который он отправил данные, выявлен как vamberlo [.] Com.

Отвечая на сообщение в Твиттере, Трой Мурш из охранной фирмы Bad Packets заявил, что тот же вредоносный код был обнаружен для еще 39 отдельных веб-сайтов.

«Ввиду недостаточной прозрачности таких атак на стороне клиента, владельцы веб-сайтов часто узнают о взломе данных через несколько дней или недель после внедрения кода. Это длительное время позволяет злоумышленникам максимально монетизировать украденные данные о картах», - пояснил Дипак Патель, офицер безопасности в PerimeterX.

«Любой сайт, который обрабатывает личные данные пользователя и принимает платежи, должен предпринять шаги для усиления безопасности своих приложений, отслеживая выполнение кода первым и третьим лицом на своих сайтах в режиме реального времени». ***(Атакован сайт сбора пожертвований для жертв Австралийского пожара // SecureNews (https://securenews.ru/attacked-the-website-collecting-donations/). 15.01.2020).***

***

«Більшість країн-членів Інтерполу мають недостатні можливості для боротьби із кіберзлочинами. Про це заявив генеральний секретар Інтерполу Юрген Сток під час дискусії на Всесвітньому економічному форумі у швейцарському Давосі…

«Напевно, 70-80% наших країн-членів та їхні поліцейські органи мають або слабкі, або взагалі не мають спроможностей для протидії кіберзлочинам», - сказав керівник міжнародної поліцейської організації.

Сток зазначив, що Інтерпол приділяє значну увагу кібербезпеці з метою посилення спроможностей та збирання якнайбільшого обсягу інформації у цій сфері.

Водночас, додав як додав генсек Інтерполу, функціонування міжнародної поліцейської організації базується на принципі національних суверенітетів та законодавств країн-членів.

При цьому, за словами генсекретаря, Інтерпол відчуває брак спільних стандартів у боротьбі з кіберзлочинами.

«У політичному вимірі ця ситуація залишається доволі складною, включаючи проведення транснаціональних операцій», - сказав керівник Інтерполу.» ***(Більшість країн Інтерполу не здатні протистояти кіберзлочинам, - генсек // Українські медійні системи (https://glavcom.ua/news/bilshist-krajin-interpolu-ne-zdatni-protistoyati-kiberzlochinam-gensek-654724.html). 23.01.2020).***

***

«Офіційні сайти прем'єр-міністра Греції, національної поліції та пожежної служби та кількох важливих міністерств були тимчасово відключені в результаті кібератаки…

Представник уряду Стеліос Петсас заявив, що DDoS-атака "призвела до збою в роботі деяких вебсайтів". Він сказав, що були успішно застосовані контр заходи. Зараз урядові сайти працюють у звичному режимі.

Поряд з вебсайтом прем'єр-міністра, цілями атаки, яка сталася в четвер ввечері, були сайти міністерств громадського порядку, внутрішніх справ, закордонних справ і торгового флоту, а також грецької поліції і пожежної служби.

Це була друга кібератака на урядові сайти менш ніж за тиждень. Відповідальність за першу атаку взяла на себе група хакерів з Туреччини». ***(Невідомі вчинили кібератаку на урядові сайти Греції // Чорноморські новини (https://www.blackseanews.net/read/160059). 24.01.2020).***

***

«Компания Lenovo провела собственное исследование по осведомленности пользователей в вопросах кибербезопасности. По данным компании, каждый второй пользователь сети хотя бы раз становился жертвой киберпреступников…

По данным Lenovo, 61% интернет-пользователей убеждены, что с легкостью справятся с кибератаками.

Те, кто беспокоятся о безопасности в сети, прежде всего озабочены защищенностью личных данных (73%) и возможными финансовыми потерями (69%). В свою очередь пользователи меньше всего боятся репутационных потерь (26%) и снижение производительности работы устройств (28%).

Только 3% пользователей не боятся стать жертвами киберпреступлений. Остальные 97% – ищут способы себя защитить, но в то же время недооценивают реальные угрозы. 23% опрошенных считают, что обычной осторожности в интернете достаточно, чтобы не потерять собственные данные. Думаете, только реальный мир может быть жестоким и опасным? Сегодня детей и взрослых ждет все больше угроз в цифровом пространстве, – отметил генеральный директор Lenovo в Украине Тарас Джамалов…

Двухфакторная аутентификация считается одним из самых надежных типов защиты информации. В банковском деле ее используют 73% пользователей, а вот для социальных сетей – 35%, чем упрощают доступ киберпреступникам.

Не менее надежной считают биометрическую аутентификацию, ее выбирает 54% пользователей. Чаще всего используют отпечаток пальца (43%) или же распознавание лица (21%). Реже всего – аутентификацию по радужной оболочке глаза (6%) и с помощью подписи (6%)». ***(Каждый второй пользователь становится жертвой киберпреступников: исследование // Телеканал новостей «24» (https://24tv.ua/techno/ru/kazhdyj_vtoroj_polzovatel_stanovitsja_zhertvoj_kiberprestupnikov_issledovanie_n1271331). 28.01.2020).***

***

«Смартфон основателя Amazon Джеффа Безоса вероятно был взломан в 2018 году посредством учётной записи в WhatsApp, связанной с наследным принцем Саудовской Аравии Мухаммедом бен Салманом. К такому выводу пришли эксперты по вопросам кибербезопасности, нанятые Безосом для расследования инцидента.

По данным экспертов, смартфон, вероятно, был взломан 1 мая 2018 года. В тот день Безос получил через приложение WhatsApp вредоносный файл, через который и произошло заражение. Сообщение якобы было получено от Мухаммеда бин Салмана, с которым незадолго до того Безос дружески общался в мессенджере.

На протяжении нескольких часов после заражения со смартфона Джеффа Безоса был скачан большой объём данных. Пока не уточняется, какая именно информация была похищена, и каким образом злоумышленники воспользовались ею. Однако напомним, в начале 2019 года – примерно через полгода после предполагаемой даты взлома смартфона – таблоид National Enquirer опубликовал личную переписку Джеффа Безоса и его возлюбленной Лорен Санчес. Также издатель этого таблоида шантажировал основателя Amazon, угрожая опубликовать его интимные фотографии.

Добавим, в прошлом году уже высказывались предположения, что за взломом смартфона Безоса могут стоять правительственные хакеры Саудовской Аравии. В этот раз представители посольства Саудовской Аравии в США опровергли сообщения о возможной причастности королевства к этому инциденту, назвав их «абсурдными».» ***(Вадим Карпусь. Смартфон Джеффа Безоса, вероятно, был взломан через аккаунт, связанный с принцем Саудовской Аравии // ООО «ХОТЛАЙН» (https://itc.ua/news/smartfon-dzheffa-bezosa-veroyatno-byl-vzloman-cherez-akkaunt-svyazannyj-s-princzem-saudovskoj-aravii/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+itc-ua+%28ITC.ua%29). 22.01.2020).***

***

«Десятки серверов офисов ООН в Женеве и Вене подверглись хакерским атакам.

Об этом стало известно из внутреннего конфиденциального документа ООН…

Согласно документу, хакеры атаковали 42 сервера. По поводу еще 25 серверов есть подозрение на взлом. Почти все они принадлежат офисам ООН в Женеве и Вене. Три сервера использует Управление верховного комиссара по правам человека, два - Европейская экономическая комиссия ООН…

По словам анонимного чиновника ООН, хакерские атаки впервые обнаружили еще летом. Степень вреда, утверждает собеседник агентства, остается непонятной с точки зрения личной, секретной или компрометирующей информации, которая могла быть украдена.

Уровень сложности атаки был настолько высок, что, возможно, за ним стоит правительство какой-то из стран, утверждает источник. Чиновник заверил, что с тех пор защита компьютерных систем ООН была усилена.

Техники в офисах ООН в Женеве минимум два раза работали в течение выходных в последние месяцы, чтобы изолировать местный центр обработки данных ООН от Интернета, переписать пароли и убедиться, что системы чистые…» ***(Хакеры напали на офисы ОНН в Женеве и Вене // Телеграф (https://telegraf.com.ua/mir/europa/5326131-hakeryi-napali-na-ofisyi-onn-v-zheneve-i-vene.html). 29.01.2020).***

***

«Японский производитель электрического и электротехнического оборудования Mitsubishi Electric пострадал от мощной хакерской атаки

В корпорации уже заверили, что закрытые и весьма чувствительны сведения о контрактах компании в сфере обороны, электрификации и железнодорожной отрасли не были похищены, передает "ДС" со ссылкой на Japan Times.

При этом не исключается, что хакеры могли получить доступ к личным данным сотрудников и руководства компании. Проводится расследование.

К атаке на Mitsubishi Electric могут быть причастны китайские хакерские группировки.» ***(Компания Mitsubishi Electric пострадала от хакерской атаки // DsNews (https://www.dsnews.ua/society/kompaniya-mitsubishi-electric-postradala-ot-hakerskoy-ataki-20012020082800). 20.01.2020).***

***

«Некоторые компании, заплатившие выкуп операторам вымогательского ПО, могут в конечном итоге так и не вернуть себе доступ к зашифрованным файлам. По словам исследователей из компании Proofpoint, злоумышленники иногда просто «берут деньги и сбегают».

Эксперты провели опрос среди 600 специалистов по безопасности в семи странах и обнаружили, что в 2019 году 65% организаций пострадали от вымогательского ПО, шифрующего данные. Несмотря на тот факт, что 33% компаний приняли решение выполнить требования преступников и заплатить выкуп, около 22% из них так никогда и не получили доступ к своим данным, заблокированным вредоносным ПО. 9% и вовсе сообщили, что после оплаты злоумышленники выдвинули дополнительные требования.

«В 2019 году особенно сильно пострадали организации здравоохранения, государственные и местные органы власти», — отметили эксперты.

Операторы вымогательского ПО не так давно начали публиковать в Сети похищенные данные тех, кто отказался выполнять требования преступников… Если жертва не платит выкуп, часть украденных данных будет публиковаться в Сети, пока не будет произведена оплата». ***(Заплатившие выкуп компании не всегда возвращают себе доступ к данным // SecurityLab.ru (https://www.securitylab.ru/news/504364.php). 24.01.2020).***

***

Діяльність хакерів та хакерські угруповування

«Киберпреступная группировка Fancy Bear (известная также как APT28) организовала фишинговую кампанию, направленную на сотрудников украинской нефтегазовой компании Burisma Holdings.

Как сообщили эксперты из ИБ-компании Area 1 Security, преступники нацелились на две дочерние компании Burisma — «КУБ-ГАЗ» и «ЕСКО-ПІВНІЧ» —, а также на связанную с ними «CUB Energy Inc». Злоумышленники использовали похожие домены, чтобы обманом заставить сотрудников компаний ввести свои пароли электронной почты. По словам специалистов, Burisma и ее дочерние компании используют один и тот же почтовый сервер.

Web-сайт компании подвергался многочисленным попыткам взлома в течение последних шести месяцев, однако остается неизвестным, какие данные пытались украсть преступники. По словам специалистов, направленная на сотрудников Burisma фишинговая кампания была успешной, и злоумышленникам удалось взломать один из почтовых серверов компании.

Взлом почтовых серверов Burisma мог привести к раскрытию переписки Хантера Байдена, который входил в состав совета директоров компании в период с 2014 по 2019 год. Хантер является сыном Джо Байдена — вероятного соперника на выборах президента США в 2020 году действующего президента США Дональда Трампа. Преступники, предположительно, искали компрометирующую информацию на политического конкурента». ***(Fancy Bear атаковала украинскую нефтегазовую компанию Burisma // SecurityLab.ru (https://www.securitylab.ru/news/504010.php). 14.01.2020).***

***

«Турецкие хакеры заявили, что в пятницу более чем на 90 минут захватывали официальные сайты парламента Греции, министерств иностранных дел и экономики, а также фондовую биржу страны.

