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

№ 9 (вересень)

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– №9 (вересень) . – 186 с.

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

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

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

ЗМІСТ

«Сьогодні, 9 вересня, начальник Департаменту кіберполіції Олександр Гринчак та директорка Тренінгового центру прокурорів України Олеся Отраднова підписали меморандум про співпрацю та партнерство.

Відтепер сторони співпрацюватимуть у сфері наукової, методичної, навчальної та інформаційної діяльності з питань протидії кіберзлочинності, обмінюватимуться досвідом у форматі навчань, семінарів і лекцій. Також передбачено розроблення пропозицій і рекомендацій до проєктів законів та інших нормативно-правових актів з питань протидії правопорушенням, вчиненим у кіберпросторі.

Очільник Департаменту кіберполіції Олександр Гринчак зазначив, що така співпраця сприятиме ефективнішій протидії злочинам, вчиненим відносно наших громадян у кіберпросторі.

«У рамках меморандуму передбачається подальше навчання прокурорів, підвищення їхніх професійних навичок та обізнаності у кіберсфері. Для цього наші фахівці нададуть Тренінговому центру весь необхідний навчальний контент, а також поділяться практичним досвідом», - зауважив Олександр Гринчак.

Директорка Тренінгового центру прокурорів України Олеся Отраднова підкреслила, що це – перший меморандум, який підписав центр з органами правопорядку.

«Таке об’єднання зусиль двох потужних правоохоронних інституцій є пріоритетним, оскільки безпека у кіберпросторі є важливою складовою життя, особливо під час карантинних заходів, коли суспільство все більше «переходить» у віртуальний світ», - сказала Олеся Отраднова». ***(Кіберполіція обмінюється досвідом із Тренінговим центром прокурорів України у сфері кібербезпеки // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-obminyayetsya-dosvidom-iz-treningovym-czentrom-prokuroriv-ukrayiny-u-sferi-kiberbezpeky-1050/). 09.09.2020).***

***

«С 15 по 17 сентября 2020 года состоялись учения по отработке совместных мероприятий по обеспечению киберзащиты информационных и информационно-телекоммуникационных систем ЦИК.

В киберучениях, которые состоялись в рамках подготовки к проведению местных выборов 25 октября 2020 года, приняли участие представители Госспецсвязи, СБУ, Национальной полиции Украины и ЦИК. Мероприятие было организовано Госспецсвязи во исполнение решения НКЦК при СНБО Украины, передает internetua.com.

Киберучения прошли в два этапа. Первый этап, прошедший в ЦИК, предусматривал отработку специалистами Госспецсвязи, ЦИК, ДКИБ СБУ и киберполиции взаимодействия в случае возникновения кризисных ситуаций при проведении местных выборов. Второй этап обучения состоялся в Тренинговом киберцентре Госспецсвязи. Обучение проводилось в формате командного

упражнения, в котором приняли участие две команды, сформированные из представителей профильных технических подразделений указанных ведомств.

Таким образом во время первого этапа представители основных субъектов обеспечения кибербезопасности отработали конкретные алгоритмы при возникновении кризисных ситуаций и определили роли и задачи каждого ведомства, привлеченного к обеспечению киберзащиты информационной инфраструктуры ЦИК. На втором этапе участники усовершенствовали сотрудничество на техническом уровне и отработали меры в случае атаки на конкретный элемент информационной инфраструктуры». ***(Госспецсвязи организовала киберучения перед местными выборами // Багнет (http://www.bagnet.org/news/tech/1292036/gosspetssvyazi-organizovala-kiberucheniya-pered-mestnymi-vyborami). 18.09.2020).***

***

«Реформи у сфері кібербезпеки енергетичного сектору України необхідно прискорити. Про це заявила в.о. міністра енергетики Ольга Буславець, відкриваючи у режимі онлайн-конференції засідання Робочої групи з питань розбудови кіберзахисту об'єктів критичної інфраструктури енергетичної галузі Міненерго…

"Як очільниця Міністерства енергетики я хочу не тільки зберегти вектори реформ в сфері кібербезпеки, що були розпочаті в галузі, але й прискорити їх реалізацію. Міненерго, як центральний орган виконавчої влади, відповідальний за безпеку й, зокрема, кібербезпеку енергетичних об'єктів, розпочало активну роботу зі створення системи, що дійсно стане ефективною в сучасних умовах", – сказала Буславець.

Актуальні питання кібербезпеки представники міністерства сьогодні обговорюють із світовими виробниками - лідерами в сфері кібербезпеки та цифрових трансформацій, які зацікавились співпрацею у цьому напрямку.

В Україні затверджено стратегію уряду й ухвалено нормативні акти, що дають загальну модель розвитку галузевих систем кібербезпеки у державі, також є останні нормативи та рекомендації Європейського Союзу щодо заходів з кібербезпеки в енергетичному секторі, які використано як базу для розробки концептуального бачення.

Як повідомлялося, в Міненерго було створено міжвідомчу робочу групу з кібербезпеки критичної інфраструктури енергетичного сектору та затверджено план короткострокових заходів. Зокрема, було вирішено створити Проєктний офіс для секторальної координації реалізації ініціативи та залучення міжнародної технічної допомоги; визначено необхідність в проведені секторального аудиту стану кібербезпеки енергетичного сектору; вирішено створити секторальний центр кібербезпеки критичної інфраструктури енергетичного сектору України». ***(Міненерго розпочало активну роботу зі створення системи кіберзахисту // Укрінформ (https://www.ukrinform.ua/rubric-economy/3105856-minenergo-rozpocalo-aktivnu-robotu-zi-stvorenna-sistemi-kiberzahistu.html). 24.09.2020).***

***

«Торгово-промислова палата України, Комітет з електронних комунікацій, Антикризовий центр кібернетичного захисту бізнесу при ТПП України, Державна служба спеціального зв'язку та захисту інформації України при підтримці РНБО України, Держспецзв'язку, Кіберполіції МВС, Україна приєдналась до європейської традиції і вже втретє проводять Місяць кібербезпеки, цього року - з 1 по 31 жовтня.

Політичним і технологічним фундаментом місяця кібербезпеки в 2019 році стали ІІ міжнародний форум «Кібербезпека. Захисти свій бізнес!» і І-ша національна виставка з кібербезпеки.

В роботі форуму взяв участь секретар РНБО України Данілов О.М., перший заступник Голови Держспецзв'язку Чаузов О.М. начальник департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ Кулешов М.П. Понад 30 профільних експертів з державних установ та бізнесу з України, США, Німеччини та Ізраїлю вели дискусію з більш ніж 600 учасниками.

Проведення Місяця кібербезпеки в Україні в 2019 році, отримало широкий відгук в суспільстві, надало можливість акцентувати увагу державних структур, бізнесу і громадянського суспільства на актуальності проблем, підтвердило ефективність державно-приватної взаємодії в розбудові безпечного кіберпростору в Україні.

Ще в листопаді 2019 року ми розпочали підготовку і планували в 2020 році розширити географію проведення заходів. Нажаль COVID-19 не тільки вніс корективи в наші плани, але і відкрив нові проблеми безпечного ведення бізнесу. Ми проводимо заходи Місяця в умовах посилення карантину.

У 2020 році, в умовах пандемії, ми провели ряд заходів, серед яких online конференція «Безпечне online середовище - коронавірусний досвід». Конференція проходила 8-9 липня 2020 року. В її роботі прийняли участь понад 300 учасників. Протягом місяця планується проведення 3 форумів, 2 міжнародних науково-практичних конференцій, тренінгів, навчальних семінарів, 2 круглих столи, очікується участь понад 200 державних і приватних суб'єктів, які продемонструють свою рішучість співпрацювати в повній взаємодоповнюваності для підвищення рівня цифрової безпеки компаній, організацій і громадян.

Ці події стануть важливими кроками Місяця кібербезпеки в Україні 2020, який пройде 1-31 жовтня, третього щорічного Міжнародного Форуму

«Кібербезпека – захистимо бізнес, захистимо державу», що відбудеться

6 жовтня 2020 в місті Києві.

https://cybersecurity-2020.ciseventsgroup.com/

Запрошуємо до участі в заходах Місяця кібербезпеки в Україні.

Переглянути план заходів:

https://www.ucci.org.ua/uploads/files/5f68943a92ff0700254020.pdf

Пропозиції щодо Ваших заходів, які можуть бути включені до плану заходів, надсилати на адресу: csm.ua@ukr.net» ***(МІСЯЦЬ КІБЕРБЕЗПЕКИ В УКРАЇНІ 2020 // Запорізька торгово-промислова палата (http://www.cci.zp.ua/presscentr4/novosti4/6171-misyats-kiberbezpeki-v-ukrajini-2020). 29.09.2020).***

***

«Во время онлайн-конференции «Цифровая трансформация государства: перспективы и риски кибербезопасности», которая прошла в конце сентября текущего года, был представлен Глобальный центр взаимодействия в киберпространстве. В качестве основной цели мероприятия организаторы назвали желание объединить ключевых участников киберпространства ради противостояния киберугрозами и в перспективе сделать Украину одним из самых влиятельных кибер-игроков в мире.

В современном цифровизованном мире возникает все больше вызовов и угроз, которые могут привести к остановке бизнес-процессов, потере персональных данных и интеллектуальной собственности, а также серьезных финансовых убытков. Преодолеть киберуязвимость можно только путем взаимодействия и сотрудничества всех игроков киберпространства.

«Глобальный центр взаимодействия в киберпространстве GC3 — это интеграционная платформа для государства, бизнеса и учебных институтов как украинского так и международного формата, цель которой — разработать новые правила взаимодействия в цифровом мире. Такое сотрудничество позволяет не только оперативно реагировать на киберугрозы, но и предупреждать их возникновение.

Задача GC3 — создать площадку для содержательного сотрудничества всех стейкхолдеров киберпространства — государственных, деловых, учебных и научных институтов, как украинских, так и международных игроков этой сферы. Мы хотим создать новые правила взаимодействия в цифровом мире», — подчеркнул Владимир Павелко, со-инициатор и CEO Глобального центра взаимодействия в киберпространстве, GC3.

Платформой, объединяющей государственные органы власти, частный сектор и академические круги ради создания безопасного киберпространства, и должен стать Глобальный центр взаимодействия в киберпространстве (GC3), созданный при содействии Министерства внутренних дел и НАК «Нафтогаз Украины».

В своем выступлении Министр внутренних дел Украины Арсен Аваков акцентировал внимание на том, что в последние годы Украина чувствовала мощные управляемые кибератаки на государственные и частные учреждения и подчеркнул, что для эффективного противодействия киберпреступности и гибридным угрозам, МВД выступает инициатором создания на базе GC3 интеграционной площадки. Это позволит объединить всех ключевых игроков и обеспечит максимальную синергию и эффективность украинской экосистемы безопасного киберпространства, и как логическое следствие — усиление системы национальной безопасности Украины.

«Каждый день Нафтогаз является объектом 800 атак в киберпространстве. Сейчас нам удается им противостоять. И надеемся, что с созданием Глобального центра взаимодействия в киберпространстве, через кооперацию с партнерами, мы будем иметь доступ не только к инструментам защиты, но и превентивного реагирования, станем сильнее и эффективнее», — добавил Андрей Коболев, председатель правления НАК» Нафтогаз Украины».

GC3 уже выстраивает эффективное сотрудничество с Национальным банком Украины, Службой безопасности Украины, Государственной службой специальной связи и защиты информации Украины, Министерством обороны Украины, разведывательными органами, Национальной полицией и Министерством цифровой трансформации Украины, Нафтогазом и другими государственными и частными организациями. Кроме того, уже подписаны меморандумы о сотрудничестве с подобными международными центрами из Канады и США. Продуктом плодотворного взаимодействия станет аналитическая информация, доступная участникам платформы, разработка стратегий в киберпространстве, законодательных инициатив, способствующих созданию экосистемы безопасного киберпространства…». ***(Сергей Кулеш. В Украине презентовали «Глобальный центр взаимодействия в киберпространстве» (GC3) // ООО «ХОТЛАЙН» (https://itc.ua/news/v-ukraine-prezentovali-globalnyj-czentr-vzaimodejstviya-v-kiberprostranstve/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+itc-ua+%28ITC.ua%29). 30.09.2020).***

***

Національна система кібербезпеки

«Сьогодні в нашій країні дуже гостро стоїть питання підготовки кадрів у сфері захисту інформації та кібербезпеки. Про це заявив Заступник Голови Держспецзв'язку Олександр Потій під час zoom-конференції на тему «Цифрова трансформація держави: перспективи та ризики кібербезпеки», повідомляють у пресслужбі Держспецзв'язку.

Олександр Потій серед інших важливим чинником назвав специфічну практичну підготовку майбутніх фахівців під час навчання.

«Для того, щоб вони отримали таку практичну підготовку, необхідно, щоб навчальні заклади мали відповідну матеріально-технічну базу. І сприятиме цьому налагодження партнерських відносин між навчальними закладами та промисловістю», - сказав він, зазначивши, що зараз в Україні близько 30 вузів готують фахівців за спеціальністю «Кібербезпека».

Дуже важливою для підготовки є можливість проходити студентам на базі органів державної влади або приватних структур тренінгів для підвищення своїх навичок у сфері кібербезпеки.

За словами Олександра Потія, Держспецзв'язку має свій навчальний заклад – Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», а також свого тренінгового кіберцентру.

«Там ми готуємо кадри для потреб нашої установи, а також для потреб інших суб'єктів сектору безпеки і оборони», - зазначив він.

Ще одним важливим завданням Олександр потій назвав питання підготовки і розроблення навчальних програм.

«Є потреба у перегляді напрямків підготовки фахівців в сфері інформаційної безпеки. Напрям «Кібербезпека» - дуже вузький по своєму профілю, тому він має

входити до напряму «Інформаційна безпека» або «Безпека інформаційних технологій», - сказав він.

Заступник Голови Держспецзв'язку підкреслив, що також дуже гостро стоїть питання щодо кадрової політики. Він пояснив, що зараз фахівці з кібербезпеки та захисту інформації, які працюють в державних органах і часто в приватному секторі, вони не знають свого кар'єрного плану.

«Вони не можуть побудувати кар'єру, оскільки в нас немає класифікатора професій кібербезпеки і захисту інформації. Якщо ми проробимо і законодавчо закріпимо класифікатор професій, відповідальності фахівців, які працюють в цих галузях, тоді і закладам освіти буде простіше розробляти відповідні освітні програми, що сприятиме підготовці майбутніх спеціалістів», - резюмував Олександр Потій». ***(Для посилення кібербезпеки необхідна співпраця наукових установ, підприємств та навчальних закладів – Потій // Агенція інформації та аналітики (https://galinfo.com.ua/news/dlya_posylennya_kiberbezpeky_neobhidna_spivpratsya_naukovyh_ustanov_pidpryiemstv_ta_navchalnyh_zakladiv__potiy_351916.html). 25.09.2020).***

***

«Обіцяного три роки ждуть. Це про ЄСІТС, яка мала почати функціонувати ще півтора роки тому, однак все виявилось не готовим. Нещодавно пролунала ще одна обіцянка про запуск системи, але ще є три місяці, щоб передумати.

Точна, неточна і змінена дата

Ніщо не заважає з 1 січня запрацювати ЄСІТС. Так вважають ініціатори законопроекту, які представили свою ініціативу на розгляд Комітету Верховної Ради з питань правової політики. На думку нардепів, до роботи готові вісім модулів системи. Тому вони запропонували внести зміни до інших законів задля успішного функціонування цієї електронної системи.

Проект закону передбачає зміни до процесуальних кодексів та закону «Про Вищу раду правосуддя». Впровадження системи має відбуватись поетапно, кожен наступний модуль має почати роботу через місяць після його анонсування ВРП у газеті «Голос України» та на веб-порталі судової влади. Законотворці пропонують підвищити роль ВРП у запуску системи.

Головне науково-експертне управління ВР доволі іронічно поставилось до такої ініціативи. Адже раніше відповідальним за ЄСІТС ні разу не вдалося дотриматися строків.

У багатьох судах система працює в тестовому режимі, всього 7 модулів — Єдиний контакт-центр судової влади України; Єдина підсистема управління фінансово-господарськими процесами; офіційна електронна адреса (електронний кабінет); офіційний веб-портал «Судова влада України»; Єдиний державний реєстр судових рішень; автоматизований розподіл; судова статистика.

Утім, автори проекту впевнені у даті запуску 8 модулів і посилаються на слова очільника ДСАУ. Проте питання запуску викликало дискусію. Адже не

відомо, чи не доведеться знову відкладати через те, що люди не вмітимуть користуватися системою.

Однак голова ДСАУ Зеновій Холоднюк запевнив, що навчання проводять щоденно, для цього створена ініціативна група. Коли з'явиться ще один модуль, навчать фахівців користуватись і ним. Хоча до кожного модуля прописані інструкції, але людський фактор також важливий. Також навчання проводить Національна школа суддів на спеціальних курсах.

Кібернебезпека у судах

ГНЕУ також не сподобалося, що законопроект не передбачає зберігання документів у паперовому вигляді. Зокрема, законотворці пропонують вилучити із процесуальних кодексів таку норму: «Процесуальні та інші документи і докази в паперовій формі зберігаються в додатку до справи в суді першої інстанції та у разі необхідності можуть бути оглянуті учасниками справи чи судом першої інстанції або витребувані судом апеляційної чи касаційної інстанції після надходження до них відповідної апеляційної чи касаційної скарги».

На думку експертів, відсутність документів і доказів у паперовій формі, які б зберігалися в додатку, зокрема тих, що використовувалися при деліктних правовідносинах, можуть створювати ризики для інформації про справу. Наприклад, якщо матеріали доведеться відновити.

Такий ризик зберігається також у разі неможливості відтворити дані справи при кібератаках, які відбуваються регулярно.

Нардепи не зацікавилися кібератаками і не обговорювали вказаного пункту. Вони запропонували взяти проект за основу і рекомендувати його для розгляду в першому читанні. Адже переконані, що це «матиме позитивні наслідки для підвищення ефективності діяльності судів, функціонування їх у режимі реального часу, що, у свою чергу, сприятиме більш зручному і доступному правосуддю для громадян». ***(Марта ЛІТЕЧКО. У павутині ЄСІТС. З нового року вершити справедливість будуть без паперу // Закон і Бізнес (https://zib.com.ua/ua/print/144677-z_novogo_roku_vershiti_spravedlivist_budut_bez_paperu.html). 28.09.2020).***

***

Правове забезпечення кібербезпеки в Україні

«Законопроєкт розрахований на підвищення ефективності боротьби з кіберзлочинністю та забезпечення дотримання санкційного режиму

У Верховну раду подано законопроект, який передбачає полегшення правоохоронним органам доступу до персональних даних інтернет-користувачів. Проект закону №4004 «Про внесення змін в Кримінально-процесуальний кодекс для підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів» розміщений на сайті Верховної Ради.

Документ передбачає зобов'язання інтернет-провайдерів встановити за свій рахунок обладнання, необхідне для проведення розшукових дій і надає

правоохоронним органам доступ до інформації про абонента, маршрути передачі інтернет-послуг, їх тривалості і змісту.

Провайдери повинні сприяти проведенню слідчих заходів та недопущенню їх розголошення.

Також автори законопроекту хочуть доповнити перелік процесуальних джерел доказів електронними файлами. Серед них зазначені текстові документи, графічні зображення, плани, фотографії, відео- і звукозапису, віртуальні активи, сайти, текстові, мультимедійні та звукові повідомлення, метадані та бази даних.

Крім того, керівник громадської організації «Лабораторія цифрової безпеки» Ірина Чулівська на своїй сторінці Facebook написала для кого і чого був розроблений законопроєкт.

«Депутати хочуть зобов'язати інтернет-провайдерів встановити у себе спеціальні технічні засоби (ми називаємо їх «чорні коробочки») для збору даних користувачів, а також дозволити правоохоронцям в рамках обшуку доступ до наших особистих смартфонів та комп'ютерів. 1 вересня члени Комітету ВР з питань правоохоронної діяльності на чолі з Денисом Монастирським зареєстрували пакет законопроєктів на підвищення ефективності боротьби з кіберзлочинністю та забезпечення дотримання санкційного режиму (№ 4002, №4003, №4004)», – написала Чулівська.

На сайті організації сказано, що на початку вересня цього року члени комітету Верховної Ради з питань правоохоронної діяльності на чолі з Денисом Монастирським внесли до парламенту законопроєкти про боротьбу з кіберзлочинністю і про дотримання режиму санкції (законопроекти № 4002, №4003, №4004).

Якщо за ці ініціативи проголосує парламент, то в українському законодавстві з'явиться новий захід забезпечення кримінального провадження як термінове зберігання інформації й нове для нас поняття «електронний доказ». Крім цього, до законопроєкту №4002 «Про внесення змін до деяких законодавчих актів України щодо встановлення відповідальності за Порушення вимог санкційного режиму, що діє на захист національної безпеки й територіальної цілісності України» сказано, що можна отримати до 8 років в'язниці з позбавленням права обіймати посади, якщо порушення режиму санкції перевищило 6,3 млн грн (нова ст. 209-2 Кримінального Кодексу України). Ці нововведення потрібні для виконання міжнародних зобов'язань України щодо впровадження у себе положень Конвенції про кіберзлочинність.

За даними коаліції «За вільний Інтернет», в законопроєктах є норми, які можуть порушити права людини.

Законопроєкт №4002 запроваджує фінансову та кримінальну відповідальність за невиконання санкцій – аж до ліквідації компаній і позбавлення волі. Такі заходи відповідальності можуть застосовуватися не лише до тих, на кого накладено санкції, а й на інших осіб, які «будь-яким чином навмисно сприяли порушенню їх застосування». При цьому оштрафувати на суму до 85 тис. грн може спеціальний уповноважений орган, який буде створений Кабміном для нагляду за дотриманням режиму санкції. Наприклад, один з таких заходів як заборона на перегляд сайтів може негативно вплинути на доступ українців до послуг провайдерів.

Законопроєкт № 4003 «Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про Адміністративні правопорушення щодо Підвищення ефективності протидії кібератакам» надає можливість доступу до інформації, яка може зберігатися в смартфоні або персональному комп'ютері.

На думку членів коаліції, ця норма надає необмежену можливість правоохоронним органам діяти на свій розсуд і ніяк не захищає права українців на таємницю кореспонденції.

Законопроєкт №4003 також зобов'язує провайдерів зберігати інформацію про рух трафіку в обсязі, достатньому для ідентифікації абонента, визначення джерела походження трафіку і маршруту його передавання протягом 12 місяців, а також в порядку вимог тимчасового зберігання інформації для цілей кримінального провадження.

Доступ до такої інформації повинен надаватися за постановою прокурора або слідчого і може також делегуватися оперативним підрозділам. Тільки у виняткових випадках, які, до того ж нечітко виписані в законопроєкті, дозвіл може давати слідчий суддя. Це говорить про те, що доступ до інформації за новими правилами відбуватиметься поза судовим наглядом.

Законопроєкт № 4004 «Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів» доповнює норму статті 39 Закону України «Про телекомунікації» і покладає на провайдерів обов'язок власним коштом встановлювати на своїх телекомунікаційних мережах технічні пристрої для розшукових заходів, негласних слідчих дій і тимчасового доступу до інформації про тривалість, зміст, маршрутів передавання інформації абонента. Також, провайдери зобов'язані будуть стежити за справністю цих пристроїв і допомагати правоохоронцям у їх роботі.

Але ця норма суперечить вимогам Директиви ЄС про електронну комерцію, яка передбачає заборону на встановлення для посередників зобов'язання моніторити інформацію або шукати факти незаконного контенту або активності.

«Коаліція «За вільний Інтернет» закликає народних депутатів-суб'єктів законодавчої ініціативи доопрацювати зареєстровані законопроєкти з урахуванням міжнародних зобов'язань України у сфері прав людини, зокрема привести норми проєктів у відповідність до Конвенції про захист прав людини та засадних свобод та практики Європейського суду з прав людини, а також узгодити пропоновані новели з вимогами законодавства Європейського Союзу, у тому числі щодо захисту персональних даних, гармонізація з яким здійснюється в рамках Угоди про Асоціацію України з ЄС», – резюмували експерт». ***(Правоохоронцям хочуть дозволити доступ до персональних даних інтернет-користувачів // Українські медійні системи (https://glavcom.ua/news/pravoohoroncyam-hochut-dozvoliti-dostup-do-personalnih-danih-internet-koristuvachiv--704365.html). 09.09.2020).***

***

«В Україні створена вся необхідна законодавча база для цифрової трансформації держави та розвитку кібербезпеки, однак критично не вистачає цілісної системи освіти в цій галузі та підготовки висококласних фахівців.

Як передає кореспондент Укрінформ, про це під час ZOOM-конференції на тему «Цифрова трансформація держави: перспективи та ризики кібербезпеки» заявив секретар РНБО Олексій Данілов.

За його словами, цифрові технології в світі набиратимуть оберти, і кожна держава робитиме все можливе, аби дбати про свою безпеку саме цьому контексті. Наразі Україна має гарне законодавче підґрунтя в сфері захисту кіберпростору.

«Дякуючи законодавцям, які у 2016, 2017, 2018 році прийняли ряд законодавчих актів, у нас сьогодні розуміння кібербезпеки країни є вже на законодавчому рівні, визначена інституція і ми маємо сьогодні вже закон про кіберзахист»», - наголосив Данілов, додавши, що завдяки громадськості відбувається багато позитивних процесів в сфері цифрових технологій.

Він також нагадав, що 28 січня 2020 року Президент України підписав указ про створення Національного координаційного центру кібербезпеки при РНБО, який працює та демонструє позитивні результати.

«Це дуже потужний хаб, який об'єднує багато потужних інформаційних ресурсів. Вони аналізуються в цьому центрі для того, щоб кібрезахист був в нашій країні на високому рівні», - розповів Данілов.

Водночас він зазначив, що після аналізу стану вищої освіти в Україні, який нещодавно провела РНБО, стало зрозуміло, що в державі критично не вистачає молодих фахівців, яких готує держава в цій сфері.

«На превеликий жаль, можемо констатувати, що на сьогоднішній день цілісних інституцій, які могли б запропонувати якісних фахівців з вищою освітою в цій царині, в нашій країні майже не існує. Ми випускаємо з вами дуже багато юристів, менеджерів, різноманітних фахівців, а те, що стосується саме цих інституціональних фундаментальних речей, які сьогодні вкрай важливі для нашої держави, на жаль, наша освіта не дає нам відповіді на ці виклики», - заявив Данілов.

Керівник Радбезу також наголосив, що наразі в Міністерстві цифрової трансформації відбувається багато процесів з цифровізації суспільства, з поширення мережі інтернет по всій країні, однак слід пам'ятати, що це буде додатковим викликом для кбіерзахисту країни.