На своей странице в Facebook группа хакеров Anka Neferler Tim обосновала свои действия, заявив, что «Греция угрожает Турции в Эгейском море и в восточной части Средиземного моря. А теперь она угрожает конференции по Ливии».

Взлом произошел, когда военный лидер Ливии Халифа Хафтар провел переговоры в Афинах, за два дня до мирной конференции в Берлине, на которой он

и глава признанного Триполи правительства ООН Файез Саррадж должны присутствовать.

Анкара оказывает военную поддержку правительству Сарраджа и объявила о том, что оно направляет войска в Ливию, чтобы помочь отразить атаки сил Хафтара.

Греческое правительство не было приглашено на конференцию в Берлине, целью которой является начало мирного процесса в Ливии под эгидой Организации Объединенных Наций.

Но за два дня до конференции премьер-министр Греции Кириакос Мицотакис встретился с Хафтаром, которого он призвал «поддерживать конструктивную позицию в Берлине». ***(Турецкие хакеры захватили официальные сайт парламента Греции и фондовую биржу страны // SecureNews (https://securenews.ru/turkish-hackers-seize-official-website-of-greek-parliament/). 20.01.2020).***

***

«Эксперты «Лаборатории Касперского» зафиксировали волну целевых атак на крупные банки нескольких стран Тропической Африки.

С первых дней января наблюдаются тысячи попыток запустить вредоносное ПО, в том числе модуль, который делает скриншоты экранов зараженных компьютеров. Используемые инструменты позволяют предположить, что за атакой стоит русскоговорящая группа Silence.

Злоумышленники Silence очень активны с конца 2017 года, в основном их жертвы – финансовые организации по всему миру. Типичный сценарий атаки начинается с рассылки фишинговых писем с вредоносными вложениями. Часто злоумышленники используют инфраструктуру уже зараженных организаций и отправляют сообщения от имени настоящих сотрудников. Если получатель откроет вложение, его компьютер подвергается попытке заражения сразу несколькими модулями троянца, конечная цель которых — собрать информацию об устройстве и отправить ее управляющему серверу. Один из основных модулей делает скриншоты экрана зараженного компьютера. Атакующие также используют легитимные администраторские инструменты, чтобы долго оставаться незамеченными. Проникнув в корпоративную сеть, злоумышленники изучают инфраструктуру и внутренние процессы, после этого крадут деньги, например, через банкоматы. В среднем злоумышленники пытаются вывести около миллиона долларов из каждой организации.

На основе данных об активности Silence в нескольких странах Африки, зафиксированной «Лабораторией Касперского», можно предположить, что злоумышленники уже проникли во внутреннюю сеть организаций и сейчас атаки находятся на финальных стадиях…». ***(Русскоязычные злоумышленники Silence атакуют банки Африки // IKSMEDIA.RU (http://www.iksmedia.ru/news/5637675-Russkoyazychnye-zloumyshlenniki-Sil.html). 14.01.2020).***

***

«Мощное вредоносное ПО Stuxnet, десять лет назад использовавшееся для атаки на ядерный объект в Иране предположительно спецслужбами США и Израиля, навсегда изменило подход к кибербезопасности у операторов критической инфраструктуры. Stuxnet показал, что при наличии ресурсов хакеры могут саботировать промышленные процессы, и обозначил начало новой эпохи в сфере спонсируемых государством кибератак на критическую инфраструктуру.

Спустя десятилетие эксперты по кибербезопасности все еще учатся на примере Stuxnet. Не является исключением специалист авиастроительной компании Airbus Флавиан Дола (Flavian Dola). Исследователь представил «Stuxnet-подобную» атаку на программируемые логические контроллеры (ПЛК). В частности, ему удалось повторить один из использовавшихся Stuxnet трюков – заменить запущенный на ПЛК файл вредоносным кодом и объединить функции в коммуникациях ПЛК для его выполнения.

В отличие от Stuxnet, атаковавшего два типа ПЛК от Siemens, разработанное исследователем ПО предназначено для атак на ПЛК от Schneider Electric. Дола внедрил свой код в ПЛК, имея к контроллерам физический доступ (в случае с Stuxnet атакующим пришлось сначала подключить портативный накопитель к компьютеру инженера, после чего они смогли получить доступ к контроллерам).

При определенных условиях вполне возможно осуществить «Stuxnet-подобную» атаку на ПЛК от других производителей, пришел к выводу исследователь. Хотя он использовал для атаки более старую версию ПО от Schneider Electric, сами контроллеры все еще используются на промышленных предприятиях.

Как сообщает CyberScoop, компания Airbus опубликовала исследование Долы на этой неделе, но по непонятным причинам затем удалила статью. По словам исследователя, его атака будет использоваться в рамках внутреннего «курса обучения техникам повышенной безопасности», который проведут специалисты подразделения Airbus CyberSecurity.» ***(Представлена «Stuxnet-подобная» атака на ПЛК Schneider Electric // SecurityLab.ru (https://www.securitylab.ru/news/504193.php). 17.01.2020).***

***

«Даже спустя несколько лет после масштабной кампании с использованием вымогательского ПО WannaCry, от которого пострадало множество пользователей в более чем 100 странах мира, вредонос все еще продолжает заражать новые устройства и даже в прошлом году занял первое место среди всех вымогателей.

Согласно исследованию специалистов из компании Precise Security, более 23,5% всех атак с использованием вымогательского ПО в 2019 году были связаны с WannaCry, а спам и фишинговые письма оставались самым распространенным источником заражения.

В числе факторов, ведущих к заражению, специалисты указывают спам/фишинговые письма (67%), отсутствие навыков кибербезопасности (36%),

ненадежные пароли (30%). Только 16% заражений были осуществлены через вредоносные сайты и рекламу.

Как и другие вымогатели, WannaCry шифрует файлы, хранящиеся на устройстве, и требует от пользователей платы за ключ дешифрования.

Число атак с использованием вымогательского ПО против правительственных учреждений, организаций в сфере здравоохранения, энергетики и образования продолжает расти, сообщают исследователи. Тогда как простые вымогатели блокируют устройства простым способом, более продвинутые вредоносные программы используют метод, называемый криптовирусным вымогательством». **(WannaCry стало самым опасным вымогательским ПО в 2019 году // SecurityLab.ru (https://www.securitylab.ru/news/503906.php). 10.01.2020).**

***

«Киберпреступники, предположительно спонсируемые иранским государством, применили новое вредоносное ПО Dustman в ходе атак на компьютерные сети бахрейнской национальной нефтяной компании Bapco.

Кибератака была осуществлена 29 декабря, однако злоумышленникам удалось повредить только часть компьютерной сети Bapco, сообщило Национальное управление по кибербезопасности Саудовской Аравии (National Cybersecurity Authority).

В ходе недавней атаки преступники использовали новое вредоносное ПО под названием Dustman, представляющее собой вайпер для удаления данных на зараженных компьютерах. По словам представителей CNA, Dustman представляет собой обновленную и улучшенную версию вайпера ZeroCleare, обнаруженного осенью прошлого года. Напомним, ранее SecurityLab писал о некотором сходстве ZeroCleare с вредоносным ПО Shamoon, который использовался против организаций, работающих в критически важных и экономических секторах Саудовской Аравии.

Общим компонентом данных вредоносов является легитимный набор инструментов EldoS RawDisk для взаимодействия с файлами, дисками и разделами. Вредоносы используют различные эксплоиты и методы для повышения привилегий до уровня администратора, после чего они распаковывают и запускают утилиту EldoS RawDisk для очистки данных на зараженных хостах.

Однако у Dustman есть определенные отличия от других вайперов. Все необходимые драйверы и загрузчики поставляются в одном исполняемом файле, а не в двух файлах, как в случае с ZeroCleare. Также Dustman перезаписывает том, тогда как ZeroCleare стирает том, перезаписывая его мусорными данными (0x55).

Преступники эксплуатировали уязвимости удаленного выполнения кода в VPN-устройствах компании, что позволило им проникнуть в сеть Bapco. Согласно отчету CNA, злоумышленники, предположительно, инициировали процесс очистки данных в качестве последней попытки скрыть улики после того, как ряд совершенных ошибок выявил их присутствие во взломанной сети.

Специалисты пока не смогли определить, какая именно группировка причастна к кибератаке». ***(Вайпер Dustman использовался для атаки на***

нефтяную компанию Варсо // SecurityLab.ru (https://www.securitylab.ru/news/503862.php). 09.01.2020).

***

«…Комп'ютерну мережу лікарні зламав вірус "Рюк", який заражає, насамперед, урядові й корпоративні комп'ютери, що працюють з конфіденційними даними.

Комп'ютерну мережу лікарні в Бенешові вивели з ладу в грудні торік. Установка нового системного забезпечення обійшлася Центрально-Чеському краю в 40 мільйонів крон, і ця сума не є остаточною. Вірус-вимагач "Рюк" належить до специфічних шкідливих програм і атакує вибірково, кажуть експерти.

"Угруповання, що управляє "Рюком", робить добірку потенційно цікавих мішеней. Це, здебільшого, багаті організації, які в разі "вдалого" зараження комп'ютерної мережі здатні виплатити за відновлення доступу до даних круглу суму. Якщо виходити з описаних раніше випадків, йдеться про мільйони доларів", - зазначив Мирослав Дворжак, технологічний директор антивірусної корпорації Eset.

"Рюк" належить до вірусів уповільненої дії. Потрапивши в комп'ютер, він спочатку аналізує дані, що містяться в пам'яті документи, іноді здатний відключити антивірусні програми, а потім повністю шифрує комп'ютер. Зламати шифр доступними засобами практично неможливо. Кримінальне російське угруповання, яке створило програму, потім вимагає від жертви нападу викуп.

"Єдина інформація, яку ви отримуєте від операторів "Рюка", це повідомлення про те, що ваш комп'ютер заражений цим видом вірусу, і адресу, за якою вам слід звернутися. Зазвичай це буває електронна адреса веб-пошти ProtonMail, яка шифрує повідомлення. А далі все залежить від вас, за яких умов або за які гроші ваш комп'ютер можуть дешифрувати", - пояснив Дворжак…***(Кібератаку на чеську лікарню здійснили за допомогою російського вірусу – ЗМІ // Європейську правду (https://www.eurointegration.com.ua/news/2020/01/14/7105118/). 14.01.2020).***

***

«На Android появился троян, без разрешения устанавливающий на устройства платные приложения. Под угрозой смартфоны со старыми версиями Android — версии 5.1 и ниже. Таких устройств около 25%, сообщает «Коммерсантъ» со ссылкой на экспертов Doctor Web.

Троян называется Android.Xiny.5261. Он попадает на смартфон через официальный магазин Google Play или другие сайты с приложениями для Android.

По данным Doctor Web, создатели трояна зарабатывают на партнерской программе. В ней участвуют разработчики, чьи платные приложения устанавливает троян.

В Doctor Web рассказали, что Android.Xiny.5261 нельзя удалить с устройства. Троян стирает приложения для управления root-правами, через которые пользователь мог бы удалить троянские компоненты.

Чтобы избавиться от трояна, нужно установить новую операционную систему, отметили в Doctor Web.