На завершення Данілов зазначив, що позитивних результатів в питанні кібербезпеки держави можна досягти лише у разі об'єднання зусиль усіх державних і недержавних структур, які працюють в цьому секторі…». ***(В Україні критично не вистачає фахівців з цифрових технологій та кіберзахисту – Данілов // Укрінформ (https://www.ukrinform.ua/rubric-polytics/3106384-v-ukraini-kriticno-ne-vistacae-fahivciv-z-cifrovih-tehnologij-ta-kiberzahistu-danilov.html). 25.09.2020).***

***

«На сегодня в Украине законодательно до сих пор не определено понятие "критическая инфраструктура" и сейчас оно только дорабатывается. Об этом заявил заместитель Председателя Госспецсвязи Александр Потий во время zoom-конференции на тему "Цифровая трансформация государства: перспективы и риски кибербезопасности", информирует пресс-служба Госспецсвязи. Так, по словам

Потия, сегодня в Украине существует очень много стратегически важных объектов и поэтому сейчас крайне важно дифференцировать такие объекты по их критерием критичности.

“В Украине сейчас разрабатывается проект закона „О защите критической инфраструктуры“, уже разработаны соответствующие проекты постановлений Кабмина, в которых определяется перечень жизненно важных функций и услуг, на основе которых осуществляется классификация отраслей по их критичности. Во-вторых, уже разработана методика и порядок оценки критичности объектов инфраструктуры и отнесения их к соответствующей категории критичности. Предполагается четыре категории критичности: первая — самая высокая критичность, а четвертая — некритические объекты”, — отметил он. Потий также добавил, что уже разработана методика, которая позволяет определить объект критической информационной инфраструктуры как критический или нет. “Если он отнесен к категории „критический“, то к нему будут выдвигаться требования, в том числе по кибербезопасности. Эти методики, подходы были разработаны с учетом опыта США, Франции, Канады и стран Евросоюза. В настоящее время такой подход является актуальным, что подтвердили специалисты из Украины и других стран”, — сказал заместитель главы Госспецсвязи. Он добавил также, что как только будут приняты соответствующие нормативно-правовые акты, специалисты Госспецсвязи вместе со специалистами других органов власти начнут работу для осуществления такой классификации объектов». ***(В Украине законодательно до сих пор не определено понятие "критическая инфраструктура" – Госспецсвязи // информационный портал "ua.today" (http://ua.today/news/politics/v_ukraine_zakonodatelno_do_sih_por_ne_opredeleno_ponyatie_kriticheskaya_infrastruktura_gosspecsvyazi). 26.09.2020).***

***

«Фахівці Національного координаційного центру кібербезпеки при РНБО розпочали розробку Стратегії кібербезпеки України…

"Після затвердження Президентом України Стратегії національної безпеки України на базі НКЦК було сформовано робочу групу з розробки Стратегії кібербезпеки. Представники ключових державних органів – суб’єктів забезпечення кібербезпеки, що входять до її складу, почали надавати НКЦК свої пропозиції", - йдеться в повідомленні.

За словами секретаря РНБО України Олексія Данілова, стратегія визначатиме пріоритети національних інтересів України у сфері кібербезпеки, а також основні підходи та напрями до формування питань кіберзахисту. Під час підготовки Стратегії враховуватимуться найкращі міжнародні практики, а до її розробки також залучатимуться фахівці приватного сектору та громадськості, які спеціалізуються на питаннях кібербезпеки, пообіцяв очільник РНБО…». ***(У РНБО почали розроблятиме стратегію кібербезпеки України // Укрінформ (https://www.ukrinform.ua/rubric-polytics/3105556-u-rnbo-pocali-rozroblati-strategiu-kiberbezpeki-ukraini.html). 24.09.2020).***

***

«Інтернет асоціація України (ІнАУ) направила листи до профільних парламентських комітетів із закликом відкликати два законопроєкти, які, на думку фахівців, створюють нові загрози кібербезпеці…

"В парламенті зареєстровані законопроєкти №4003 ("Про внесення змін до Кримінального процесуального кодексу України та Кодексу України про адміністративні правопорушення щодо підвищення ефективності протидії кібератакам" - ред.) та 4004 ("Про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів" - ред.), які під гаслами боротьби з кіберзлочинністю та кібератаками закладають механізми монополізації ринку та створюють нові загрози кібербезпеці держави", - йдеться у повідомленні.

В Асоціації вважають, що за своїм змістом ці законодавчі новації жодним чином не сприятимуть протидії кіберзлочинності.

"Фактично, це створення чергового механізму негативного управління операторами, провайдерами телекомунікацій, втручання в їх господарську діяльність, як це іноді відбувається, коли правоохоронні органи, ігноруючи положення кримінального процесуального законодавства, вилучають телекомунікаційне обладнання", - зазначають в ІнАУ.

На думку експертів, результатом прийняття цих документів стане "не лише посилення репресивного механізму в інтернеті, а й значне підвищення вартості телекомунікаційних послуг". "Адже придбання операторами за власний кошт обладнання для потреб силовиків для здійснення оперативно-розшукових заходів та негласних слідчих дій витримають лише монополісти сфери телекому. Вони не лише перекладуть на споживачів вартість поліцейського обладнання, але й сповна скористаються «перевагами» від знищення конкурентів з малого та середнього бізнесу", - вважають в ІнАУ.

Інтернет асоціація України закликає парламентаріїв "відкликати новації, які під гаслами боротьби з кіберзлочинністю та кібератаками знищують цивілізований український телеком-ринок", а натомість імплементувати в українське законодавство європейську (Будапештську) Конвенцію про кіберзлочинність». ***(Інтернет асоціація України просить відкликати два законопроєкти // Укрінформ (https://www.ukrinform.ua/rubric-technology/3098046-internet-asociacia-ukraini-prosit-vidklikati-dva-zakonoproekti.html). 11.09.2020).***

***

«Верховная Рада Украины приняла Закон о разведке (№2412-д от 15.01.2020). В статье 15 закона сказано, что разведывательные органы могут по решению суда снимать информацию с транспортных телекоммуникационных сетей, а также отслеживать местоположение человека в сетях мобильной связи.

“Статья 15. Разведывательные мероприятия, которые проводятся на основании решение суда

1. Разведывательные органы могут проводить в отношении лица, места или вещи, которые находятся на территории Украины, такие разведывательные мероприятия:

1) наблюдение за лицом, вещью или местом, которое заключается в проведении визуального наблюдения за лицом или определенной вещью или местом в публично доступных местах с фиксацией соответствующих сведений и данных;

2) снятие информации с транспортных телекоммуникационных сетей, которое заключается в проведении отбора и фиксации содержания информации, которая передается лицом;

3) снятие информации в электронных информационных системах, которое заключается в поиске, обнаружении, фиксации сведений или данных, содержащихся в электронной информационной системе или ее части, путем доступа к такой системе или ее части без ведома ее владельца, владельца или держателя;

4) обследование публично недоступных мест, жилища или иного владения лица, которое заключается в негласном проникновении в такие места, жилье или владение лица и, при необходимости, фиксация сведений и данных об указанных объектах;

5) установление местонахождения радиоэлектронного средства, которое заключается в локализации местонахождения радиоэлектронного средства, в том числе мобильного терминала систем связи и других радиоизлучающих устройств, активированных в сетях операторов, провайдеров телекоммуникаций, без раскрытия содержания передаваемых;

6) обзор корреспонденции, который заключается в негласном отборе по идентификационным признакам корреспонденции, ее обработке, снятии копий или получении образцов.

Такие разведывательные мероприятия проводятся при условии, что они непосредственно связаны с осуществлением разведывательной деятельности за пределами Украины или направлены на получение разведывательной информации, которая имеет источник происхождения за пределами Украины, и исключительно на основании решения суда.”

Кроме того, внесены изменения в часть четвертую статьи 39 Закона Украины "О телекоммуникациях"

"Операторы телекоммуникаций обязаны за собственные средства устанавливать на своих телекоммуникационных сетях технические средства, необходимые для осуществления уполномоченными органами оперативно-розыскных мероприятий и разведывательных и обеспечивать функционирование этих технических средств, а также в пределах своих полномочий содействовать проведению оперативно-розыскных мероприятий и разведывательных и недопущению разглашения организационных и тактических приемов их проведения. Операторы телекоммуникаций обязаны обеспечивать защиту указанных технических средств от несанкционированного доступа"…» ***(Герман Богапов. Закон о разведке заставит провайдеров следить за гражданами за счет повышения абонплаты // Internetua (https://internetua.com/zakon-o-razvedke-zastavit-provaiderov-sledit-za-grajdanami-za-scset-povysheniya-abonplaty). 21.09.2020).***

***

«Одна из крупнейших ИТ-компаний Украины SoftServe, которая занимается консалтингом и предоставляет услуги в сфере цифровых технологий, подверглась кибератаке. В результате ряд внутренних сервисов работали с перебоями. На странице компании в Facebook сообщается, со ссылкой на старшего вице-президента по информационным технологиям, Адриана Павликевича:

«На компанию была осуществлена хакерская атака. Ее удалось быстро обнаружить и локализовать. Для предотвращения распространения атаки были изолированы некоторые сегменты внутренней сети и ограничена связь с сетями клиентов.

В течение дня работники сталкивались с перебоями в работе почтовых серверов, временно была приостановлена работа некоторых внутренних сервисов.

Внутреннее расследование продолжается, однако по предварительным оценкам, ни важная информация, ни клиентские данные не пострадали».

По предварительным данным, хакеры смогли получить частичный доступ к инфраструктуре SoftServe и запустить в нее вирус-шифровальщик и другие вредоносные программы. В результате пострадали часть почтовой системы и вспомогательных тестовых сред». ***(Шифровальщик временно вывел из строя почтовую систему SoftServe // Компьютерное Обозрение (https://ko.com.ua/shifrovalshhik_vremenno_vyvel_iz_stroya_pochtovuyu_sistemu_soft serve_134363). 03.09.2020).***

***

«Система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури на об'єктах моніторингу зафіксувала з 2 по 8 вересня на 14% більше підозрілих подій, ніж попереднього тижня, повідомляє Державна служба спецзв'язку і захисту інформації України.

«Переважна більшість зафіксованих підозрілих подій стосується спроб мережевого сканування (88%), застосування нестандартних протоколів (10%) і виявлення мережевого ШПЗ (1%). Система захищеного доступу державних органів до мережі інтернет заблокувала 24 765 різних видів атак. Переважна більшість – це мережеві атаки прикладного рівня (90%), атаки типу Harvest Attack (6%) та Brute-force (1%). DDoS-атак не зафіксовано», – йдеться в повідомленні.

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA у цей період зареєструвала та опрацювала 3343 кіберінциденти, що на 14% більше, ніж попереднього тижня.

«Переважна більшість опрацьованих інцидентів належить доменній зоні UACOM (близько 99%). Основна кількість інцидентів стосується розповсюдження ШПЗ (95%) та фішингу (4%) від загальної кількості», – йдеться в повідомленні…». ***(Кількість кіберінцидентів за тиждень зросла на 14% – Держспецзв'язку //***

Радіо Свобода (https://www.radiosvoboda.org/a/news-ukraina-kiberintsydenty/30827316.html). 08.09.2020).

***

«Оновлена робота проксі в мобільному додатку “ВКонтакте” має на меті збір російськими спецслужбами даних про громадян України. Спеціалісти Національного координаційного центру кібербезпеки при Раді національної безпеки та оборони взаємодіють з міжнародними колегами та партнерами для блокування роботи додатку “ВКонтакте” на території України. Про це йдеться у заяві РНБО, передає УНН.

"Активізація роботи російських соціальних мереж напередодні виборів може становити загрозу національній безпеці країни", - заявив заступник секретаря РНБО Сергій Демедюк, коментуючи інформацію щодо поновлення роботи на території України мобільного додатку соцмережі “ВКонтакте”, представники якої заявили, що обійшли блокування на території нашої країни.

За його словами, після застосування санкцій щодо соціальної мережі “ВКонтакте” фахівці українських правоохоронних органів вживають заходів до забезпечення реалізації санкційних обмежень.

"Водночас спецслужби Російської Федерації із використанням можливостей розробників програмного забезпечення шукають нові методи обходу санкцій. Зокрема нещодавно вчергове було оновлено роботу проксі в мобільному додатку та надано доступ до соцмережі “ВКонтакте” українським користувачам", - вели далі у РНБО.

“З моменту застосування санкцій ми бачимо періодичне поширення інформації про відновлення доступу до цієї соцмережі на території України, навіть не зважаючи на нестабільну роботу проксі. Ми впевнені, що цей додаток використовується російськими спецслужбами для збору даних про громадян України і всіх, у кого він встановлений”, — зазначив Демедюк.

Він також додав, що активізація роботи додатку має на меті не надання користувачеві доступу до соціальної мережі без застосування додаткових сервісів для обходу санкцій, а збір даних громадян України та поширення дезінформації для впливу на громадську думку і маніпулювання нею. “Такі дії зазвичай проводяться напередодні визначних подій. Нині це проведення в Україні місцевих виборів”, — сказав заступник секретаря РНБО.

"Спеціалісти Національного координаційного центру кібербезпеки при РНБО України взаємодіють з міжнародними колегами та партнерами для напрацювання заходів щодо реагування та блокування роботи мобільного додатку “ВКонтакте” на території України", - вказали у РНБО…». ***(Юлія Шрамко. У РНБО відреагували на обхід додатком "ВКонтакте" блокування // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1891670-u-rnbo-vidreaguvali-na-obkhid-dodatkom-vkontakte-blokuvannya). 15.09.2020).***

***

«РНБО посилює заходи для прихильників соціальної мережі “Вконтакте”. Заборони на її роботу на території України виявилося замало.

Тепер Рада планує поставити на облік в правоохоронних органах всіх українських користувачів “Вконтакте”.

Про це заявив секретар РНБО Олексій Данилов на онлайн-конференції “Перспективи діджіталізації країни і ризики кібербезпеки” 25 вересня.

“Я хотів би звернути увагу на користувачів, які користуються цим ресурсом, який є забороненим. Це повинна бути їх відповідальність – навіщо вони це роблять і для чого вони це роблять. Справа в тому, що зараз та система, яка починає працювати, – про всіх цих користувачів матимемо розуміння, вони будуть всі на обліку перебувати.

І якщо вони і далі будуть поширювати російську контент на території країни, то вони будуть мати певні проблеми вже безпосередньо з нашою Нацполіцією, з нашими силовими структурами “, – заявив Данилов.

Тг-канал “Жінка з косою” пише, що Зеленський був вкрай незадоволений заявою Глави РНБО Олексія Данилова. Данилов отримав чергове усне зауваження. Готується його відставка.

“Сьогодні Секретар РНБО Олексій Данилов на презентації Глобального центру взаємодії у кіберпросторі заявив, що в Україні будуть ставити на облік тих, хто користується ВКонтакте.

В Офісі Президента вже пішли чутки, що Данилова хочуть давно зняти, тому він гне таку жорстку лінію, щоб «врятувати» себе в кріслі Глави РНБО або після стати опозиціонером до своїх чинних «товаришів».

Всі наші джерела серед політтехнологів кажуть, що дана заява відмінний постріл по рейтингу Слуги Народу на Південному Сході. Десь дуже радіє ОПЗЖ і російські ЗМІ, які сміливо можуть сьогодні розганяти меседж, що в Україні немає демократії і свободи слова, а влада залякує народ “, – йдеться в повідомленні каналу». ***(Мар'яна Шажко. Готується відставка – Зеленський вкрай незадоволений. Після гучних заяв – його “попруть”. “Це постріл у спину” // Корупція Інфо (https://korupciya.com/gotuyetsya-guchna-vidstavka-zelenskyj-vkraj-nezadovolenyj-pislya-guchnyh-zayav-jogo-poprut-cze-postril-u-spynu/). 26.09.2020).***

***

«Обчислити кількість активних користувачів забороненої російської соцмережі "ВКонтакте"в Україні неможливо.

Так прокоментував ініціативу РНБО поставити на їх на облік експерт з питань кібербезпеки Сергій Денисенко…

За його словами, користувачі, які заходить на сайт соцмережі в Україні, через сервіси VPN помилково відображаються як відвідувачі з інших країн.

"Як можна поставити користувачів на облік - для цього потрібно упевнитися, що аккаунт дійсний і належить конкретній людині, а не "тролю". Для цього потрібно відстежувати інформацію на сторінці, моніторити зв'язки і проводити аналітику. Інформація про користувачів знаходиться у власника соцмережі. Це телефонний номер, пошта і так далі. Якщо правоохоронці зможуть брати цю інформацію у власника, тоді зможуть моніторити", - пояснив Денисенко.

Він також розповів, навіщо українці використовують заборонену соцмережу.

"Варто відзначити, що багато користувачів через соцмережу спілкуються з близькими людьми за кордоном. Також в цій мережі активно поширюються фейки. Вона залишається одним з майданчиків інформаційної війни", - сказав він…». ***(Експерт розповів, чи можливо поставити на облік українських користувачів "ВКонтакте" // Багнет (http://www.bagnet.org/news/tech/1292932/ekspert-rozpoviv-chi-mozhlivo-postaviti-na-oblik-ukrayinskih-koristuvachiv-vkontakte). 29.09.2020).***

***

«Держспецзв'язку повідомила інформацію щодо захисту державних інформаційних ресурсів за період з 16 по 22 вересня 2020 року. Система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури на об'єктах моніторингу зафіксувала 533 453 підозрілих події. Це на 11% більше, ніж попереднього тижня. Переважна більшість зафіксованих підозрілих подій стосується спроб мережевого сканування (82%), застосування нестандартних протоколів (15%), виявлення мережевого ШПЗ та спроб отримання прав адміністратора (по 1% кожний).

Система захищеного доступу державних органів до мережі Інтернет заблокувала 306 376 атак різних видів. Переважна більшість – це мережеві атаки прикладного рівня (99%). Також система кіберзахисту зафіксувала 1 DDoS-атаку. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA у цей період зареєструвала та опрацювала 2 894 кіберінциденти, що на 24% менше, ніж попереднього тижня. Переважна більшість опрацьованих інцидентів стосується недержавного сектору (близько 99%). Основна кількість інцидентів стосується розповсюдження ШПЗ (99%)». ***(Грицина Вікторія. Державна система кіберзахисту зафіксувала понад півмільйона підозрілих подій // Pingvin Pro (https://pingvin.pro/gadgets/news-gadgets/derzhavna-systema-kiberzahystu-zafiksuvala-ponad-pivmiljona-pidozrilyh-podij.html). 22.09.2020).***

***

«У великій українській компанії готуються до нових публікацій даних, які викрали хакери, а також пояснили як сталася кібератака

Про це передає Економічна правда."У результаті [атаки] було пошкоджено поштовий сервер компанії, виведено з ладу низку корпоративних сервісів, скомпрометовано внутрішній файловий сервер. Зловмисникам вдалося скачати фрагменти різної інформації, яку, з метою тиску на компанію, вони виклали у відкритий доступ.

…Ми очікуємо, що нові дані знову можуть бути опубліковані і готові до цього", — пояснюють у SoftServe.

Також у компанії пояснюють, що усі ключові корпоративні системи знаходяться на захищених хмарних платформах низки світових провайдерів, які не постраждали.

«Ми залучили зовнішню компанію — одного з провідних світових експертів з кібербезпеки для проведення комплексного незалежного розслідування цього інциденту, яке буде завершене найближчим часом», — резюмують у компанії». ***(IT-***

шники розповіли про те, як їх зламали та готуються до нового зливу // Високий Замок (https://wz.lviv.ua/news/420805-it-shniki-rozpovili-pro-te-yak-jikh-zlamali-ta-gotuyutsya-do-novogo-zlivu). 21.09.2020).

***

«Сайти обласних управлінь поліції по всій Україні зазнали кібератаки. Невідомі оприлюднили на регіональних сайтах низку фейкових повідомлень.

Зокрема, на сайті Вараської міськради (м. Вараш Рівненської області) сьогодні з'явилось фейкове повідомлення про нібито викид радіації на Рівненській АЕС. Цю інформацію поспішили спростувати як у міськраді, так і на самій електростанції.

Тим часом, на сайті львівської поліції з'явився фейк про загибель трьох бійців ЗСУ. Наразі в Львській області проходять міжнародні військові навчання «Rapid Trident-2020».

Поліція Миколаївської області повідомила про несанкціоноване втручання у роботу свого офіційного вебсайта, він тимчасово відключений. У місцевій журналістській Facebook спільноті повідомили, що там було оприлюднено неправдиву інформацію про ДТП з п'ятьма загиблими.

Аналогічна ситуація склалась з поліцією Херсонської області. На її сайті з'явилось фейкове повідомлення про загибель американських військових радників. Інформацію вже спростували.

Прес-служба національної поліції у Facebook повідомила про злам свого сайту. Стверджується, що «у зв'язку з цим на деяких інтернет-сторінках обласних управлінь поліції була поширена недостовірна інформація». Сайт Національної поліції України тимчасово відключений». ***(Сайти органів влади по всій Україні атакували хакери: оприлюднено низку шейків // SVOBODA.FM (http://svoboda.fm/adventure/275406.html). 23.09.2020).***

***

«В то время, как кибермошенники переключились на онлайн-шопинг, мошенники с помощью QR-кодов воруют деньги с карточек украинцев и блокируют их телефоны…

Так, сообщается, что QR-коды ведут на вредоносные сайты. Перейдя по зашифрованной в коде ссылке, можно попасть на ресурс, где сразу же предложат скачать вредоносную программу.

Как сообщила эксперт по кибербезопасности Маргарита Сичкарь, такая программа способна украсть пароли от социальных сетей, позволит мошенникам попасть в банковское приложение или даже заблокирует телефон.

«Сейчас во многих местах общественного питания используют QR код в качестве меню. Этот способ мошенничества уже давно работает в других странах, там массово распространяют коды просто на столбах», – рассказывает Сичкарь.

Как уберечь себя:

- считывать QR код только в том случае, если вы знаете, кто его разместил;
- проверять перед считыванием, не наклеили ли на QR код новую наклейку;
- не загружать файлы с любых сайтов по коду.

«Если вы используете код в кафе и ресторанах, попросите, убедитесь, что это код, который оставили именно сотрудники ресторана. Считывать коды со столбов, в метро и т.д. вообще нельзя ни в коем случае», – рассказывает Сичкарь». ***(Мошенники научились красть деньги с QR-кодов. Способы уберечь свой телефон // NDEPENDENT MASSMEDIA LLP (https://job-sbu.org/moshenniki-nauchilis-krast-dengi-s-qr-kodov-sposobyi-uberech-svoy-telefon-27193.html). 21.09.2020).***

***

«…Арсен Аваков сказав, що за останні 5 років кількість кіберзлочинів зросла у 2,5 рази, а кіберпростір став п'ятою сферою ведення бойових дій.

«На жаль, Україна опинилась на передовій цієї нової війни. Агресія з боку Російської Федерації відбувається не тільки у вигляді військових дій, інформаційних компаній та економічних диверсій, але і у вигляді жорсткої кібервійни», - заявив міністр.

Арсен Аваков наголосив, що для ефективної протидії кіберзлочинності та гібридним загрозам, МВС виступає ініціатором створення на базі глобального центру взаємодії в кіберпросторі інтеграційного майданчика, який об'єднає усіх ключових гравців та забезпечить максимальну синергію та ефективність української екосистеми безпечного кіберпростору, та як логічний наслідок – посилення системи Національної безпеки України.

«На наше переконання та зважаючи на вимоги сьогодення, підрозділи кібербезпеки повинні бути створені у кожному державному органі та установі. Крім того, кіберполіція переходить на новий рівень - її діяльність, окрім безпосередньої боротьби із кіберзлочинністю, буде спрямовано на:виявлення та прогнозування можливих кіберзагроз, у тому числі з використанням штучного інтелекту; надання партнерам інформаційно-консультативної підтримки; вироблення у міжнародній кооперації механізму протидії існуючим та потенційним загрозам, у тому числі глобальним», - підкреслив очільник МВС.

Окремо міністр внутрішніх справ зазначив що лише у цьому році Департамент кіберполіції Національної поліції України знешкодив злочинне угрупування, яке за допомогою криптовалют легалізувало більше 40 мільйонів доларів США, здобутих злочинним шляхом, припинив діяльність хакерського угрупування, учасники якого створювали шкідливе програмне забезпечення, несанкціоновано втручалися у роботу банків, викрадали та легалізовували кошти, ліквідував злочинну групу, яка здійснювала втручання у роботу електронних систем та баз даних державних органів, незаконно збирала інформацію з обмеженим доступом (персональні дані громадян, закриті відомості фінансово-господарської діяльності фізичних та юридичних осіб) та реалізовувала її на різноманітних вебресурсах.

«Наразі ми оголошуємо новий набір до лав Кіберполіції – запрошуємо сміливих, яскравих, вмотивованих і креативних – тих, хто готовий боротися і захищати Україну! Ми маємо стати «командою команд», яка буде потужним партнером світової спільноти безпечного віртуального простору», - зазначив Арсен Аваков». ***(Арсен Аваков: Кіберполіція переходить на новий рівень роботи та***

оголошує великий набір спеціалістів // Кіберполіція України (https://cyberpolice.gov.ua/news/arsen-avakov-kiberpolicziya-perexodyt-na-novyj-riven-roboty-ta-ogoloshuye-velykyj-nabir-speczialistiv-1858/). 25.09.2020).

***

«За фактом несанкціонованого втручання в роботу вебсайта Нацполіції розпочато кримінальне провадження

У рамках досудового розслідування встановлюються обставини несанкціонованого доступу та особи, які його здійснили.

Нагадаємо: сьогодні об 11:45 зафіксовано несанкціоноване втручання у роботу офіційного вебсайта Нацполіції. У зв'язку з цим на деяких інтернет-сторінках обласних управлінь поліції була поширена недостовірна інформація на інтернет-сторінках поліції Херсонської, Рівненської, Миколаївської, Вінницької та Львівської областей.

На цей час сайт Національної поліції України проходить техобслуговування, фахівці працюють над відновленням його роботи.

За цим фактом розпочато кримінальне провадження за 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.

Кіберполіцейські з'ясовують обставини несанкціонованого доступу до сайта та встановлюють причетних осіб.

Аналогічне кримінальне провадження розпочато за фактом несанкціонованого втручання в роботу Вараської міської ради, де невідомі також сьогодні розмістили фейкову інформацію.

Санкція статті передбачає позбавлення волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років». ***(За фактом несанкціонованого втручання в роботу вебсайта Нацполіції розпочато кримінальне провадження // Кіберполіція України (https://cyberpolice.gov.ua/news/za-faktom-nesankczionovanogo-vtruchannya-v-robotu-vebsayta-naczpoliczii-rozpochato-kryminalne-provadzhennya-4911/). 23.09.2020).***

***

«Голова Нацполіції Ігор Клименко заявив, що після злому сайту Національної поліції України ніяких витоків документів з відомства не відбулося. Кібератака торкнулася тільки розділу новин порталу…

"Сайт Нацполіції не "ліг". "Ліг" виключно новинний розділ сайту Нацполіції. Ми його відразу відключили від мережі. Буквально з'явилося дві новини - і сайт Національної поліції нами ж відразу був покладений, щоб з'ясувати, чому сталося втручання в роботу сайту", - сказав Клименко.