Трояны группы Android.Xiny появились в 2016 году. Специалист группы исследования угроз Positive Technologies Денис Кувшинов оценил ущерб от них в

миллионы рублей». ***(Наталья Бархатова. Четверть устройств на Android оказались под угрозой неудаляемого трояна // Rusbase (https://rb.ru/news/android-troyan/). 20.01.2020).***

***

«Примерно в то же время, когда напряженность в отношениях между США и Ираном начала нарастать, власти Саудовской Аравии обнаружили новый вариант вредоносного ПО для очистки данных, которое, как подозревают аналитики по кибербезопасности, создано иранскими хакерами…

Специалисты утверждают, что внедрение вредоносного ПО в сети Саудовской Аравии произошло 29 декабря и все оставленные злоумышленниками зацепки указывают именно на Иранский след.

Вредоносное ПО, используемое в атаке 29 декабря под названием Dustman, содержит несколько вредоносных файлов, в том числе очиститель, который уничтожает данные. Власти Саудовской Аравии описали Dustman как разновидность вредоносного программного обеспечения, которое использовалось при атаках по уничтожению данных против промышленных организаций на Ближнем Востоке в конце прошлого года. IBM, которая раскрыла эту атаку, приписала это APT34, хакерской группе, связанной с иранским правительством». ***(Саудовская Аравия обвиняет Иран в создании нового вредоносного ПО // SecureNews (https://securenews.ru/iran-nova-chto-to-atakuet/). 10.01.2020).***

***

«Команда исследователей Check Point Research опубликовала отчет Global Threat Index с самыми активными угрозами в декабре 2019 года. Уже три месяца лидирующую позицию занимает троян Emotet. В основном Emotet распространяется через спам-рассылки, которые используют в заголовках актуальные темы. В декабре, например, были такие темы: «Support Greta Thunberg — Time Person of the Year 2019» and «Christmas Party!».

Электронные письма в обеих кампаниях содержали вредоносный документ Microsoft Word, который при открытии пытался загрузить Emotet на компьютер жертвы. В дальнейшем через Emotet могут распространяться вымогатели и другие вредоносные кампании.

В декабре также значительно увеличилось использование удаленного внедрения команд по протоколу HTTP: этому подверглись 33% организаций во всем мире. При успешном использовании уязвимость представляла собой бот-сеть DDoS. Вредоносный файл, использованный при атаке, также содержал ряд ссылок на полезные нагрузки, использующие уязвимости в умных устройствах. В дальнейшем эти устройства объединялись в ботнеты. Потенциально уязвимы были устройства от таких производителей как D-Link, Huawei и RealTek…

Самое активное вредоносное ПО в декабре 2019 в России:

XMRig — программное обеспечение с открытым исходным кодом, впервые обнаруженное в мае 2017 года. Используется для майнинга криптовалюты Monero.

Agent Tesla — усовершенствованная RAT. AgentTesla заражает компьютеры с 2014 года, выполняя функции кейлоггера и похитителя паролей. Вредоносная программа способна отслеживать и собирать вводимые данные с клавиатуры

жертвы, делать скриншоты и извлекать учетные данные, относящиеся к различным программам, установленным на компьютер жертвы (включая Google Chrome, Mozilla Firefox и Microsoft Outlook).

Emotet – продвинутый самораспространяющийся модульный троян. Emotet когда-то был рядовым банковским трояном, а в последнее время используется для дальнейшего распространения вредоносных программ и кампаний. Новый функционал позволяет рассылать фишинговые письма, содержащие вредоносные вложения или ссылки.

Самое активное вредоносное ПО в декабре 2019 в мире:

В декабре Emotet затронул 13% организаций во всем мире, по сравнению с 9% в ноябре

Emotet – продвинутый самораспространяющийся модульный троян. Emotet когда-то был рядовым банковским трояном, а в последнее время используется для дальнейшего распространения вредоносных программ и кампаний. Новый функционал позволяет рассылать фишинговые письма, содержащие вредоносные вложения или ссылки.

XMRig — программное обеспечение с открытым исходным кодом, впервые обнаруженное в мае 2017 года. Используется для майнинга криптовалюты Monero.

Trickbot — один из доминирующих банковских троянов, который постоянно дополняется новыми возможностями, функциями и векторами распространения. Trickbot – гибкое и настраиваемое вредоносное ПО, которое может распространяться в рамках многоцелевых кампаний.

Самые активные мобильные угрозы декабря 2019:

xHelper и Guerrilla лидируют в рейтинге мобильных вредоносных программ.

xHelper — вредоносное приложение для Android, активно с марта 2019 года, используется для загрузки других вредоносных приложений и отображения рекламы. Приложение способно скрывать себя от пользовательских и мобильных антивирусных программ и переустанавливать себя, если пользователь удаляет его.

Guerilla — кликер для Android, который может взаимодействовать с сервером удаленного управления, загружать дополнительные вредоносные плагины и агрессивно накручивать клики по рекламе без согласия или ведома пользователя.

Hiddad — Модульный бэкдор для Android, который предоставляет права суперпользователя для загруженного вредоносного ПО, а также помогает внедрить его в системные процессы. Он может получить доступ к ключевым деталям безопасности, встроенным в ОС, что позволяет ему получать конфиденциальные данные пользователя.

Самые распространенные уязвимости декабря 2019:

Удаленное внедрение команд по протоколу HTTP стало самой распространенной уязвимостью, затрагивающей 33% организаций во всем мире. Уязвимости «удаленное выполнение кода MVPower DVR» и «раскрытие информации в хранилище Git на веб-сервере» на втором и третьем месте, затронули 32% и 29% организаций соответственно.

Удаленное внедрение команд по протоколу HTTP. Злоумышленники удаленно используют эту уязвимость, отправляя жертве специальный запрос.

Успешная эксплуатация позволит злоумышленнику выполнить произвольный код на устройстве жертвы.

Удаленное выполнение кода MVPower DVR. В устройствах MVPower DVR существует уязвимость удаленного выполнения кода. Злоумышленник может использовать эту уязвимость для выполнения произвольного кода в уязвимом маршрутизаторе с помощью специально созданного запроса.

Раскрытие информации в хранилище Git на веб-сервере. В Git Repository была обнаружена уязвимость, которая могла привести к раскрытию информации учетной записи».

(Вредоносные спам-кампании используют имя Греты Тунберг // KSMEDIA.RU (http://www.iksmedia.ru/news/5638205-Vredonosnye-spamkampanii-ispolzuyut.html). 16.01.2020).

***

«Лаборатория Касперского» обнаружила троянца, с помощью которого злоумышленники распространяют многочисленные рекламные объявления и без ведома владельцев устанавливают на их устройства различные приложения, а также оставляют фейковые отзывы в Google Play от их имени.

Чаще всего в декабре 2019 года зловред, получивший название Shopper, атаковал российских пользователей. Их доля составила 31%. На втором месте оказалась Бразилия с 18% заражённых пользователей, а на третьем — Индия с 13%.

Троянец эксплуатирует службу поддержки специальных возможностей Google Accessibility Service, созданную с целью облегчить использование приложений людям с ограниченными возможностями. Сервис, например, позволяет озвучивать текст в интерфейсе приложений, чтобы люди, которые не могут читать, могли слышать их содержимое. Однако злоумышленники используют его возможности для взаимодействия с интерфейсом системы и приложениями. Shopper может перехватывать данные, появляющиеся на экране, нажимать кнопки и даже имитировать жесты пользователя.

Эксперты «Лаборатории Касперского» предполагают, что троянец может попадать на устройство из мошеннических рекламных объявлений или из сторонних магазинов приложений при попытке скачать якобы легитимную программу. Вредонос притворяется системным ПО, например сервисами для очистки и ускорения работы смартфона, и маскируется под приложение с названием ConfigAPKs. Троянец собирает информацию об устройстве жертвы и отправляет её на серверы злоумышленников, а затем получает команды, в результате исполнения которых возможна реализация следующих сценариев:

Google- или Facebook-аккаунты владельца устройства могут быть использованы без его ведома для регистрации в приложениях для шопинга или развлечения;

могут быть созданы фейковые отзывы на приложения;

может быть выключена функция Google Play Protect, которая проверяет на безопасность приложения из магазина Google Play до начала загрузки;

могут быть открыты ссылки, полученные от удалённого сервера в невидимом окне;

могут выскакивать многочисленные окошки с рекламой и создаваться ярлыки для рекламных приложений в меню приложений;

без ведома владельца из Google Play могут быть скачаны и установлены приложения;

ярлыки установленных приложений могут быть изменены на ярлыки рекламных страниц.

«Сейчас Shopper в основном нацелен на онлайн-магазины, а его действие ограничивается распространением рекламы, созданием фейковых отзывов и подтасовыванием рейтингов, но нет гарантий, что его авторы остановятся на этом и не будут модифицировать зловред, добавляя в него новые функции. В любом случае, мы рекомендуем пользователям внимательно относиться к тому, из каких ресурсов они скачивают приложения и, по возможности, установить на смартфон защитное решение, чтобы минимизировать риски заражения», — отметил Игорь Головин, антивирусный эксперт «Лаборатории Касперского».

Чтобы снизить риск заражения подобными угрозами, пользователям рекомендуется:

внимательно проверять те программы, которые просят доступ к сервису Google Accessibility Service;

не скачивать приложения из сторонних источников, даже если они активно рекламируются;

использовать надёжное мобильное защитное решение, которое умеет распознавать потенциально опасные или сомнительные запросы от приложений и объяснять риски, связанные с разными типами разрешений.» ***(Россиян атакует новый троянец // IKSMEDIA.RU (http://www.iksmedia.ru/news/5637347-Rossiyan-atakuet-novyj-troyanecz.html). 13.01.2020).***

***

«…По данным Check Point 2020 Security Report, 28% организаций во всем мире подверглись атакам вредоносных многоцелевых бот-сетей. Даже если организация оснащена самыми современными продуктами безопасности, риск взлома все равно остается, он не может быть полностью устранен, сделали вывод аналитики. Организациям необходимо разработать упреждающий план для опережения киберпреступников и предотвращения потенциальных атак.

Основные тренды и методы вредоносного ПО остались те же, что и в прошлом году. К ним относится, например, криптомайнинг. Несмотря на то что в 2019 году он значительно сократился, 38% компаний по всему миру были атакованы криптомайнерами.

Целевые программы-вымогатели становятся сильнее: число целевых атак на организации относительно невелико, но они способны нанести значительный ущерб. Атаки на мобильные устройства снижаются: в 2018 году с ними столкнулись 33% организаций, в 2019 - 27%. Компании осознают угрозу и тщательнее защищают мобильные устройства сотрудников.

Атаки Magecart стали эпидемией. Вирус внедряется в веб-сайты онлайн-магазинов для кражи платежных данных клиентов. В 2019 году он заразил сотни сайтов на всех платформах, причем как крупного, так и среднего и малого бизнеса, от сетей отелей до онлайн-магазинов.

В настоящее время более 90% предприятий используют облачные сервисы. 67% специалистов по безопасности жалуются на недостаточную прозрачность их облачной инфраструктуры, безопасности и соответствия требованиям. Масштабы облачных атак и нарушений продолжали расти в 2019 году. Неправильная настройка облачных ресурсов — главная причина для облачных атак, однако произошло и увеличение числа атак, направленных непосредственно на поставщиков облачных услуг». ***(Check Point: почти треть организаций во всем мире подверглась атакам многоцелевых бот-сетей // Открытые системы (https://www.computerworld.ru/news/Check-Point-pochti-tret-organizatsiy-vo-vsem-mire-podverglas-atakam-mnogotselevyh-bot-setey). 21.01.2020).***

***

«Команда исследователей Check Point Research подготовила отчет Cyber Security Report 2020. В нем освещены основные инструменты, которые киберпреступники используют для атак на организации по всему миру, и предоставляет специалистам по кибербезопасности и руководителям компаний информацию, необходимую для защиты организаций от текущих кибератак и угроз пятого поколения.