Він також заявив, що в Нацполіції встановили причини злому.

"Але ніякої видачі (інформації назовні, - ред.), ніяких документів, ніяких скріншотів просто не може бути, це я вам заявляю відповідально", - підкреслив Клименко.

Нагадаємо, в середу, 23 вересня, зловмисники скоїли несанкціоноване втручання в роботу офіційного веб-сайту Нацполіції. У зв'язку з цим на деяких інтернет-сторінках обласних управлінь поліції була поширена недостовірна інформація.

Повідомлення про викид радіоактивних речовин під час навчання на АЕС з'явилося на кількох сторінках обласних управлінь Нацполіції і на сайті Варашского міської ради. Незабаром спікерка Нацполіції в Рівненській області Марія Юстицкий заявила, що цій інформації довіряти не варто». ***(Елизавета Чижик. Нацполіція: Витоку документів в результаті кібератаки на сайт не було // Дзеркало тижня. Україна (https://zn.ua/ukr/UKRAINE/natspolitsija-vitoku-dokumentiv-v-rezultati-kiberataki-na-sajt-ne-bulo.html). 29.09.2020).***

***

«З 23 по 29 вересня було зафіксовано та заблоковано 8 DDoS-атак, переважна більшість — на веб-ресурси Офісу Президента України. Про це повідомляє УНН із посиланням на пресслужбу Державної служби спеціального зв’язку та захисту інформації України.

“Система кіберзахисту державних інформаційних ресурсів та об’єктів критичної інфраструктури на об’єктах моніторингу зафіксувала 1 073 948 підозрілих подій. Переважна більшість зафіксованих підозрілих подій стосується спроб мережевого сканування (91%) та застосування нестандартних протоколів (7%)”, — сказано у повідомленні.

Зазначається, що система захищеного доступу державних органів до мережі Інтернет заблокувала 48 742 атаки різних видів.

“Переважна більшість — це мережеві атаки прикладного рівня (99%). Також зафіксовано 8 DDoS-атак. Переважна більшість стосується веб-ресурсів Офісу Президента України”, — додається у повідомленні.

Так, урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA у цей період зареєструвала та опрацювала 2 268 кіберінцидентів, що на 22% менше, ніж попереднього тижня.

Переважна більшість опрацьованих інцидентів стосується недержавного сектору (близько 99%). Основна кількість інцидентів стосується розповсюдження ШПЗ (99%)…». ***(Валерія Гуржий. За тиждень зареєстровано низку кібератак на сайт Офісу Президента // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1894425-za-tizhden-zareyestrovano-nizku-kiberatak-na-sayt-ofisu-prezidenta). 29.09.2020).***

***

Боротьба з кіберзлочинністю в Україні

«Група українських компаній, за даними Служби безпеки України, продавала шпигунське програмне забезпечення, розроблене російськими спецслужбами. Про блокування цієї схеми СБУ відзвітувала в п'ятницю, 4 вересня.

За оперативною інформацією, було продано більше 100 шкідливих програмних прод уктів. Серед покупців були, зокрема, державні структури. Софт, про який йдеться, збирав інформацію і передавав її на сервера спецслужб РФ.

Експертиза підтвердила, що програми є шпигунськими. Згідно з попередніми висновками фахівців з кібербезпеки, софт працював в інтересах спецслужб держави-агресора.

У рамках розслідування СБУ провела обшуки в офісах підприємців у Києві і Дніпропетровській області. Правоохоронці вилучили обладнання, речі та документи.

У СБУ стверджують, що кіберспеціалісти спецслужби допомагають потерпілим коректно видалити шпигунський софт, а оперативники - встановлюють усіх покупців.

Організатору групи вручили повідомлення про підозру за ч. 2 ст. 359 Кримінального кодексу (незаконне придбання, збут або використання спеціальних технічних засобів отримання інформації за попередньою змовою групою осіб)…» ***(СБУ відзвітувала про блокування продажу російського шпигунського софта // Дзеркало тижня. Україна (https://zn.ua/ukr/UKRAINE/sbu-vidzvituvala-pro-blokuvannja-prodazhu-rosijskoho-shpihunskoho-softa.html). 05.09.2020).***

***

«Как сообщается, неизвестный подсадил в IT-системы четырех немецких компаний программу-троян «Rapid (VI)», и зашифровал с ее помощью все важные документы и данные. Связавшись по электронной почте с сотрудниками этих компаний, он предложил восстановить данные.

Восстановление он попросил оплатить биткойнами, в эквиваленте 2 тыс. долларов США (если деньги переведут в течение 2 дней). Если же с переводом денег возникнут проволочки – стоимость дешифровки автоматически поднимется до 5 тысяч долларов.

Чтобы подтвердить, что он в состоянии сдержать свое обещание, хакер прислал несколько дешифрованных файлов.

Большинство законопослушных немцев не стали вести переговоров с вымогателем и обратились в компетентные органы. И только сотрудник частного конструкторского бюро попробовал выполнить требования вымогателя и отправил ему 0,25 BTC (2002,00 $). Несмотря на это, хакер так и не выполнил своего обещания.

Проанализировав все факты и данные, немецкая полиция пришла к заключению, что, хотя адреса электронной почты, с которых писали компаниям, были разными, все эти случаи имеют схожий почерк – одинаковый текст сообщений и та же самая версия программы-трояна, несмотря на то, что на момент инцидента существовали уже более свежие версии. Следовательно, пришли к заключению немцы, во всех эпизодах фигурирует один и тот же человек, либо группа людей.

Использовав телекоммуникационные методы слежения, правоохранители выяснили IP-адреса, с которых злоумышленник осуществлял доступ к почтовому серверу и переписку. Большинство из них удалось проследить до типичных

серверов анонимизации TOR и VPN, на этом следы обрывались и следствию не удалось продвинуться в данном направлении.

Однако часть соединений осуществлялась с украинских IP-адресов. Сперва эти случаи были единичными, а в последствии они участились. Следователи пришли к заключению, что эти адреса не были зашифрованы в результате сбоя анонимайзера, и являются настоящими IP-адресами злоумышленника.

В результате, на основании ст. 29 Конвенции о киберпреступности, Федеральное управление уголовной полиции Германии затребовало осуществить так называемое «предварительное сохранение» всех учетных данных ряда украинских интернет-провайдеров.

На основании данного запроса, Святошинский суд Киева постановил предоставить доступ к данным указанных интернет-провайдеров, поскольку они имеют существенное значение в деле установления, кто являлся пользователем подозреваемых IP-адресов в искомый период времени.

В случае, если до 5 сентября 2020 года провайдеры не предоставят интересующие следствие данные добровольно, суд дал полицейским право на временное изъятие серверов и документов компаний». ***(Андрей Майданик. Киберполиция вышла на след украинского хакера-вымогателя, совершившего преступления в Германии // InternetUA (https://internetua.com/kiberpoliciya-vyshla-na-sled-ukrainskogo-hakera-vymogatelya-sovershivshego-prestupleniya-v-germanii). 04.09.2020).***

***

«Правопорушник, 27-річний одесит, маючи заздалегідь збережені логіни та паролі доступу до облікових записів, через власний комп’ютер підключався до бази даних однієї з державних установ та зчитував з неї інформацію.

Викрили неправомірні дії чоловіка слідчі Приморського відділу поліції, під оперативним супроводом кіберполіцейських та під процесуальним керівництвом місцевої прокуратури №3, в ході розслідування кримінального провадження.

Про викриття зловмисника, у пособництві з яким правопорушник скоював вказані неправомірні дії, повідомлялося раніше. Йому правоохоронці оголосили про підозру за частинами 1 та 3 ст. 358 (Підроблення документів, печаток, штампів та бланків, збут чи використання підроблених документів, печаток, штампів), частинами 1 та 2 ст. 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) та ч. 1 ст. 263 (Незаконне поводження зі зброєю, бойовими припасами або вибуховими речовинами) Кримінального кодексу України.

В подальшому правоохоронці провели обшук за місцем мешкання пособника 34-річного одесита та вилучили комп’ютерну техніку, телефон та накопичувач на магнітних дисках, що прямо вказують на його причетність до злочину.

Фігуранту оголосили підозру за ч. 5 ст. 27, частинами 1 та 2 ст. 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку) Кримінального кодексу України. Таке правопорушення, згідно з

чинним законодавством, карається позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років». ***(Співробітники кіберполіції затримали хакера, який несанкціоновано втручався в роботу державних інформаційних систем // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/spivrobitnyky-kiberpolicziyi-zatrymaly-xakera-yakyj-nesankczionovano-vtruchavsya-v-robotu-derzhavnyx-informaczijnyx-system-2284/). 04.09.2020).***

***

«Співробітники Департаменту кіберполіції викрили 24-річного мешканця Харкова, який маючи певні навички у комп'ютерній інженерії, неодноразово блокував онлайн-бронювання квитків на концерти улюбленої співачки (за неперевіреною інформацією Христина Соловій).

Про це повідомляє пресслужба Департаменту кіберполіції.

Чоловік здійснював DDoS-атаки на сайти та налаштував бот-мережу, яка перешкоджала іншим користувачам у купівлі квитків. При цьому фігурант використовував іноземні VPN сервіси.

В результаті таких дій, два концерти співачки були скасовані. Ще три – відбулися за присутності лише 30% глядачів.

За попередніми даними, сума збитків сягає більше пів мільйона гривень.

Правоохоронці провели обшук за місцем проживання фігуранта. За результатами вилучили комп'ютерну техніку та мобільні телефони. Речові докази направлені на проведення відповідних експертиз.

"Відкрито кримінальне провадження за ч.1 ст. 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України. Максимальне покарання, яке загрожує зловмиснику – позбавлення волі на строк до шести років. Слідчі дії тривають", – йдеться у повідомленні». ***(Шанувальник української співачки вчиняв кібератаки, аби зривати її концерти, — кіберполіція // Новини Полтавщини (https://np.pl.ua/2020/09/shanuval-nyk-ukrains-koi-spivachky-vchyniav-kiberataky-aby-zryvaty-ii-kontserty-kiberpolitsiia/). 22.09.2020).***

***

«16-річний житель Донеччини створив «вірус», який викрадав конфіденційну інформацію користувачів. Свою розробку хлопець продавав у месенджерах. Один екземпляр такого програмного забезпечення коштував 300 гривень.

Працівники кіберполіції в Донецькій області спільно зі слідчими поліції регіону, під процесуальним керівництвом обласної прокуратури, викрили юнака у створенні та збуті шкідливого програмного забезпечення. Кіберполіція встановила, що 16-річний мешканець Маріуполя, маючи відповідні знання та навички у сфері програмування, самостійно розробив шкідливе програмне забезпечення.

Програма мала фунціонал прихованого шпигунства за користувачем і викрадала збережену конфіденційну інформацію. «Вірус» був налаштований таким чином, щоб викрадена інформація надсилалась листом на поштову скриньку зловмиснику. Юнак власну розробку продавав бажаючим у месенджерах по 300 гривень.

Правоохоронці провели обшук за місцем проживання фігуранта. За результатами вилучено комп'ютерну техніку та мобільний телефон. Речові докази направлені на проведення відповідних експертиз.

Відкрито кримінальне провадження за ч. 1 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) Кримінального кодексу України. Вирішується питання щодо оголошення підозри». ***(Кіберполіція викрила юного хакера у створенні та продажі шкідливого програмного забезпечення // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-yunogo-xakera-u-stvorenni-ta-prodazhi-shkidlyvogo-programnogo-zabezpechennya-1585/). 16.09.2020).***

***

«Как сообщается, сотрудники департамента Киберполиции выявили, что неустановленная личность, путем подбора паролей систематически получала доступ к аккаунтам пользователей ряда торговых интернет-площадок. Это дало ему доступ к платежным картам и Paypal аккаунтам пользователей, средства с которых он тратил в различных интернет-магазинах на покупку дорогостоящей электроники.

Начав расследовать этот инцидент, полиция установила группу лиц, проживающих на территории Одесской области, которые являются постоянными участниками даркнетовских форумов для кардеров (сайты, расположенные в зашифрованной области интернета).

Сперва правоохранителям удалось раздобыть IP-адрес одного из них. Пробив данные через местного интернет-провайдера, полицейские идентифицировали молодого человека, проживающего вместе с родителями. Дальнейший анализ его контактов и переписки на тематических форумах кардеров, дал полицейским возможность установить личности еще двух никнеймов, которые занимаются кражей и копированием банковских карт.

Несмотря на то, что следствию удалось установить личности подозреваемых и даже провести обыски по месту их жительства, полицейские до сих пор не вручили им подозрения, поскольку не успели провести все необходимые компьютерно-технические экспертизы и не установили свидетелей, которым известны обстоятельства преступлений.

Поэтому они обратились в суд, чтобы продолжить срок досудебного расследования – до января 2021 года. Причины, по которым расследование затягивается, указаны следующие: необходимость проведения специальной технической экспертизы, а также загруженность другими, более тяжкими, уголовными преступлениями.

Вообще, поимка киберпреступников, ворующих и подделывающих банковские карты – нечастый праздник на улице украинской Киберполиции. Если заглянуть в Единый реестр судебных решений, по запросу «кардер» можно найти «аж» 12 постановлений, связанных с уголовными делами и всего 1 приговор (и тот – оправдательный), который был вынесен еще в 2013 году.

Большинство же постановлений, которые датированы периодом 2018 – 2019 г.г. касаются как раз расследования южноукраинской группировки кардеров. Поэтому, если следствие успеет завершить все необходимые процессуальные действия и предъявит кардерам подозрение в январе 2021 года, это будет большим достижением отечественной Киберполиции». ***(Андрей Майданик. Киберполиция напала на след украинской группировки карточных хакеров // Internetua (https://internetua.com/kiberpoliciya-napala-na-sled-ukrainskoi-gruppirovki-kartocsnyh-hakerov). 23.09.2020).***

***

«Мережу ботоферм виявили на території Києва та Запорізької області.

Столичні правоохоронці викрили межрегіональну мережу ботоферм із майже 3,5 тис. акаунтів. Про це повідомляє пресслужба Київської міської прокуратури у Facebook.

У ході розслідування правоохоронці встановили, що мережа ботоферм діяла на території Києва та Запорізької області. Її організатори керували обліковими записами у соціальних мережах, електронними поштовими скриньками та електронними гаманцями з використанням фейкових персональних даних. Для реєстрації акаунтів використовувались українські та іноземні SIM-картки операторів зв'язку.

Вказані послуги, за даними прокуратури, надавались в інтересах третіх осіб з метою інспірування соціальних конфліктів, поширення неправдивої інформації щодо політичних конкурентів замовників, підбурювання до протестів тощо.

У межах кримінального провадження проведено одночасні обшуки за адресами розташування спеціального обладнання, під час яких вилучено технічне забезпечення, понад 6 тисяч сім-карток та інші речові докази.

Слідство наразі встановлює осіб причетних до організації діяльності ботоферм…» ***(Столичні правоохоронці викрили межрегіональну мережу ботоферм із майже 3,5 тис. Акаунтів // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/25517/2020-09-17-stolichni-pravookhorontsi-vikrili-mezhregionalnu-merezhu-botoferm-iz-maizhe-35-tis-akauntiv/). 17.09.2020).***

***

«…Співробітники Департаменту кіберполіції спільно з Головним слідчим управлінням та слідчими Херсонщини, під процесуальним керівництвом Офісу Генпрокурора України, а також у співпраці з іноземними правоохоронними органами, викрили групу зловмисників у несанкціонованому списанні грошей з банківських рахунків громадян Східної Європи.

Кіберполіція встановила, що до таких дій причетні п’ятеро жителів Херсонщини, віком 22-27 років. Молодики розробили шкідливе програмне забезпечення, що давало змогу їм заволодівати грошима з банківських карток.

Правопорушники, видаючи себе за працівників банку, у телефонних розмовах дізнавалися реквізити рахунків та інші персональні дані іноземців. Молодики надсилали їм на електронні скриньки листи, що містили посилання на «вірус». Таким чином вони отримували доступ до банківського рахунку. Далі гроші потерпілих списували та обготівковували в Україні.

За попередніми підрахунками, від таких дій постраждали близько ста осіб. Їм завдано збитків на понад 20 тисяч доларів.

Правоохоронці провели обшуки за місцями проживання фігурантів та вилучили речові докази.

Фігурантам оголошено про підозру у вчинені правопорушення, передбаченого 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.

Максимальне покарання, яке загрожує підозрюваним – позбавлення волі на строк до шести років. Слідчі дії тривають». ***(Кіберполіція викрила групу зловмисників у спустошенні банківських карток іноземних громадян // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-grupu-zlovmysnykiv-u-spustoshenni-bankivskyx-kartok-inozemnyx-gromadyan-3599/). 28.09.2020).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Сьогодні Україна та Іспанія підписали низку важливих документів…

Зокрема, йдеться про Конвенцію між Україною та Королівством Іспанія про уникнення подвійного оподаткування стосовно податків на доходи та запобігання податковим ухиленням і уникненням та протокол до неї.

“Усунення перешкоди для закордонних інвестицій та торгівлі. Угода, підписана на заміну застарілої радянсько-іспанської від 1985 року, остаточно скасовує подвійне оподаткування однієї дії двома країнами та унеможливлює всі махінації навколо”, – повідомили у відомстві.

Також було підписано Меморандум про взаєморозуміння між Міністерством розвитку економіки, торгівлі та сільського господарства України та Міністерством сільського та рибного господарства і продовольства Королівства Іспанія в галузі сільського господарства та харчової промисловості.

“Реалізація українсько-іспанського потенціалу розвитку співпраці в аграрній сфері. Нові можливості для обміну досвідом та найефективнішими практиками, а також поглиблена взаємодія у сфері торгівлі аграрною продукцією”, – прокоментували в МЗС.

Окрім цього, сторони підписали Меморандум про взаєморозуміння між Міністерством закордонних справ України та Міністерством закордонних справ, Європейського Союзу та співробітництва Королівства Іспанія у сфері кібербезпеки.

“Обмін “чутливою” інформацією заради спільної кібербезпеки. Міжгалузева взаємодія – від юридичних до научних аспектів. Україна та Іспанія координуватимуть позиції профільних інституцій при міжнародних організаціях”, – зазначили в МЗС.

Четвертим документом, який підписали сьогодні, є Угода між Україною та Королівством Іспанія про співпрацю та взаємну допомогу в митних справах.

“Тісніша взаємодія та обмін інформацією між митницями України та Іспанії. Зменшення простору для шахрайства – збільшення простору для чесної взаємовигідної торгівлі”, – прокоментували у відомстві». ***(Податки, кібербезпека: Україна та Іспанія підписали 4 угоди // UA\|TV (https://uatv.ua/podatky-kiberbezpeka-ukrayina-ta-ispaniya-pidpysaly-4-ugody/). 10.09.2020).***

***

«Заместитель Секретаря СНБО Украины Сергей Демедюк и старший директор Международного фонда избирательных систем (IFES) Питер Эрбен подписали Меморандум о сотрудничестве между Аппаратом СНБО Украины и IFES, сообщили в пресс-службе СНБО.

Отмечается, что документ направлен на организацию сотрудничества в сферах кибербезопасности и защиты критической инфраструктуры, в частности развитие системы подготовки и переподготовки кадров в сфере защиты критической инфраструктуры и киберзащиты критической инфраструктуры.

Демедюк ознакомил Эрбена с работой Национального координационного центра кибербезопасности (НКЦК) при СНБО Украины и отметил, что Центр приобретает все большее значение в жизни государства, поскольку в нем на высшем уровне «объединены усилия и ресурсы для противодействия угрозам в киберпространстве, информационном пространстве и угрозам критической инфраструктуре».

«Если мы говорим о кибербезопасности, то она сегодня охватывает безопасность повседневной жизни людей и страны во всех сферах», — добавил Демедюк, поблагодарив государства-партнеры и соответствующие организации за всестороннюю поддержку в развитии национальной системы кибербезопасности.

Заместитель Секретаря СНБО Украины выразил уверенность, что Меморандум с IFES будет способствовать привлечению лучших мировых практик для усиления национальной системы образования и обучения по вопросам защиты критической инфраструктуры и киберзащиты критической инфраструктуры.

«В дальнейшем это будет способствовать разработке эффективных стратегий деятельности владельцев и управленцев критической инфраструктуры, сделает их активы более безопасными и жизнеспособными», — отметил Демедюк.

В свою очередь, Эрбен убежден, что киберугрозы являются «одними из основных угроз демократии во всем мире», что требует углубления сотрудничества государств-партнеров в вопросах эффективного противодействия этим угрозам.

Как сообщал «Журналист», в СНБО заявили, что в Украине кризис с действующей системой образования, что формирует угрозы государственной и национальной безопасности». ***(СНБО подписал Меморандум о сотрудничестве с Международным фондом избирательных систем // journalist (https://journalist.today/snbo-podpisal-memorandum-o-sotrudnichestve-s-mezhdunarodnym-fondom-izbiratelnyh-sistem/). 11.09.2020).***

***

«США планируют подписать с Грузией, Украиной и Сербией меморандум о безопасности создания сетей мобильной связи пятого поколения (5G). Об этом сообщил и.о. помощника госсекретаря США по делам Европы и Евразии Филип Рикер.

«Планируется подписать меморандум о взаимопонимании по 5G с Украиной, Грузией и Сербией, чтобы заручиться обязательствами этих стран-партнеров по неиспользованию запрещенных технологий», — говорит Рикер в письменном вступительном слове, подготовленном к слушаниям в комитете Сената Конгресса США по иностранным делам.

Он напомнил о Пражских положениях, согласованных представителями 32 стран в рамках международной конференции по вопросам безопасности сетей мобильной связи 5G в мае 2019 года.

«Более 30 стран внесли свой вклад в Пражские предложения по созданию безопасной сетевой инфраструктуры 5G, отказа от услуг поставщиков из авторитарных государств, таких как Коммунистическая партия Китая», — добавил Рикер.

Пражские предложения – рамочная программа кибербезопасности. Она представляет собой набор рекомендаций, которые следует учитывать странам при разработке, строительстве и управлении своей телекоммуникационной инфраструктурой 5G.

США неоднократно предупреждали союзников об опасности использования китайского оборудования производства компаний Huawei или ZTE для построения телекоммуникационной инфраструктуры своих стран. В Вашингтоне считают, что Пекин может использовать 5G для шпионажа. Законодательство Китая, включая законы КНР о безопасности и разведке, позволяет Пекину принуждать китайские компании к сотрудничеству с органами разведки страны…». ***(США планируют подписать с Грузией меморандум о безопасности создания сетей 5G // Новости-Грузия (https://www.newsgeorgia.ge/%d1%81%d1%88%d0%b0-%d0%bf%d0%bb%d0%b0%d0%bd%d0%b8%d1%80%d1%83%d1%8e%d1%82-%d0%bf%d0%be%d0%b4%d0%bf%d0%b8%d1%81%d0%b0%d1%82-%d1%81-%d0%b3%d1%80%d1%83%d0%b7%d0%b8%d0%b5%d0%b9-%d0%bc%d0%b5%d0%bc%d0%be/). 18.09.2020).***

***

«США и Эстония выступили с совместным заявлением о важности безопасной телекоммуникационной инфраструктуры.

Заместитель госсекретаря США по вопросам экономического роста, энергетики и окружающей среды США Кит Крак и министр иностранных дел Эстонии Урмас Рейнсалу подчеркнули твердую приверженность двух стран общим принципам безопасности сетей 5G и международно признанным стандартам доверия к цифровым технологиям.

В ходе встречи в Таллинне они обсудили пути дальнейшего развития сотрудничества в обеспечении безопасности критически важной телекоммуникационной инфраструктуры и обеспечении чистоты цепочек поставок.

Как отмечается в заявлении, Эстония активно борется за безопасность телекоммуникационной инфраструктуры, кибербезопасность и ответственное поведение государств в киберпространстве. США демонстрируют аналогичную приверженность этим принципам. Госсекретарь Помпео призвал правительства и компании присоединиться к инициативе Clean Network, которая представляет собой комплексный подход к борьбе с угрозами для конфиденциальности и безопасности данных.

Признавая, что сети 5G необходимо строить на основе свободной и честной конкуренции, прозрачности и верховенства закона, в ноябре 2019 года США и Эстония опубликовали Совместную декларацию о безопасности 5G. Впоследствии обе стороны работали над продвижением этих принципов. Эстония и США предприняли шаги по внедрению решительных мер по повышению безопасности 5G и защите личных и деловых данных.

Кроме того, США и Эстония сотрудничают с другими странами и международными организациями для продвижения своего общего видения безопасного и прозрачного развития цифровых обществ. Обе страны активно выступают за безопасную телекоммуникационную инфраструктуру и кибербезопасность. Признавая важность безопасности в цифровой сфере, страны договорились развивать сотрудничество на двусторонней основе, в региональных форматах, а также в международных организациях.

Крак и Рейнсалу отметили важность использования проверенных поставщиков для обеспечения защиты технологий, данных и интеллектуальной собственности следующего поколения от краж и манипуляций со стороны злоумышленников. Рейнсалу приветствовал инициативу 5G Clean Path Initiative (Чистый путь 5G), анонсированную Майклом Помпео 29 апреля». ***(США и Эстония подтвердили приверженность безопасности телекоммуникационной инфраструктуры // Голос Америки (https://www.golos-ameriki.ru/a/us-estonia-joint-statement/5594812.html). 23.09.2020).***

***

Коронавірус COVID-19 та питання кібербезпеки

«Компания Acronis опубликовала доклад о киберготовности (Acronis Cyber Readiness Report), основанный на опросе специалистов из 3400 транснациональных компаний, а также сотрудников, работающих в

дистанционном режиме из-за пандемии COVID-19. Отчет показывает, что 92% обследованных компаний для обеспечения дистанционной работы используют различные новые технологии, включая инструменты совместной работы и решения для обеспечения конфиденциальности и кибербезопасности.

Как отмечается в документе, значимой проблемой для организаций становится управление защитой на новых устройствах и требует использование целого ряда различных решений, что требует больших затрат, отнимает много времени и характеризуется немалой сложностью. Кроме того, недостаточная интеграция создает слабые места в защите, которые активно используют киберпреступники.

Нацеливаясь на дистанционных работников, хакеры чаще всего используют фишинг, DDoS-атаки и атаки на видеоконференции.