Отчет 2020 Security Report раскрывает основные тренды и методы вредоносного ПО, которые исследователи Check Point наблюдали в прошлом году:

Криптомайнеры по-прежнему доминируют в среде вредоносного ПО – Несмотря на то, что криптомайнинг в 2019 г. значительно сократился (что связано с падением стоимости криптовалют и закрытием майнингового сервиса Coinhive в марте), 38% компаний по всему миру были атакованы криптомайнерами. Киберпреступники используют криптомайнеры, потому что риски достаточно низки, а доходность высокая.

Увеличение бот-сетей – 28% организаций по всему миру подверглись атакам ботнетов, что на 50% больше, чем в 2018 г. Emotet был наиболее распространенным вредоносным ПО для ботов, главным образом из-за его универсальности и способности распространять другие вредоносные программы и спам. Другие действия ботнета, такие как sextortion-вымогательства – (кибермошенничество с электронной почтой, основанное на эксплуатации чьей-либо половой жизни), и DDoS-атаки, также резко возросли в 2019 г.

Целевые программы-вымогатели бьют все сильнее – число целевых атак на организации относительно невелико, но они способны нанести значительный ущерб: примером могут служить атаки 2019 г. против городских администраций США. Злоумышленники тщательно выбирают жертву для атаки с целью вымогательства, чтобы получить максимальный доход.

Атаки на мобильные устройства снижаются – в 2019 г. 27% организаций столкнулись с кибератаками на мобильные устройства, по сравнению с 33% в 2018 г. Организации осознают угрозу и тщательнее защищают мобильные устройства сотрудников.

Атаки Magecart стали эпидемией – Такие атаки внедряют вредоносный код в веб-сайты онлайн-магазинов для кражи платежных данных клиентов. В 2019 г. они охватили сотни сайтов на всех платформах, причем как крупного, так и среднего и малого бизнеса: от сетей отелей до онлайн-магазинов.

Рост облачных атак – В настоящее время более 90% предприятий используют облачные сервисы. 67% специалистов по безопасности жалуются на недостаточную прозрачность их облачной инфраструктуры, безопасности и соответствия требованиям. Масштабы облачных атак и нарушений продолжали расти в 2019 г. Неправильная настройка облачных ресурсов по-прежнему является главной причиной для облачных атак, но теперь мы видим увеличение числа атак, направленных непосредственно на поставщиков облачных услуг.» ***(Количество организаций, атакованных ботнетами, выросло в 1,5 раза // Компьютерное Обозрение (https://ko.com.ua/kolichestvo_organizacij_atakovannyh_botnetami_vyroslo_v_1_5_raza_131598). 21.01.2020).***

***

«Неизвестные лица (или лицо) удаляют вредоносное ПО Phorpiex (Trik) с зараженных систем. На системах пользователей также появляется окно с рекомендацией установить антивирусное ПО и обновить компьютер.

Первоначально многие пользователи подумали, что это была шутка, закодированная внутри вредоносной программы командой Phorpiex с целью троллинга ИБ-экспертов. Однако вскоре оказалось, что вредоносное ПО в самом деле удаляется с пользовательских систем.

«Это действительно происходит. Мы внимательно следили за данным семейством вредоносных программ и недавно зафиксировали подобное поведение», — сказал руководитель отдела кибер-исследований в Check Point Янив Балмас (Yaniv Balmas) изданию ZDNet.

Балмас также поделился своими теориями касательно данной ситуации: операторы вредоноса могли собственноручно отключить ботнет, это может быть дело рук правоохранительных органов, неизвестного исследователя безопасности или же операторов конкурирующих вредоносных программ, саботирующих команду Phorpiex». ***(Кто-то удаляет вредоносное ПО Phorpiex с зараженных компьютеров // SecurityLab.ru (https://www.securitylab.ru/news/504398.php). 24.01.2020).***

***

«Новая версия ботнета Muhstik атакует уязвимые маршрутизаторы с прошивкой Tomato. Muhstik в основном запускает криптовалютные майнеры и осуществляет DDoS-атаки.

Специалисты команды Unit 42 компании Palo Alto Networks обнаружили вредоносную кампанию в начале декабря 2019 года. Результаты поискового запроса Shodan выявили около 4600 доступных в Сети маршрутизаторов с прошивкой Tomato.

Новый вариант ботнета сканирует уязвимые маршрутизаторы на предмет TCP-порта 8080 и обходит web-аутентификацию администратора путем брутфорса встроенных учетных данных. В маршрутизаторах с прошивкой Tomato учетными данными по умолчанию являются «admin: admin» и «root: admin». Он также сканирует серверы Linux с установленной системой управления содержимым сайта

WordPress и хостинговой панелью управления Webuzo и в нем реализованы модули для компрометации WebLogic-серверов.

Полезная нагрузка вредоносного ПО представляет собой двоичный файл tty0. Он содержит команды bash, которые могут выполняться на данных системах. Как отметили эксперты, первая команда используется для загрузки двоичного файла nvr.

«Файл nvr содержит команды для загрузки четырех дополнительных файлов, представляющих собой варианты IRC-ботнетов, которые работают на базе архитектур ARM и MIPS. Мы сосредоточили наш анализ на двоичном Pty5, поскольку он загружает файл daymon, представляющий собой сканер и содержащий новый модуль, нацеленный на уязвимые маршрутизаторы», — пояснили эксперты.

Затем скомпрометированное устройство отправляет команду подключения на IRC-сервер, которая содержит псевдоним устройства для присоединения к каналу…». ***(Тысячи маршрутизаторов с прошивкой Tomato уязвимы к атакам ботнета Muhstik // SecurityLab.ru (https://www.securitylab.ru/news/504353.php). 23.01.2020).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Полиция Шотландии будет использовать специальные «кибер-киоски» для взлома заблокированных устройств.

Данная технология позволит специально обученным сотрудникам осматривать мобильные устройства на предмет наличия информации, которая может представлять ценность в ходе расследования преступлений. Таким образом полиция получит возможность извлекать данные без какой-либо помощи со стороны компании-производителя устройства.

Полиция Шотландии будет проверять цифровое устройство только в тех случаях, где есть правовая основа и необходимость для расследуемого инцидента или преступления. Используемые полицией «кибер-киоски» не смогут хранить данные с цифровых устройств, поскольку после завершения обследования вся информация об устройстве будет удалена. Это позволит ускорить процесс расследования на ранних стадиях, а устройства, не имеющие отношения к делу, будут быстрее возвращены владельцам.

В общей сложности полиция закупила 41 «кибер-киоск», которые будут размещены в полицейских участках. Ожидается, что все устройства будут введены в эксплуатацию к концу мая 2020 года.» ***(Полиция Шотландии сможет взламывать смартфоны с помощью «кибер-киосков» // SecurityLab.ru (https://www.securitylab.ru/news/504215.php). 17.01.2020).***

***

«ФБР изъяло домен WeLeakInfo.com за предоставление пользователям платного доступа к данным, утекшим в Сеть в результате взломов. Операция была проведена совместно с Национальным агентством по борьбе с преступностью в Великобритании (National Crime Agency, NCA), Корпусом национальной полицейской службы Нидерландов (Netherlands National Police Corps), Федеральным ведомством уголовной полиции Германии (Bundeskriminalamt) и полицией Северной Ирландии (Police Service of Northern Ireland).

«Web-сайт предоставлял пользователям доступ к поисковой системе для просмотра конфиденциальной информации, незаконно полученной в результате более чем 10 тыс. утечек данных, включающих более 12 млрд проиндексированных записей, в том числе имена, адреса электронной почты, логины, номера телефонов и пароли», — сообщается на сайте Министерства юстиции США.

Стоимость подписки варьировалась от $2 до $75 и предоставляла пользователям неограниченный доступ к поисковой системе и данным на ограниченный период времени.

В настоящее время сотрудники правоохранительных органов ищут дополнительную информацию о владельцах сайта. Владельцы We Leak Info пока не прокомментировали данную ситуацию.» ***(ФБР изъяло домен WeLeakInfo за продажу доступа к похищенным данным // SecurityLab.ru (https://www.securitylab.ru/news/504194.php). 17.01.2020).***

***

«Кибер-преступник был заключен в тюрьму на девять месяцев за совершение преступлений против Национальной лотереи Великобритании.

Как сообщило Национальное агентство по преступности Великобритании (NCA), 29-летний Анвар Батсон из Лондона был осужден за мошенничество и четыре нарушения в соответствии с Законом о неправомерном использовании компьютеров 1990 года. Мужчина был арестован в мае 2017 года и первоначально отрицал свою причастность, утверждая, что он стал жертвой хакеров. Но позже признал себя виновным после того, как следователи обнаружили на его компьютере разговоры между ним и другими участниками преступления.

По данным NCA, Батсон использовал Sentry MBA для запуска атак против Камелота - компаний, которая управляет национальной лотереей.

Среди других лиц, которые совершали совместно с Батсоном нападения на Камелот, были 27-летний Дэниел Томпсон из Ньюкасла и 21-летний Идрис Кайоде Акинвунми из Бирмингема. Томпсон и Акинвунми были приговорены в июле 2018 года к восьми и четырем месяцам тюремного заключения соответственно.

Когда в ноябре 2016 года Камелот объявил о нападении на Национальную лотерею, компания заявила, что хакеры получили около 26 500 учетных записей. NCA сообщает, что в базе данных клиентов Национальной Лотереи приблизительно 9 миллионов записей.

Ранее Камелот утверждал, что злоумышленники не взломали ни одну из его систем, и в компании заверяли, что пострадавшие клиенты не понесут никаких финансовых потерь в результате кибератаки.

Тем не менее, в пятницу 10 января NCA заявило, что Акинвунми украл 13 фунтов со счета одного игрока в лотерею, имя пользователя и пароль которого он

получил от Бэтсона». ***(Хакер, взломавший Национальную лотерею Великобритании, приговорен к тюремному заключению // SecureNews (https://securenews.ru/national-lottery-hacker-jailed/). 13.01.2020).***

***

«Двадцатилетний житель Кемерова «заработал» 4,5 млн руб. с помощью вредоносного ПО, но отделался лишь условным сроком.

Как сообщает местная пресса, за небольшую сумму (не более 5 тыс. руб.) молодой человек приобрел в даркнете инфостилеры и в период с апреля 2018-го по февраль 2019 года заражал им компьютеры пользователей. Похищенные с помощью вредоносного ПО логины и пароли злоумышленник продавал третьим сторонам.

Кемеровчанин был задержан сотрудниками ФСБ, и против него было возбуждено уголовное дело. Суд назначили молодому человеку наказание в виде двух лет лишения свободы условно. Также решается вопрос о передаче полученных им незаконным путем средств в пользу государства…». ***(Инфостилер принес молодому кемеровчанину 4,5 млн руб. // SecurityLab.ru (https://www.securitylab.ru/news/504354.php). 23.01.2020).***

***

Технічні аспекти кібербезпеки

«Некоторые легитимные и встроенные функции в промышленных системах, работающих в сферах нефтегазовой, энергетической, нефтеперерабатывающей и химической промышленности, могут подвергать системы угрозе атак.

В большинстве случаев злоумышленники могут воспользоваться встроенными специализированными функциями, просто изменив конфигурации и настройки. По словам специалиста Марка Карригана (Mark Carrigan) из компании PAS Global, для осуществления атак даже не нужно применять вредоносное ПО. Специалисты изучили около 10 тыс. промышленных систем с целью выявить уязвимые функции.

Как оказалось, многие из этих систем являются устаревшими и имеют небезопасные встроенные функции для упрощения работы инженеров. Обновить их непросто, говорит Карриган, а устранение некоторых слабых мест может повлечь за собой сбой в работе системы и производственном процессе.

Специалисты не указывают названия затронутых поставщиков. Отмечается, что в 10 тыс. промышленных систем было обнаружено около 380 тыс. известных уязвимостей, большинство из которых были связаны с Microsoft Windows. В числе обнаруженных уязвимостей проблемы, связанные с выходными данными, ЧМИ (человеко-машинный интерфейс), использованием вшитых учетных данных для инженеров и пр.

Подробные результаты исследования будут представлены 21 января 2020 года на ИБ-конференции S4x20 ICS в Майами, США.» ***(Встроенные функции АСУ***

ТП подвергают системы риску атак // SecurityLab.ru (https://www.securitylab.ru/news/504058.php). 15.01.2020).

***

Виявлені вразливості технічних засобів та програмного забезпечення

«В пятницу, 17 января, компания Microsoft выпустила уведомление безопасности, в котором представила способы обхода критической уязвимости в Internet Explorer, эксплуатируемой киберпреступниками в реальных атаках.

Согласно уведомлению, уязвимость (CVE-2020-0674) связана с тем, как скриптовый движок обрабатывает объекты в памяти браузера. «Уязвимость может вызвать повреждение памяти, что позволит атакующему выполнить произвольный код в контексте текущего пользователя», - сообщается в уведомлении.

Эксплуатация уязвимости позволит злоумышленнику получить на уязвимой системе те же привилегии, что и у авторизованного пользователя. Если авторизованный пользователь является администратором, атакующий получит полный контроль над системой – сможет устанавливать и деинсталлировать программы, осуществлять различные действия с данными и создавать учетные записи с полными правами пользователя.

Для проведения web-атаки злоумышленник должен создать особым образом сконфигурированный сайт, способный проэксплуатировать уязвимость, а затем заманить на него жертву, например, с помощью ссылки в электронном письме.

В настоящее время Microsoft работает над патчем, который может выйти вне запланированных обновлений, как в случае с сентябрьским патчем для уязвимости нулевого дня в Internet Explorer (CVE-2019-1367).» ***(Microsoft уведомила об уязвимости нулевого дня в Internet Explorer // SecurityLab.ru (https://www.securitylab.ru/news/504218.php). 18.01.2020).***

***

«Компания Oracle выпустила обновления безопасности, устраняющие в общей сложности 334 уязвимости в 93 различных продуктах.

Исправлены проблемы во флагманском сервере базы данных Oracle, которые могут быть удаленно проэксплуатированы неавторизованным злоумышленником, в том числе уязвимость в контейнере сервлетов Apache Tomcat (CVE-2019-10072), в шлюзе базы данных Big Red (CVE-2020-2512) и в компоненте Core RDBMS (CVE-2020-2510).

В коммуникационных приложениях Oracle было обнаружено в общей сложности 25 уязвимостей, 23 из которых могут быть проэксплуатированы неавторизованным пользователем. Шесть из них получили оценки в 9 или выше баллов по шкале CVSS.

В семействе связующих технологий Oracle для создания инфраструктуры приложений Fusion Middleware исправлено 38 проблем, три из которых (CVE-2020-

2555, CVE-2020-2551, CVE-2020-2546) получили оценки в 9,8 балла по шкале CVSS.

Операционная система Solaris получила 10 патчей, а в системе хранения данных Sun ZFS Storage Appliance была устранена уязвимость удаленного выполнения кода (CVE-2019-9636).

Администраторам уязвимых устройств настоятельно рекомендуется как можно скорее протестировать и применить все исправления от Oracle.» ***(Oracle исправила 334 уязвимости в своих продуктах // SecurityLab.ru (https://www.securitylab.ru/news/504136.php). 16.01.2020).***

***

«На следующий день после выхода исправления для одной из самых опасных уязвимостей за всю историю Windows исследователь безопасности Салим Рашид (Saleem Rashid) продемонстрировал, как с ее помощью можно выдать вредоносный сайт за любой сайт в интернете с точки зрения криптографии.

Речь идет об уязвимости CVE-2020-0601 в криптографической библиотеке crypt32.dll в Windows, позволяющей подписывать вредоносные файлы таким образом, чтобы система принимала их за легитимные, а также подделывать цифровые сертификаты. Проблема была обнаружена специалистами Агентства национальной безопасности США, сообщившими о ней Microsoft.

В среду, 15 января, Рашид опубликовал в Twitter скриншот, на котором видно, как музыкальное видео Never Gonna Give You Up популярного певца 1980-х Рика Эстли играет на сайтах Github.com и NSA.gov. С помощью уязвимости исследователю удалось осуществить в браузерах Edge и Chrome спуфинг сайтов Github и АНБ США.

Созданный Рашидом эксплоит состоит из 100 строк кода, однако его можно легко сжать до 10 строк, если урезать «несколько полезных фишек», сообщил исследователь изданию Ars Technica.

Хотя проэксплуатировать уязвимость не так-то просто, и для осуществления атаки требуется соблюдение ряда условий, АНБ назвало ее высокоопасной, и представленная Рашидом PoC-атака объясняет, почему. Согласно опубликованном агентством уведомлению безопасности, опытный хакер может «очень быстро» сообразить, как проэксплуатировать ее.

Другие ИБ-эксперты разделяют мнение коллег из АНБ. «Вот что Салим только что продемонстрировал: с помощью [короткого] скрипта можно создать сертификат для любого сайта, и он будет доверенным в IE и Edge при стандартных настройках Windows. Это ужасно. Проблема затрагивает VPN-шлюзы, VoIP, практически все, что использует сетевые коммуникации», - сообщил руководитель отдела безопасности MongoDB Кенн Уайт (Kenn White).» ***(Представлена первая PoC-атака с эксплуатацией уязвимости в Windows // SecurityLab.ru (https://www.securitylab.ru/news/504149.php). 16.01.2020)/***

***

«В рамках «вторника исправлений» 14 января 2020 года компания Intel исправила шесть уязвимостей в своих продуктах, в том числе высокоопасную

уязвимость в VTune и баг в драйверах Intel Processor Graphics drivers для Windows и Linux. Эти уязвимости позволяют авторизованному атакующему вызвать отказ в обслуживании и повысить свои привилегии на системе, тогда как остальные могут привести к раскрытию информации.

Наибольшую опасность представляет уязвимость (CVE-2019-14613) в приложении Intel VTune Amplifier для Windows, позволяющая локальному авторизованному атакующему повысить свои привилегии. Проблема была обнаружена специалистами Intel в ходе внутреннего тестирования. По шкале оценивания опасности CVSS уязвимость получила 8,1 балла из максимальных 10.

Далее следует CVE-2019-14601, получившая оценку 6,7 балла. Проблема затрагивает Intel RWC 3 для Windows и позволяет локальному авторизованному атакующему повысить свои привилегии.

Уязвимость (CVE-2019-14600) в Intel SNMP Subagent Stand-Alone для Windows также позволяет локальному авторизованному атакующему повысить свои привилегии. Опасность уязвимости оценивается в 6,5 балла.

Уязвимость в Intel Processor Graphics (CVE-2019-14615) позволяет раскрыть информацию. Проблема получила оценку 6,3 балла.

Уязвимость в утилите Intel Chipset Device Software INF» ***(CVE-2019-14596), позволяющая вызвать отказ в обслуживании, получила оценку 5,9 балла. (Intel исправила шесть уязвимостей в своих продуктах // SecurityLab.ru (https://www.securitylab.ru/news/504103.php). 16.01.2020).***

***

«Фонд Cloud Native Computing Foundation (CNCF), занимающийся управлением Kubernetes, совместно с Google и HackerOne запустил программу вознаграждения за найденные уязвимости в данном ПО. Размер вознаграждения будет варьироваться от $100 до $10 тыс. Программа в течение нескольких месяцев работала в закрытом режиме, но теперь в ней могут принять участие все желающие исследователи безопасности.

Программа охватывает все основные компоненты Kubernetes. В частности, организаторов интересуют проблемы, связанные с кластерными атаками, такие как уязвимости повышения привилегий, обхода аутентификации и удаленного выполнения кода в экземплярах и API-серверах. Также будут рассматриваться отчеты об утечках информации о рабочих процессах или неожиданных изменениях разрешений.

Программа не распространяется на инструменты управления сообществом, например, списки рассылок Kubernetes или канал Slack. Выход из окружения контейнера, атаки на ядро Linux либо зависимости, такие как etcd, также не будут рассматриваться. Более подробную информацию о программе и размере вознаграждений можно узнать по данной ссылке. Kubernetes — открытое программное обеспечение для автоматизации развертывания, масштабирования контейнеризированных приложений и управления ими.» ***(Запущена программа bug bounty для Kubernetes // SecurityLab.ru (https://www.securitylab.ru/news/504095.php). 15.01.2020).***

***

«Специалисты компании Check Point опубликовали отчет о серьезных уязвимостях в популярном приложении TikTok. С их помощью злоумышленники могли не только похищать данные пользователей, но и манипулировать их статусами в профиле и видео.

В частности, уязвимости позволяли получать доступ к чужим учетным записям и манипулировать их контентом, удалять и загружать видео, делать скрытые видеоролики видимыми для всех и раскрывать сохраненную в аккаунте персональную информацию (например, электронный адрес).

В ходе исследования безопасности приложения эксперты обнаружили, что сайт TikTok позволяет от своего имени отправлять SMS-сообщения на любые номера телефонов. Злоумышленник может осуществить спуфинг сообщения, изменив параметр download_url в перехваченном HTTP-запросе, вставить любую, в том числе вредоносную, ссылку и отправить ее пользователю от имени команды TikTok.

Злоумышленник может осуществить реинжиниринг поддельной ссылки и отправить TikTok запросы вместе с cookie-файлами жертвы. Здесь могут быть проэксплуатированы другие обнаруженые исследователями уязвимости. Даже без межсайтовой подделки запросов злоумышленник может выполнить JavaScript-код и совершать действия от лица пользователя. С помощью комбинации POST- и GET-запросов атакующий может менять настройки приватности скрытых видео, создавать новые ролики и публиковать их в учетной записи жертвы.

Выполнение JavaScript-кода также позволяет получать персональную информацию жертвы через существующие вызовы API, однако для этого атакующему сначала придется обойти механизмы безопасности SOP (правило ограничения домена) и CORS (совместное использование ресурсов между разными источниками).

Разработчик приложения исправил уязвимости до публикации отчета исследователей». **(В приложении TikTok исправлены серьезные уязвимости // SecurityLab.ru (https://www.securitylab.ru/news/503899.php). 09.01.2020).**

***

«Исследователи обнаружили уязвимость в программном коде Microsoft Access, которая, если ее не исправить, может привести к утечке данных на тысячах предприятий в США и по всему миру, использующих офисное программное обеспечение.

Ошибка, обнаруженная командой исследовательской лаборатории Mimecast, может привести к раскрытию конфиденциальной информации. По оценкам Mimecast, около 85 тыс. предприятий США находятся в опасности. Однако, исследователи пока не верят в то, что компании подверженные риску, будут скомпрометированы.

Утечка информации очень похожа на ту, что была обнаружена в Microsoft Office в прошлом году. Приложение будет случайным образом сохранять фрагменты данных, называемые элементами памяти, в каждый файл. Обычно это просто фрагмент бесполезного контента, но иногда это может быть что-то деликатное или важное, например, пароли или личная информация пользователя.