Атаки на видеоконференции за последние три месяца пережили 39% компаний, сотрудники которых использовали приложения типа Zoom, Cisco Webex и Microsoft Teams. Специалисты Cisco недавно обнаружили в своем приложении Webex уязвимость, которая может позволить злоумышленникам получать доступ к потенциально ценному или дискредитирующему контенту.

Количество атак с использованием вредоносного ПО (например, программ-вымогателей) во время пандемии также выросло: представители 31% компаний сообщили о ежедневных кибератаках, а 50% подвергались им как минимум раз в неделю. Большую известность получила кибератака в июле, когда ведущий производитель GPS-технологий по неподтвержденной информации выплатил 10 млн долларов вымогателям, использовавшим программу WastedLocker. Созданные компанией Acronis Операционные центры киберзащиты (Cyber Protection Operating Centers, CPOC) обнаружили, что 35% клиентских оконечных устройств были подвержены атакам с использованием вредоносного ПО, которые начались до внедрения Acronis Cyber Protect.

Фишинговые атаки достигли как никогда высокого уровня, что совершенно не удивительно, так как, по данным рассматриваемого доклада, лишь 2% компаний используют URL-фильтрацию при оценке решений в сфере кибербезопасности. Это упущение делает дистанционных работников уязвимыми к воздействию фишинга – специалисты операционных центров Acronis установили, что в мае, июне и июле на вредоносные сайты заходило примерно 10% пользователей.

Все эти данные, полученные в ходе исследований, проведенных специалистами Acronis и других организаций, наглядно демонстрируют, зачем компаниям нужны новые решения в сфере киберзащиты, снижающие сложность и повышающие безопасность при обеспечении надлежащих условий дистанционной работы, а также не требующие больших затрат и, соответственно, дающие возможность охватить всех дистанционных работников.

«Ландшафт киберугроз очень сильно изменился за последние несколько лет и особенно за последние шесть месяцев. Традиционные автономные антивирусы и решения для резервного копирования неспособны защитить от современных киберугроз, – говорит Сергей Белоусов, основатель, и генеральный директор компании Acronis. – Организации, использующие комплексные системы защиты данных и кибербезопасности не только повышают свою безопасность, но и

снижают расходы и увеличивают эффективность работы. Автоматизация и оптимизированное управление, характерные для Acronis Cyber Protect 15, означают, что любая компания может снизить свои риски, избежать простоев и повысить производительность труда своей IT-команды». ***(Переход на дистанционную работу принес компаниям новые проблемы в сфере защиты // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5690235-Perexod-na-distancionnuyu-rabotu.html). 10.09.2020).***

***

«Пандемия COVID-19 стала катализатором изменений, побуждающих компании тратить больше на технологии, необходимые для поддержания и обеспечения безопасной удаленной работы, даже несмотря на то, что доходы предприятий существенно снизились. Об этом в своем отчете сообщил специалист компании Spiceworks Зифф Дэвис (Ziff Davis), опросивший представителей 1 тыс. предприятий.

76% участников исследования намерены в долгосрочной перспективе внедрять изменения в свои IT-системы из-за пандемии COVID-19. Однако в связи с тем, что из-за снижения доходов организации стремятся сократить свои расходы, увеличение бюджета на IT замедлилось по сравнению с прошлым годом. Только 33% предприятий планируют в 2021 году увеличить расходы на IT, что на 11% меньше по сравнению с прошлым годом. 17% компаний ожидают в следующем году сокращения расходов на IT.

Как и в предыдущих исследованиях, в 2021 году одними из основных факторов роста расходов на IT станут замена устаревшей IT-инфраструктуры и растущие опасения по поводу безопасности. Тем не менее, с учетом того, что больше половины предприятий намерены и впредь продолжать политику гибких графиков работы, необходимость обеспечения возможности безопасной удаленной работы продолжит стимулировать новые расходы.

По словам представителей компаний, планирующих в 2021 году увеличить расходы на IT, на рост бюджета в следующем году будут влиять следующие факторы: повышенный приоритет IT-проектов (45%), изменения в бизнес-операциях во время пандемии COVID-19 (38%) и необходимость поддержки удаленных сотрудников (36%).

Поскольку удаленная работа становится новой нормой, потребности в IT меняются. Как и в предыдущие годы, в 2021 году большая часть всего бюджета на IT будет уходить на оборудование. Но в процентном выражении ожидаемые расходы в этой категории значительно снизились за последние два года (с 35% в 2019 году до 31% в 2021 году) по мере увеличения расходов предприятий на облачные и управляемые услуги.

Хотя предприятия продолжат инвестировать в новые технологии, ожидается, что их внедрение из года в год будет значительно сокращаться, особенно среди представителей малого бизнеса. В свою очередь, это приведет к снижению приоритета передовых технологий в пользу более насущных потребностей, таких как обновление устаревшей инфраструктуры и обеспечение безопасности удаленного доступа. сотрудников.

В течение следующих двух лет крупные предприятия (более 1000 сотрудников) будут внедрять избранные новые технологии в 5 раз быстрее, чем малые предприятия (1-99 сотрудников). Кроме того, крупные предприятия будут внедрять технологии автоматизации IT, виртуальную реальность, периферийные вычисления, контейнеры, 5G и VDI значительно быстрее, чем предприятия малого и среднего бизнеса». ***(Пандемия COVID-19 побудила 76% организаций внедрять изменения в свои IT-системы // SecurityLab.ru (https://www.securitylab.ru/news/512365.php). 22.09.2020).***

***

«Китайские хакеры похитили конфиденциальные данные у испанских исследовательских центров, работающих над созданием вакцины против COVID-19, сообщает испанское издание elpais.com. По данным Национального разведывательного центра Испании (National Intelligence Center, CNI), злоумышленники атаковали не только испанские, но и другие исследовательские организации, занимающиеся разработкой вакцин.

Как сообщили источники elpais.com, большинство кибератак были осуществлены из Китая и РФ. Зачастую за ними стояли спецслужбы, но некоторые атаки были осуществлены университетскими специалистами и киберпреступниками, жаждущими наживы.

За кибератаками на испанские лаборатории стоят хакеры из КНР, сообщили источники, которые, однако, отказались раскрывать характер и актуальность похищенной информации.

Выступая на семинаре, организованном Ассоциацией европейских журналистов, глава CNI Пас Эстебан Лопес сообщила о «качественном и количественном росте» общего числа кибератак в период карантина и отметила, что удаленная работа в период изоляции делает работников более уязвимоыми к online-угрозам…». ***(Китайские хакеры похитили данные у испанских разработчиков вакцины против COVID-19 // SecurityLab.ru (https://www.securitylab.ru/news/512271.php). 18.09.2020).***

***

«Поскольку пандемия затягивается, а удаленная рабочая сила остается удаленной, на первый план должны выйти нулевое доверие и другие извлеченные уроки.

Поскольку штаты имеют дело с повторным открытием и в некоторых случаях повторным закрытием, реальность такова, что для многих организаций удаленная работа будет играть значительную роль в бизнесе до 2020 года и в последующий период. Как и рост активности киберпреступников, о чем свидетельствует рост вирусов на 131 процент и около 600 новых фишинговых атак в день, когда началась пандемия.

Первоначально мы наблюдали ряд фишинговых атак, непосредственно связанных с COVID-19 (в том числе якобы со стороны Центров по контролю и профилактике заболеваний). Позже эти атаки были сосредоточены на пакетах стимулов и страховании от безработицы, а затем переросли в такие темы, как

вакцины и фондовый рынок. Теперь злоумышленники используют самые разные темы - от «стоянок» до аренды лодок и доставки еды. И они не просто используют электронную почту для этих попыток - онлайн-реклама и мобильные приложения - это всего лишь пара других используемых тактик.

Даже если организации создали более гибкие политики удаленной работы, чтобы лучше удовлетворять потребности своих сотрудников в краткосрочной перспективе, эти предприятия должны гарантировать, что их стратегии удаленной работы могут поддерживать и обеспечивать безопасность удаленного подключения в долгосрочной перспективе.

Ясность из кризиса

Из-за пандемии руководители по информационным технологиям сначала столкнулись с невероятной нагрузкой, связанной с поддержанием непрерывности бизнеса: почти 100 процентов сотрудников всего за пару дней перешли на работу из дома. Многие успешные подходы, которые мы видели для этого, основаны на тщательном анализе существующих возможностей, поэтому вместо того, чтобы спешить с добавлением новых технологий, они использовали потенциал уже имеющихся решений. Прелесть оценки того, что у вас есть в свете этих бизнес-императивов, заключается в том, что вы в конечном итоге задаете правильные вопросы о том, какие процессы, данные и приложения на самом деле важны для поддержания бизнеса.

Этот здоровый ответ на кризис вызвал некоторое «Ага!» моменты и, как следствие, единые методы обеспечения безопасности в филиалах (т. е. в основной и облачной инфраструктурах). Многие организации просто не знали о некоторых слабых местах и узких местах в своей инфраструктуре. Многие знали, что фишинговые электронные письма представляют собой угрозу, но они, возможно, не ожидали, что корпоративные ноутбуки окажутся в опасности, если кто-то из их семьи щелкнет ссылку во время чата или игры в онлайн-игры. Чтобы решить эти проблемы, когда они стали очевидными, некоторые компании внесли изменения и дополнения в свою среду таким образом и с такой скоростью, которые сделали невозможным понимание последующих эффектов.

Совершая переход

Хотя поначалу это могло показаться сложным, по крайней мере, с технической точки зрения, реализация надежной и безопасной программы для удаленных сотрудников не обязательно была такой сложной, как думали многие организации. Однако для этого требовались правильная политика и открытость, чтобы принять изменения, чтобы все это было эффективно и в сжатые сроки.

Некоторые организации использовали общие подходы к VPN, в то время как другие организации создают надежные и масштабируемые облачные решения, решения для SD-WAN и управления доступом к сети (NAC). Масштабирование решений стало проще, когда у предприятий с самого начала уже была правильная инфраструктура. При тщательном планировании и правильном технологическом партнерстве некоторые организации смогли преодолеть препятствие и реализовать или расширить свою стратегию удаленной работы.

В дальнейшем удаленная работа может стать более важной частью корпоративных стратегий. Опыт пандемии заставил предприятия понять, что

причины для сохранения или возможного расширения их стратегий удаленной работы быстро превзошли числом причины против того, чтобы удаленная работа стала стандартной частью бизнес-процесса организации в будущем.

Извлеченные уроки и следующие шаги

В той или иной степени удаленная работа никуда не денется. Опрос 317 финансовых директоров и финансовых руководителей, проведенный Gartner в конце марта, показал, что 74% переместят не менее 5% ранее находившихся на работе сотрудников на постоянно удаленные должности после COVID 19. И почти 25% респондентов заявили, что они перейдут как минимум на другую работу. 20 процентов своих сотрудников на постоянных удаленных должностях.

Следовательно, доступ к сети с нулевым доверием будет приобретать все большее значение. В настоящее время этой концепции уделяется большое внимание, поскольку компании признают, что, во-первых, у них есть множество туннелей VPN, которые должны понимать и подтверждать, кто является пользователями; и, во-вторых, у них есть пользователи на всех типах устройств, которые теперь имеют доступ к корпоративной сети. Организации будут обращать внимание на своих поставщиков средств обеспечения безопасности и OEM-производителей, чтобы реализовать лучшие функции нулевого доверия таким образом, чтобы это было управляемо и повышалось общее состояние безопасности организации. Есть основания полагать, что организации будут применять разные стратегии нулевого доверия для разных частей своего бизнеса, таких как облачные, удаленные и центры обработки данных.

Именно здесь способность понимать и видеть все в сети становится критически важной. Имея за плечами несколько месяцев удаленной работы, организации могут сделать шаг назад и оценить, принимают ли они все необходимые меры безопасности, чтобы их решения для удаленной работы были эффективными в долгосрочной перспективе. В результате многие из них укрепляют свои возможности нулевого доверия, чтобы в будущем точно знать, кто и что находится в их сети, поскольку сотрудники продолжают работать удаленно.

Еще одним результатом является то, что потребность в более тесно интегрированных функциях сети и безопасности будет расти. Сетевая инфраструктура должна поддерживать и задействовать другие аспекты бизнеса. Он должен допускать динамические изменения и интеграцию новых технологий, а также должен иметь интегрированные и автоматизированные функции безопасности для уменьшения сложности и повышения эффективности. Это должно распространяться от филиала к периферии и от центра обработки данных к облаку, с единой политикой и централизованной видимостью и управлением.

Теперь, когда предприятия быстро признают, что облако является продолжением центра обработки данных, для политик сети и безопасности становится критически важным беспрепятственное расширение в этих средах и сохранение той же простоты развертывания (и уровня безопасности), что и их более традиционные физические аналоги.

Долгосрочная перспектива

По мере развития пандемии становится все более очевидным, что удаленная работа - это не просто временное решение. За последние несколько месяцев мы

стали свидетелями резкого сдвига как в способности бизнес-сообщества адаптироваться, так и в киберпреступном сообществе, которое следует тенденциям по увеличению циклов атак. Видимость сети и возможности нулевого доверия становятся ключевыми для непрерывной безопасной удаленной работы. Короче говоря, пандемия привела к необходимости гибкости как в обеспечении непрерывности бизнеса, так и в сетевой инфраструктуре; пусть эти уроки будут учтены по мере нашего продвижения вперед». ***(Aamir Lakhani. Security Takeaways from the Great Work-from-Home Experiment // Threatpost (https://threatpost.com/security-takeaways-work-from-home/159358/). 18.09.2020).***

***

«В отчете Cynet содержится несколько интересных данных и выводов, таких как изменение объема кибератак, наблюдаемое в различных отраслях промышленности, более широкое использование целевого фишинга в качестве исходного вектора атаки и подходы, используемые для распространения вредоносных программ в целевых фишинговых атаках.