Для пытливого и терпеливого хакера это может быть довольно ценной информацией…

Microsoft выпустила патч для исправления проблемы. Mimecast рекомендует компаниям загружать и устанавливать это исправление, а также следить за сетевым трафиком, чтобы отслеживать, как злоумышленники ищут потенциально важные файлы». ***(Романов Роман. Уязвимость Microsoft Access делает доступными данные 85-ти тысяч предприятий // Internetua (http://internetua.com/uyazvimost-microsoft-access-delaet-dostupnymi-dannye-85-ti-tysyacs-predpriyatii). 08.01.2020).***

***

«…Агентства національної безпеки США прокинулася совість, і воно вирішило попередити компанію Microsoft, а разом з нею і всіх користувачів десятої «вінди», що в архітектурі системи є вразливість. Крім людей, що використовують Windows 10, небезпеки піддаються також користувачі двох останніх версій Windows Server.

Microsoft не було відомо про дану вразливість, але зловмисники також не чули про неї і скористатися не встигли.

…Крім людей, що використовують Windows 10, небезпеки піддаються також користувачі двох останніх версій Windows Server». ***(Користувачі Windows 10 опинилися в небезпеці через один файл // Українські медійні системи (https://glavcom.ua/world/hitech/koristuvachi-windows-10-opinilisya-v-nebezpeci-cherez-odin-fayl-653536.html). 18.01.2020).***

***

«Компания Mozilla ищет добровольцев для поиска уязвимостей в ночных сборках браузера Firefox. Данную ситуацию компания объясняет освободившимися позициями после «недавних увольнений».

Как сообщается в отправленных компанией электронных письмах, поиск ошибок не займет более 30 минут в неделю, и «это хороший способ узнать больше о структуре Firefox и взаимодействовать с его кодом».

«Из-за недавних увольнений в нашей новой программе Nightly Crash Triage есть много свободных позиций, поэтому, если у вас есть лишнее время, пожалуйста, приходите и помогайте нам! Суть программы заключается в поиске ошибок в работе конкретной версии ночных сборок и их регистрации», — пояснила компания.

Недавно Mozilla сократила 70 сотрудников по всему миру, объяснив решение тем, что в 2019 году компания получила меньше выручки от новых продуктов по подписке, чем ожидалось…» ***(Mozilla набирает волонтеров для поиска уязвимостей в Firefox // SecurityLab.ru (https://www.securitylab.ru/news/504522.php). 29.01.2020).***

***

«Нидерландский исследователь, использующий псевдоним Ollypwn, опубликовал PoC-коды для двух критических уязвимостей (CVE-2020-0609 и CVE-2020-0610) в шлюзовом сервере удаленного рабочего стола Windows RD Gateway в Windows Server (2012, 2012 R2, 2016 и 2019).

Вышеупомянутые проблемы, получившие коллективное название BlueGate, представляют собой уязвимости предаутентификационного удаленного выполнения кода. Обе были исправлены Microsoft в рамках январского выпуска обновлений безопасности.

Согласно описанию техногиганта, «уязвимость проявляется при подключении неавторизованным пользователем к целевой системе по RDP и отправке специально сформированного пакета». Проблема затрагивает только транспортный уровень UDP (порт UDP 33910), а ее эксплуатация не требует взаимодействия с пользователем.

Опубликованные Ollypwn эксплоиты предоставляют возможность вызвать отказ в обслуживании на уязвимых системах. Кроме того, они также содержат встроенный сканер для проверки систем на наличие уязвимостей CVE-2020-0609 и CVE-2020-0610.

Известный эксперт Маркус Хатчинс (Marcus Hutchins) также предложил сканер для проверки систем на уязвимость. Отмечается, что инструмент являляется демонстрационным и не предназначен для широкого применения.

На данный момент нет информации о попытках эксплуатации вышеуказанных уязвимостей. Согласно результатам поиска Shodan, в настоящее время в Интернете доступно более 15 тыс. уязвимых RDP Gateway серверов. Для защиты от потенциальной эксплуатации эксперты рекомендуют установить соответствующие обновления либо отключить UDP или защитить порт UDP (порт 3391) межсетевым экраном.

Шлюз удаленных рабочих столов - решение для предоставления услуг виртуального рабочего стола внешним пользователям для доступа к внутренним ресурсам. RD Gateway способен защищать связь с клиентами через туннель SSL и может использовать HTTP или UDP в качестве транспортного уровня». ***(Опубликованы эксплоиты для критических уязвимостей в Windows RD Gateway // SecurityLab.ru (https://www.securitylab.ru/news/504405.php). 26.01.2020).***

***

«Специалист из ИБ-компании IOActive Джейсон Ларсен (Jason Larsen) взломал компьютерную сеть подстанций европейской энергетической компании, используя один из методов группировки Sandworm.

Первый этап атаки заключался в получении доступа с правами суперпользователя на прошивке конвертера Moxa, что заняло у него 14 часов. Для того чтобы проникнуть в компьютерную систему энергетической компании, Ларсен нацелился на преобразователь Serial to Ethernet (STEC), транслирующий команды от устройств на системы управления подстанцией предприятия.

В конце 2015 года злоумышленники из группировки Sandworm воспользовались данным методом для осуществления атак с применением вредоносного ПО на украинскую энергетическую компанию «Прикарпатьеоблэнерго». Преступники атаковали сетевое оборудование и преобразователи Serial to Ethernet (STEC), оставив без электроснабжения большую часть Ивано-Франковской области и сам город.

Ларсен изучил прошивку на устройстве и обнаружил уязвимость, которая позволяла ему извлекать данные из памяти устройства и восстанавливать пароль.

Как в случае с Sandworm, исследователь внедрил имплант в прошивку для управления конвертером.

Затем он проник в сеть подстанции энергокомпании, которая отвечает за преобразование энергии с высокого на низкое напряжение, чтобы ее можно было доставлять в дома и на предприятия. Он использовал внедренный имплант для манипулирования данными, проходящими через преобразователь, что позволяло избежать обнаружения.

Хотя Ларсен совершил данную атаку еще несколько лет назад, свои выводы он представил лишь недавно на конференции S4 в Майами-Бич (США). Он воздержался от обнародования подробностей атаки, пока производитель конвертера Моха не выпустил патч для уязвимости». ***(Эксперт имитировал атаку Sandworm на энергокомпанию // SecurityLab.ru (https://www.securitylab.ru/news/504403.php). 24.01.2020).***

***

«Специалисты из компании CyberMDX обнаружили шесть уязвимостей в ряде медицинских устройств компании GE Healthcare, пять из которых являются критическими. Эксплуатация проблем, получивших общее название «MDhex», позволяет злоумышленникам отключать устройства, собирать персональную медицинскую информацию, изменять настройки сигналов тревоги и удаленно выполнять произвольный код.

Уязвимости содержатся в версиях CARESCAPE Central Information Center 4.X и 5.X, телеметрическом сервере ApexPro (4.2 и ниже), Central Station (1.X и 2X), Telemetry Server (4.2 и ниже, а также 4.3), мониторах пациента B450 (2.X), B650 (1.X и 2.X) и B850 (1.X и 2.X).

«Хотя компания GE Healthcare отказалась комментировать точное количество уязвимых устройств, используемых по всему миру, предполагается, что их количество исчисляется сотнями тысяч», — отметили эксперты.

Эксплуатация первой уязвимости (CVE-2020-6961) позволяет злоумышленнику получить доступ к закрытому SSH-ключу в файлах конфигурации в связи с хранением учетных данных в незашифрованном виде. Вторая уязвимость (CVE-2020-6962) связана с некорректной проверкой входных данных в web-утилите конфигурации системы. Ее эксплуатация позволяет удаленно выполнить произвольный код. Третья (CVE-2020-6963) проблема позволяет получить встроенные учетные данные в ОС Windows XP Embedded (XPe) по SMB-протоколу и удаленно выполнить произвольный код. Четвертая уязвимость (CVE-2020-6964) содержится в интегрированном сервисе для переключения клавиатур уязвимых устройств. Отсутствие аутентификации для критически важных функций позволяет злоумышленнику получить удаленный доступ с клавиатуры. Пятая уязвимость (CVE-2020-6966) связана с использованием слабой схемы шифрования для управления удаленным рабочим столом, которая позволяет злоумышленнику удаленно выполнить код. Данные уязвимости получили максимальную оценку в 10 баллов по шкале CVSS v3.1.

Последняя уязвимость (CVE-2020-6965) содержится в механизме обновления программного обеспечения. Ее эксплуатация позволяет авторизованному злоумышленнику через специально сформированный пакет обновления загружать

произвольные файлы в систему. Уязвимость получила оценку в 8,5 балла по шкале CVSS.

Эксперты сообщили GE об обнаруженных уязвимостях, и компания в настоящее время разрабатывает патчи для них». ***(В медицинском оборудовании GE Healthcare обнаружены критические уязвимости // SecurityLab.ru (https://www.securitylab.ru/news/504387.php). 24.01.2020).***

***

«Специалисты Университета имени Бен-Гуриона в Негеве (Израиль) представили атаку Chameleon, позволяющую модифицировать контент в соцсетях.

Исследователи проанализировали семь платформ и выявили на Facebook, Twitter и LinkedIn одну и ту же серьезную уязвимость. Как правило, Twitter не позволяет редактировать публикации, а Facebook и LinkedIn отмечают, что пост был отредактирован. Однако атака Chameleon позволяет обойти это.

«Представьте, вы увидели в своей ленте новостей в Facebook милое видео с котенком и поставили “лайк”, а на следующий день вам звонит друг и спрашивает, почему вы “лайкнули” видео с казнью ДАИШ. Вы возвращаетесь назад, и действительно, там стоит ваш “лайк”», - сообщили исследователи.

Представленная специалистами атака позволяет менять то, как контент отображается пользователям, без каких-либо изменений, пока пользователь сам не вернется и не посмотрит еще раз. Содержание публикации уже будет другим, но все комментарии и «лайки» к публикации сохранятся.

Для осуществления атаки Chameleon злоумышленник сначала собирает информацию о жертве. Затем он создает публикации или профили с ссылками и привлекает внимание жертвы, как в случае с фишинговыми атаками. Злоумышленник завоевывает доверие пользователей, собирает социальный капитал и взаимодействует с жертвами. Этот этап очень важен для успеха атаки Chameleon, независимо от того, является она целенаправленной или нет.

Исследователи уведомили Facebook, Twitter и LinkedIn о проблеме, но их ответ оказался неубедительным. Представители Facebook заявили, что описанная атака является фишинговой и не подходит для участия в программе bug bounty. По словам администрации Twitter, ей уже было известно о проблеме ранее, а в LinkedIn согласились провести расследование». ***(Атака Chameleon позволяет менять контент в Facebook, Twitter и LinkedIn // SecurityLab.ru (https://www.securitylab.ru/news/504341.php). 22.01.2020).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Национальный институт стандартов и технологий США (The National Institute of Standards and Technology, NIST) разработал инструмент для

управления рисками конфиденциальности NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management.

Конфиденциальные данные включают информацию о конкретных людях, такую как адреса или номера социального страхования, которую компания может собирать и использовать для своих целей. Поскольку подобную информацию можно использовать для идентификации людей, организация должна гарантировать их безопасность. Разработанная платформа предоставляет полезный набор стратегий защиты конфиденциальности для организаций, которые хотят улучшить свой подход к использованию персональных данных и их защите.

NIST Privacy Framework поможет организациям управлять рисками конфиденциальности, связанными с их продуктами и услугами, а также соблюдать законы, которые могут на них повлиять, такие как Калифорнийский закон о защите прав потребителей (The California Consumer Privacy Act) и Общий регламент ЕС по защите персональных данных (General Data Protection Regulation).

Privacy Framework разработан на основе платформы NIST Cybersecurity, что использовать их совместно. Privacy Framework состоит из трех разделов: один посвящен практикам защиты конфиденциальности, второй — действиям, которые должна предпринять организация для наиболее эффективного достижения целей, а третий — оптимизации ресурсов для управления рисками конфиденциальности.» ***(NIST разработал инструмент для управления рисками конфиденциальности // SecurityLab.ru (https://www.securitylab.ru/news/504258.php). 20.01.2020).***

***

«В четверг, 16 января, компания Google выпустила новую версию своего браузера Chrome 79.0.3945.130, в которой реализовала защиту от атак с эксплуатацией недавно исправленной уязвимости в Windows.

Речь идет об уязвимости CVE-2020-0601 в криптографической библиотеке crypt32.dll, о которой Microsoft стало известно от специалистов Агентства национальной безопасности США. С ее помощью злоумышленник может создать TLS-сертификат или цифровую подпись для кода и осуществить спуфинг любого сайта в интернете. Проблема была исправлена производителем с выходом январских обновлений безопасности. На следующий же день после выхода патча была представлена PoC-атака с эксплуатацией уязвимости.

В новую версию Chrome был добавлен код, позволяющий браузеру более глубоко изучить целостность цифрового сертификата сайта, прежде чем позволить пользователю на него зайти. По словам разработчика кода, специалиста Google Райана Сливи (Ryan Sleevi), новая функция дополнительной проверки сертификатов не безупречна, но является хорошим временным решением, пока пользователи устанавливают обновления на свои Windows-устройства, а Google работает над более совершенными технологиями проверки.

«Она (новая функция – ред.) не идеальна, но ее вполне достаточно для проверки безопасности до тех пор, пока мы не перейдем на наш инструмент верификации или не усилим блокировку модулей 3P, даже для CAPI», – сообщил Сливи.» ***(Новая версия Chrome получила защиту от атак через уязвимость в crypt32.dll // SecurityLab.ru (https://www.securitylab.ru/news/504180.php). 17.01.2020).***

***

«Команда безопасности пакетного менеджера npm (Node Package Manager) для экосистемы JavaScript удалила вредоносный пакет, похищавший данные с UNIX-подобных систем. Речь идет о пакете 1337qq-js, загруженном в репозиторий npm 30 декабря 2019 года. Вредонос находился в репозитории до 13 января, и к тому времени, как его обнаружили специалисты из Microsoft Vulnerability Research, был загружен по крайней мере 32 раза.

Как показал проведенный командой npm анализ 1337qq-js, пакет похищает чувствительные данные с помощью установки скриптов и нацелен исключительно на UNIX-подобные системы. Вредонос похищает такие данные, как переменные среды, запущенные процессы, содержимое /etc/hosts, функция uname –a и файл npmrc.

Похищение переменных среды представляет большую угрозу безопасности, поскольку в некоторых JavaScript web- и мобильных приложениях неизменяемые пароли и токены доступа API хранятся в виде переменных среды.

Команда npm рекомендует разработчикам, загрузившим или использовавшим пакет 1337qq-js в своих проектах, удалить его с систем и осуществить ротацию скомпрометированных учетных данных.

За последние несколько лет из репозитория npm вредоносные пакеты удалялись несколько раз. К примеру, в августе прошлого года был обнаружен пакет bb-builder, похищавший учетные данные с систем, на которых он был установлен. Вредонос находился в репозитории в течение года.» ***(Вредоносный пакет npm похищает данные с UNIX-подобных систем // SecurityLab.ru (https://www.securitylab.ru/news/504021.php). 14.01.2020).***

***

«Специалисты из компании Google рассказали о своей успешной операции по борьбе с вредоносным ПО Bread, также известным как Joker. За последние три года компания удалила более 1700 приложений в Play Store, которые были заражены различными версиями данного вредоноса.

В то время как большинство операторов вредоносных программ сдаются, как только Google обнаруживает их приложения, операторы Bread продолжили свою деятельность. Уже более трех лет злоумышленники каждую неделю выпускают новые версии своих программ.

«В какой-то момент преступники использовали почти каждую технику маскировки и обхода защиты, пытаясь остаться незамеченными. В разное время мы обнаруживали три или более активных варианта вредоноса, использующих разные подходы или нацеленных для разных носителей. В пиковые периоды активности преступников мы видели до 23 различных приложений данного семейства в Google Play за один день», — сообщила Google в своем блоге.

По словам специалистов, злоумышленники активно эксплуатировали уязвимость в Google Play с целью обойти защитные механизмы. Тактика под названием «versioning» позволяла загружать чистую версии приложения, а уже потом добавлять вредоносные функций путем обновления программы.

Преступники также часто использовали видео YouTube для направления пользователей на вредоносные приложения, пытаясь заразить как можно больше устройств. Операторы вредоноса также использовали поддельные обзоры для повышения популярности приложений и сокрытия негативных отзывов.

Первоначальные версии вредоноса Bread были ориентированы на мошенничество с использованием SMS-сообщений, когда зараженные устройства использовались для оплаты продуктов или услуг путем отправки SMS-сообщения на платный номер.

Когда Google ввела более строгие разрешения для Android-приложений, требующие доступ к SMS на устройстве, преступники сменили тактику и переключились на мошенничество с WAP, в рамках которого зараженные устройства использовались для подключения к платежным страницам через WAP-соединение». **(Google удалила более 1700 приложений, зараженных вредоносом Bread // SecurityLab.ru (https://www.securitylab.ru/news/503943.php). 10.01.2020).**

***

«Американская некоммерческая организация MITRE Corporation объявила о выпуске версии базы знаний MITRE ATT&CK, посвященной промышленным системам управления (Industrial Control System, ICS).

«MITRE ATT&CK for ICS Matrix» представляет собой базу знаний, описывающую различные действия, которые может предпринять злоумышленник внутри компьютерной сети ICS. База знаний предоставляет обзор тактик и техник, ассоциируемых с киберпреступными группировками, осуществлявшими атаки на системы промышленной автоматизации.

Цель матрицы заключается в содействии операторам критической инфраструктуры и другим использующим АСУ ТП организациям в оценке киберрисков.

База данных включает категорию «Assets» («Активы»), которую организации могут использовать для лучшей классификации типов угроз.

В настоящее ATT&CK for ICS содержит информацию о 10 киберпреступных группировках, 81 методе атак, 17 семействах вредоносных программ и 7 типах активов». ***(Представлена версия MITRE ATTACK для промышленных систем управления // SecurityLab.ru (https://www.securitylab.ru/news/503898.php). 09.01.2020).***

***

«Исследователи Университета имени Бен-Гуриона планируют представить первую полностью оптическую технологию шифрования, которая будет значительно более безопасной и конфиденциальной для передачи высокочувствительной информации по финансовым, медицинским или социальным сетям.

Технология будет представлена на конференции "Cybertech Global" в Тель-Авиве, которая состоится 28-30 января. Сегодня информация, передаваемая в Интернете, шифруется для защиты конфиденциальности и безопасности данных с использованием цифровых технологий, имеющих ряд недостатков.

Новое комплексное решение обеспечивает шифрование, передачу, дешифрование и обнаружение данных оптическим, а не цифровым способом. Используя стандартное оптическое оборудование, исследователи смогли сделать передачу данных незаметной и полностью "скрытой".» ***(Оптическое шифрование данных - новое слово в кибербезопасности // ISRAland Online Ltd (http://www.isra.com/news/240836). 29.01.2020).***

***

«Крупные производители антивирусного ПО будут поддерживать ОС Windows 7 на протяжении двух лет со дня прекращения ее официальной поддержки компанией Microsoft.

Как сообщает немецкая ИБ-компания AV-TEST, большинство крупных вендоров подтвердили, что их антивирусы буду доступны пользователям Windows 7 до 2022 года. Благодаря этому пользователи устаревшей ОС, поддержка которой прекратилась 14 января, смогут защитить себя от кибератак.

О продолжении поддержки Windows 7 в течение следующих двух лет сообщили: AhnLab, AVG & Avast, Avira, Bitdefender, BullGuard, Carbon Black, ESET, FireEye, F-Secure (до декабря 2021 года), G Data, Ikarus, «Лаборатория Касперского», K7 Computing, McAfee (до декабря 2021 года), Microsoft Security Essentials (только обновления сигнатур), Microworld, PC Matic, Quickheal, Seqrite, Sophos (локальная поддержка до декабря 2020 года, облачная – до июня 2021 года), Symantec/NortonLifeLock, ThreatTrack/Vipre, TotalAV и Trend Micro.

Корпоративные пользователи Windows 7 могут и впредь получать обновления безопасности от Microsoft, но для этого им нужно заплатить за расширенную поддержку. Представителям малого и среднего бизнеса, а также домашним пользователям расширенная поддержка не доступна. Если они хотят продолжать работать с Windows 7, единственный способ обезопасить себя от кибератак с использованием новых уязвимостей – установить антивирусное решение из представленного выше списка». ***(Популярные антивирусы продолжат поддерживать Windows 7 // SecurityLab.ru (https://www.securitylab.ru/news/504497.php). 29.01.2020).***

***

«Пользователи системы MaxPatrol SIEM теперь могут выявлять злоумышленников на этапе, когда они собирают данные о скомпрометированной сети, чтобы развивать свою атаку. Для этого в MaxPatrol SIEM загружен пакет экспертизы с правилами обнаружения атак, проводимых с использованием тактики «Разведка» (Discovery) по модели MITRE ATT&CK [1].

После получения постоянного доступа к сети жертвы злоумышленникам требуется определить, где в инфраструктуре они находятся, что их окружает и что они могут контролировать. Во время разведки атакующие собирают данные о скомпрометированной системе и внутренней сети, и это помогает им сориентироваться, чтобы решить, как действовать дальше. Для этого злоумышленники часто используют встроенные инструменты операционных систем.

Новый пакет экспертизы [2] включает в себя правила детектирования 15 популярных техник разведки. Теперь пользователи смогут обнаружить активность злоумышленников еще во время их попыток получить список учетных записей домена, сведения о парольной политике, перечень установленных приложений и служб, информацию о состоянии средств защиты.

«Отличить активность атакующих, которые проводят разведку, от легитимных запросов обычных пользователей непросто, — комментирует Антон Тюрин, руководитель отдела экспертных сервисов PT Expert Security Center . — Если злоумышленники действуют под учетной записью реального пользователя и используют встроенные утилиты, то их активность, как правило, теряется в потоке событий. Новый пакет экспертизы поможет обратить внимание специалистов по ИБ на события, которые на первый взгляд могут не вызывать подозрений».

Пакет экспертизы, посвященный тактике «Разведка» (Discovery), — это пятый пакет с правилами обнаружения атак по модели MITRE ATT&CK; всего в матрице ATT&CK описано 12 тактик. Пакеты, ранее загруженные в MaxPatrol SIEM, продолжают пополняться правилами по мере появления новых способов обнаружения атак [3]. Так, одновременно с выходом пятого пакета экспертизы первый пакет из серии получил 14 правил корреляции для выявления техник выполнения кода и обхода защиты.

[1] База знаний с описанием тактик, техник и процедур атак злоумышленников.

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

[3] Предыдущие пакеты экспертизы покрывают тактики «Выполнение», «Обход защиты», «Перемещение внутри периметра», «Закрепление» и «Получение учетных данных». ***(MaxPatrol SIEM выявляет присутствие киберпреступников в корпоративной сети на этапе разведки // SecurityLab.ru (https://www.securitylab.ru/news/504465.php). 28.01.2020).***

***

«Армия США работает над созданием программного обеспечения для защиты технологий распознавания лиц, используемых в военных приложениях, от возможной компрометации. Команда ученых Университета Дьюка (Северная Каролина, США) разработала инструмент, предназначенный для отражения кибератак на военные приложения с технологиями распознавания лиц.

Армия США использует технологии распознавания лиц и объектов для обучения систем искусственного интеллекта (ИИ), использующихся в беспилотных летательных аппаратах, системах слежения и пр. Большую угрозу представляют

бэкдоры в платформах распознавания лиц, поскольку с их помощью злоумышленники могут повлиять на обучение ИИ.

Модели ИИ опираются на массивные наборы данных, и в случае компрометации используемых для распознавания лиц данных (таких как одежда, форма, ушей, цвет глаз и т.п.) ИИ будет неверно идентифицировать людей. Подобные угрозы могут иметь серьезные последствия для программ слежения: находящиеся под наблюдением подозреваемые будут идентифицированы неверно и в итоге избегут обнаружения.

Такую атаку невозможно выявить невооруженным взглядом, поскольку используемые для обучения наборы данных выглядят нормально и не вызывают никаких сбоев в работе нейронных сетей. Тем не менее, в них могут быть внедрены вредоносный код или визуальные подсказки, способные повлиять на обучение ИИ.

Разработанный учеными Университета Дьюка инструмент способен слой за слоем сканировать изображения в поисках признаков постороннего вмешательства. На его создание ушло девять месяцев и $60 тыс., выделенных в качестве гранта Армейской исследовательской лабораторией». ***(Армия США защитит свои системы распознавания лиц от компрометации // SecurityLab.ru (https://www.securitylab.ru/news/504444.php). 27.01.2020).***

***

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

Бєльська Т.В. Інформаційні війни та інформаційна безпека: загрози та виклики для демократії / Бєльська Т.В., Крюков О.І. // Вісник Національного університету цивільного захисту України. Серія : Державне управління.- 2019.- Вип. 2 (11).- С. 3-11.

Розглянуто неконтрольовану інформацію, яка може стимулювати різні інформаційні безпеки. Визначено потреби пристосування управління до умов зовнішнього середовища. Встановлено, що інформаційні війни тісно пов’язані з громадянським суспільством.

Шифр зберігання НБУВ: Ж74479

***

Бухарєв В. В. Адміністративно-правові засади забезпечення кібербезпеки України : автореф. дис. ... канд. юрид. наук : 12.00.07 / Бухарєв Владислав Вікторович ; Сум. держ. ун-т. - Суми, 2018. - 20 с.

Визначено сутності та особливості адміністративно-правових засад забезпечення кібербезпеки України. З’ясовано особливості кібербезпеки як об’єкта адміністративно-правової охорони. Здійснено історико-правовий аналіз розвитку та становлення правового інституту кібербезпеки. Встановлено види об’єктів кібербезпеки та кіберзахисту. Охарактеризовано правові засади забезпечення

кібербезпеки України. Систематизовано адміністративно-правові форми та методи забезпечення кібербезпеки України. Виокремлено види та особливості юридичної відповідальності за порушення законодавства у сфері кібербезпеки України. Узагальнено зарубіжний досвід забезпечення кібербезпеки.

Шифр зберігання НБУВ: РА443345

***

Гавриленко С. Ю. Методи та засоби ідентифікації стану комп'ютерних систем критичного застосування для захисту інформації : автореф. дис. ... д-ра техн. наук : 05.13.05 / Гавриленко Світлана Юріївна ; Нац. техн. ун-т «Харків. політехн. ін-т». - Харків, 2019. - 36 с.

Проведено аналіз науково-технічної проблеми ідентифікації стану комп'ютерних систем критичного застосування (КСКЗ) для захисту даних. Виконано порівняльні дослідження існуючих методів та відомих комп'ютеризованих систем ідентифікації стану. Розроблено схему ідентифікації стану КСКЗ, яка включає підсистему ідентифікації аномалій та зловживань. Запропоновано експертну систему з непродукційним механізмом логічного виведення, що дозволиловиконати ідентифікацію стану КСКЗ з необмеженим числом контрольованих показників. Синтезовано новий показник нормального функціонування КСКЗ, на основі BDS-статистики, який відрізняєтьсявід відомих використанням синтезованого показника джиттера параметрів системи.

Шифр зберігання НБУВ: РА443205

***

Захарко А. В. Аналіз стану законотворчої діяльності щодо імплементації процедурних положень конвенції про кіберзлочинність / Захарко А. В. // Науковий вісник Дніпропетровського державного університету внутрішніх справ. - 2019. - № 2. - С. 134-142.

Розглянуто процедурні положення Конвенції про кіберзлочинність. Проаналізовано актуальний стан кримінального процесуального законодавства на наявність норм, що кореспондують процедурним положенням Конвенції про кіберзлочинність. Вивчено порядок денний десятої сесії Верховної Ради України восьмого скликання на предмет наявності законопроектів щодо імплементації процедурних положень Конвенції про кіберзлочинність до Кримінального процесуального кодексу України. Зазначені законопроекти досліджено на предмет охоплення ними усієї системи відповідних процедурних положень Конвенції про кіберзлочинність.

Шифр зберігання НБУВ: Ж70666

***

Інформаційна безпека : навч. посіб. / Ю. Я. Бобало [та ін.]. - Львів : Вид-во Львів. політехніки, 2019. - 573 с.

Розглянуто основні поняття та визначення в галузі інформаційної безпеки. Описано математичні основи криптології. Розглянуто відомі та сучасні методи криптографії, криптоаналізу, стеганографії. Розглянуто питання ідентифікації,

автентифікації та санкціонованого доступу. Значну увагу приділено практичному захисту інформації. Розглянуто питання безпеки інформаційних систем. Висвітлено особливості захисту програмного забезпечення в інформаційних системах. Розглянуто питання інформаційної безпеки підприємств та організацій.

Шифр зберігання НБУВ: ВС66548

***

Інформаційне суспільство: проблеми та перспективи : матеріали IV Всеукр. наук.-практ. конф., 14 черв. 2019 р., м. Одеса. - Одеса : Фенікс, 2019. - 118 с.

Зі змісту:

- Болейко А.А. Кібербезпека: вітчизняний та зарубіжний досвід;
- Васильєв Б.Г. Кіберзлочинність як загроза національної безпеки в Україні;
- Венцурик Д.П. Особливості нового Закону України «Про основні засади забезпечення кібербезпеки в Україні»;
- Руденко В.О. Основні засади забезпечення кібербезпеки України;
- Сарокина В.В. Правовое регулирование киберзащиты: зарубежный и национальный опыт;
- Султанов Б. Киберполиция Украины;
- Трофименко О.Г. Стан кібербезпеки України в оцінках міжнародних рейтингів.

Шифр зберігання НБУВ: ВА838304

***

Кримінальні загрози в секторі безпеки: практики ефективного реагування : матеріали панел. дискусії III Харків. міжнар. юрид. форуму , м. Харків, 26 верес. 2019 р. - Харків : Право, 2019. - 170 с.

Зі змісту:

- Бусол О.Ю. Кібернетичні війни та кібертероризм як загрози міжнародній безпеці: диференціація злочинів від традиційної війни;
- Воронов І. Захист персональних даних в мережі Інтернет;
- Колб О.Г., Дучимінська Л.М. Про деякі прояви кіберзлочинності у місцях позбавлення волі;
- Команцева Л. Лінгвістична експертиза соціальних мереж як інструмент ідентифікації гібридних загроз;
- Копотун І.М., Довбань І.М. Види кіберзлочинів відповідно до міжнародних нормативних актів;
- Кудінов С.С., Марущак А.І., Петров С.Г. актуальні кіберзагрози національним інтересам України: протидія і міжнародне співробітництво;
- Левченко Ю.О. Сучасний стан протидії кіберзлочинності в Україні;
- Миронюк Т.В. Сучасний стан та тенденції кіберзлочинності в Україні;
- Настюк В.Я., Бєлєвцева В.В. Особливості правових режимів забезпечення кібербезпеки в Україні;

- Радутний О.Е. Злочини майбутнього та інші загрози кібербезпеці, пов’язані зі штучним інтелектом;
- Ткачова О.В. Міжнародний досвід у сфері інформаційної та кібернетичної безпеки;
- Ткачук Н.А. Демократичний цивільний контроль у сфері кібербезпеки;
- Шаблистий В.В. Способи мінімізації кримінальних загроз безпеці критичної інфраструктури та кібернетичній безпеці людини в Україні;
- Шевчук В.М. Використання інформації із соціальних Інтернет-мереж при розслідуванні кіберзлочинів: криміналістичні проблеми;
- Шкута О.О. Кіберзлочинність у місцях несвободи;
- Шило О.Г., Шило А.В. Проблема забезпечення кібербезпеки: чинне законодавство України та сучасні виклики;
- Таволжанський О.В. Деякі аспекти регламентації приватності у кіберпросторі.

Шифр зберігання НБУВ: ВА838033

***

Проблеми розвитку публічного управління в Україні : пленар. засід. наук.-практ. конф. за міжнар. участю, 11-12 квіт. 2019 р. - Львів, 2019. - 80 с.

Зі змісту:

- Надюк З.О. Узгодження принципів відкритості і прозорості з базовими вимогами кібербезпеки у діяльності органів публічної влади в Україні.

Шифр зберігання НБУВ: ВА838370

***

Рижук О. М. Інформаційна безпека України в умовах глобалізаційних викликів та гібридної війни : монографія / О. М. Рижук. - Київ : Університет «Україна», 2019. - 177 с.

Досліджено питання інформаційної безпеки України з огляду на глобалізаційні виклики та гібридну війну з урахуванням сучасного стану інформаційної безпеки та тенденцій її розвитку Значну увагу приділено напрямам удосконалення інформаційної безпеки української держави у захисті свого інформаційного простору.

Шифр зберігання НБУВ: ВА838269

***

Сторчак А. С. Метод оцінювання рівня захищеності мережевої частини комунікаційної системи спеціального призначення від кіберзагроз / А. С. Сторчак, С. В. Сальник // Системи обробки інформації. - 2019. - Вип. 3. - С. 98-109.

Представлено удосконалений метод оцінки рівня захищеності мережевої частини комунікаційної системи спеціального призначення від кіберзагроз на основі алгоритму розподільчої ідентифікації та динамічного програмування. Визначено вектори процесу оцінки захищеності і процесу реалізації засобів

захисту, які забезпечують мінімізацію значення ризиків на всіх етапах функціонування системи захисту.

Шифр зберігання НБУВ: Ж70474

***

Тези доповідей Міжнародної науково-практичної конференції «Проблеми інтеграції освіти, науки та бізнесу в умовах глобалізації», 4 жовтня 2019 року. - Київ, 2019. - 157 с.

Зі змісту:

- Кононенко Г. Проблеми інформаційної безпеки вищої освіти в умовах глобалізації.

Шифр зберігання НБУВ: ВС66573

***

Цивілістика в інформаційному суспільстві : матеріали Всеукр. кругл. столу, 17 трав. 2019 р. - Одеса, 2019. - 102 с.

Зі змісту:

- Звєрєва Т.В. До питання забезпечення кібербезпеки на міжнародній арені.

Шифр зберігання НБУВ: ВА838297

***

Шостак Н. В. Аналіз стійкості стеганографічних методів вбудовування даних в відеофайли до атак / Н. В. Шостак, А. А. Астраханцев // Системи обробки інформації. - 2019. - Вип. 3. - С. 110-116.

Зроблено порівняльний аналіз сучасних методів вбудовування цифрових водяних знаків (ЦВЗ) у відеофайли з метою виявлення методів з найкращими показниками по стійкості до атак та скритності вбудовування ЦВЗ. Досліджено методи підвищення завадостійкості та стійкості до основних атак.

Шифр зберігання НБУВ: Ж70474

***