Большинство профессионалов в области кибербезопасности полностью ожидали, что киберпреступники будут использовать страх и замешательство, окружающие пандемию COVID-19, в своих кибератаках. Конечно, вредоносные электронные письма будут содержать темы, касающиеся COVID-19. Конечно, вредоносные загрузки могут быть связаны с COVID-19. Так действуют киберпреступники. Любая возможность максимизировать эффективность, какой бы ничтожной она ни была, используется.

Хотя многие из них неофициально предлагали варианты развития кибератак, связанных с COVID-19, у нас мало данных, подтверждающих фактическое влияние COVID-19 на кибербезопасность. Некоторые сообщили, что количество вредоносных писем, связанных с Covid-19, выросло на несколько сотен процентов и что большинство писем, связанных с COVID-19, теперь являются вредоносными.

Помимо ожидаемого увеличения количества вредоносных электронных писем, видео и множества загружаемых файлов, связанных с COVID-19, чего мы все ожидали, что еще происходит за кулисами?

Интересно, что компания Cynet, занимающаяся кибербезопасностью, только что выпустила отчет (скачать здесь), в котором подробно описаны изменения в кибератаках, которые они наблюдали в Северной Америке и Европе с начала пандемии COVID-19. В отчете содержится ряд интересных данных и выводов, таких как изменение объема кибератак, наблюдаемое в различных отраслях промышленности, более широкое использование целевого фишинга в качестве исходного вектора атаки и подходы, используемые для распространения вредоносных программ в целевых фишинговых атаках.

Далее следуют два более интересных вывода.

Борьба с огнем с помощью огня

Cynet обнаружила, что киберпреступники не просто «в какой-то мере» используют пандемию COVID-19, они идут ва-банк. Киберпреступники используют весь свой арсенал новых методов атаки, чтобы обеспечить успех атаки.

Это похоже на то, что спортивная команда использует все новые приемы, которые они разработали в одной игре, а не распределяет их по сезону.

В отчете указывается, что процент атак с использованием новых методов исторически составлял около 20%. То есть в 80% атак использовались хорошо известные методы, которые легко идентифицировать, если компании обновили превентивные меры.

Cynet обнаружила, что с начала пандемии COVID-19 количество новых атак увеличилось примерно до 35% от всех атак. Новые методы атак не могут быть в достаточной степени обнаружены одним антивирусным программным обеспечением и могут быть эффективно обнаружены только с использованием новых механизмов обнаружения поведения. То есть необходимо использовать новые подходы к обнаружению, чтобы обнаружить применяемые новые методы атак.

Перегруженные сотрудники службы безопасности

Еще одно интересное наблюдение в отчете Cynet - это огромный всплеск количества клиентов, запрашивающих экспертную помощь от своей группы обнаружения и реагирования (которую Cynet называет CyOps). Во время пандемии взаимодействие с клиентами увеличилось на 250%. Помимо использования передовых механизмов обнаружения и реагирования, необходимы глубокие навыки кибербезопасности как для обнаружения, так и для смягчения резкого роста новых методов атак, развернутых во время пандемии COVID-19.

Лечение?

К сожалению, многие компании еще не имеют передовых технологий обнаружения и реагирования, таких как расширенное обнаружение и реагирование (XDR), или постоянного доступа к круглосуточной группе управляемого обнаружения и реагирования (MDR). Когда кибератаки с использованием новых методов резко увеличиваются, как это происходит во время этой пандемии (или могут случиться в любое время), компании без этих передовых средств защиты подвергаются более высокому риску. Мы настоятельно рекомендуем изучить решения XDR и MDR как способ защиты и иммунизации вашего стека кибербезопасности в будущем.

И независимо от того, какой стек безопасности вы развернули, остерегайтесь новых атак вредоносного ПО. Используйте методы поиска угроз, чтобы прочесать свои системы, чтобы убедиться, что новые вредоносные программы не проскользнули сквозь трещины. Рост числа новых вредоносных программ означает, что их предотвращение и обнаружение становятся более сложными, и постоянный поиск угроз должен стать нормой». ***(Report Looks at COVID-19's Massive Impact on Cybersecurity // Threatpost (https://threatpost.com/cynet-report-looks-at-covid-19s-massive-impact-on-cybersecurity/159249/). 16.09.2020).***

***

«По оценкам перестраховщика из Германии Munich Re, в течение ближайших пяти лет стоимость глобального рынка страхования кибернетических рисков возрастет в три раза и достигнет $20 млрд.

Как сообщает интернет ресурс УкрСтрахование со ссылкой на отчет Munich Re, доля рынка киберстрахования, приходящаяся на Munich Re в 2025 году достигнет 10%.

«Киберрынок может вырасти даже сильнее, чем ожидалось, перед лицом дополнительного импульса от цифровизации», — отметил главный андеррайтер Munich Re Штефан Голлинг. По его словам, в компании работает профессиональная команда из более чем 130 экспертов, готовых разрабатывать «кибер-решения для всей цепочки создания стоимости, от анализа и предотвращения рисков до передачи рисков. Кроме того, у нас есть постоянно растущая сеть внешних экспертов и партнеров, предлагающих услуги до и после кибератаки»…». ***(К 2025 году рынок кибернетического страхования увеличится втрое и достигнет $20 млрд // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/k-2025-godu-rynok-kiberneticheskogo-strahovaniya-uvelichitsya-vtroe-i-dostignet-20-mlrd). 08.09.2020).***

***

«По прогнозам Gartner, по мере сближения ИТ-систем, Интернета вещей и операционных технологий атаки на киберфизические системы в промышленных, медицинских и других сценариях будут иметь ужасные последствия.

К 2024 году 75 процентов высшего руководства компаний будут лично подвергнуты риску инцидентов в области кибер-физической безопасности (CSP), особенно тех, которые связаны со смертельным исходом.

Это согласно исследовательской фирме Gartner, которая на этой неделе предсказала, что генеральные директора вскоре больше не смогут прятаться за своими корпоративными юридическими командами, если что-то пойдет не так.

Gartner определяет CPS как «системы, которые спроектированы для координации измерений, вычислений, управления, сетей и аналитики для взаимодействия с физическим миром (включая людей)». Последствия для безопасности таких систем возросли по мере того, как ИТ-системы, IoT и операционные технологии (OT), управляющие физическими системами, продолжают сближаться. К физическим системам, которые ранее были разделены или изолированы, теперь можно получить доступ через взломанную ИТ-сеть или конечную точку IoT. В то же время многие компании не знают, что у них есть системы OT, подключенные к корпоративным сетям; или, возможно, они не соблюдают надлежащую сегментацию сети или другие меры предосторожности.

В настоящее время эти конвергенции в основном встречаются в критически важной инфраструктуре и клинических медицинских учреждениях, но они получат более широкое распространение с расширением 5G, а также в качестве инноваций в мире интеллектуальных зданий, умных городов, подключенных автомобилей и

автономных транспортных средств, а также телемедицины / удаленного управления. В компании отметили, что операции продолжают развиваться.

В таких условиях «инциденты могут быстро привести к физическому ущербу для людей, разрушению имущества или экологическим катастрофам», - заявляет компания. «Аналитики Gartner прогнозируют, что в ближайшие годы количество инцидентов будет быстро расти из-за недостаточного внимания к безопасности и расходов, которые в настоящее время соответствуют этим активам».

Gartner также прогнозирует, что финансовое воздействие CPS-атак, приводящих к смертельному исходу, к 2023 году достигнет более 50 миллиардов долларов. Сюда входят расходы организаций с точки зрения компенсации за гибель людей, судебные тяжбы, страхование, нормативные штрафы и потерю репутации.

«Регулирующие органы и правительства незамедлительно отреагируют на рост серьезных инцидентов, возникающих в результате неспособности обеспечить безопасность CPS, и резко ужесточат правила и нормы, регулирующие их», - заявила Кателл Тилеманн, вице-президент Gartner по исследованиям, в заявлении для СМИ. «В США ФБР, АНБ и Агентство по кибербезопасности и безопасности инфраструктуры (CISA) уже увеличили частоту предоставления подробных сведений об угрозах критически важным системам, связанным с инфраструктурой, большинство из которых принадлежит частной отрасли. Вскоре руководители не смогут ссылаться на незнание или отступать за страховые полисы».

В июле, например, ICS-CERT выпустил уведомление о критической ошибке безопасности в Schneider Electric Triconex TriStation и модуле связи Tricon. Эти контроллеры инструментальных систем безопасности (SIS) несут ответственность за остановку работы станции в случае возникновения проблемы и действуют как автоматическая защита безопасности промышленных объектов, предназначенная для предотвращения отказа оборудования и катастрофических инцидентов, таких как взрывы или пожары. В прошлом они подвергались атаке TRITON в 2017 году.

Таким образом, в компании отметили, что акцент на кибербезопасности в пространстве CSP имеет решающее значение в будущем. Непомерно высокая стоимость в долларах и репутация киберфизических жертв для организаций приведут к усилению внимания к OT и CPS. Руководители высшего звена и члены совета директоров потребуют большей прозрачности и контроля за состоянием безопасности CPS организации, и Gartner сообщил Threatpost, что ожидает, что относительно молодой рынок средств безопасности для OT резко вырастет с 250 миллионов долларов в 2018 году до 1,115 миллиарда долларов в следующем году. CAGR 45,7 процента.

«Крайне необходимо сосредоточить внимание на ORM - или управлении операционной устойчивостью - помимо кибербезопасности, ориентированной на информацию», - сказал Тилеманн.

Что касается передовой практики, Gartner рекомендовала организациям сначала идентифицировать все подключенные активы в организации, независимо от того, считаются ли они ИТ-оборудованием, оборудованием OT, системами управления зданием, интеллектуальными устройствами или любым другим типом (беспроводным) подключенным устройством. Затем им следует скорректировать используемые в настоящее время методы оценки рисков, чтобы определить

вероятность и влияние событий, влияющих на безопасность человека и окружающую среду. После этого они могут разработать метод классификации, который учитывает физические аспекты данных и систем, а не просто схему классификации данных; а затем разверните информационную кампанию, чтобы убедиться, что все заинтересованные стороны как внутри, так и за пределами организации осведомлены о киберфизических рисках, исходящих от подключенных систем в организации…». ***(Tara Seals. CEOs Could Be Held Personally Liable for Cyberattacks that Kill // Threatpost (https://threatpost.com/ceos-personally-liable-cyberattacks-kill/158990/). 07.09.2020).***

***

«Во втором квартале 2020 года доход мирового рынка решений в области информационной безопасности вырос в годовом выражении на 7,5%, достигнув отметки в $4,2 млрд, Также на 8% возросли поставки устройств, составив 1,1 млн единиц. Такие данные приводятся в отчете компании IDC.

Согласно отчету, продажи UTM-решений в апреле-июне 2020 года повысились на 10,7% в годовом исчислении и составили 61,8% в общем объеме рынка. Кроме того, продолжает расти спрос на продукты по обеспечению web-безопасности, демонстрируя рост в 10% в годовом выражении, а вот продажи решений по обнаружению и предотвращению вторжений (IDS и IPS) снизились на 6,2% и 5,1% соответственно.

«Несмотря на продолжающуюся пандемию, продажи устройств для сетевой безопасности продемонстрировали значительный рост на 10% во втором квартале 2020 года в отличие от спада в первом квартале 2020 года. Это связано с увеличением расходов на расширение удаленной работы и обеспечение локальных ресурсов», - отметил старший аналитик компании IDC Пит Финалл (Pete Finalle).

По данным IDC, на долю США пришлось 44,3% продаж ИБ-решений во втором квартале 2020 года против 42,7% годом ранее. В Центральной и Восточной Европе продажи таких продуктов поднялись на 7,2% в сравнении от года к году, в Западной Европе наблюдался рост продаж на 5,5%, в Канаде и Латинской Америке - на 5,4% и 4,6% соответственно. Единственным регионом продемонстрировавшим спад продаж оказался Китай (на 3%).

Исследование также приводит рейтинг компаний, занявших первые строчки в списке поставщиков ИБ-оборудования. На первом месте оказалась компания Palo Alto Networks, заработавшая на продаже ИБ-решений $759,4 млн по итогам второго квартала 2020 года (рыночная доля 18,1%), второе место заняла компания Cisco с рыночной долей в 17%, замыкают пятерку лидеров компании Fortinet (12,7%), Check Point (10%) и SonicWALL (3,9%)». ***(На фоне пандемии вырос спрос на решения для обеспечения сетевой безопасности // SecurityLab.ru (https://www.securitylab.ru/news/511770.php). 07.09.2020).***

***

«По мнению двух третей жителей стран западной Европы, добавление в тело человека цифровых технологий поможет улучшить жизнь, в том числе,

здоровье. К такому выводу пришли специалисты «Лаборатории Касперского» по результатам исследования, проведенного по их заказу компанией Opinium Research.

В ходе исследования были опрошены 14,5 тыс. жителей 16 стран, в том числе Великобритании, Германии, Франции, Италии и Испании. Как показал опрос, 63% из них готовы усовершенствовать свои тела с помощью технологий.

Больше всего людей, готовых стать киборгами, в Испании и Португалии – более 60%. А вот британцы, французы и швейцарцы настроены не столь решительно – 25%, 32% и 36% соответственно.

«На сегодняшний день улучшение человека является одной из самых значительных технологических тенденций. Энтузиасты улучшения уже проверяют пределы возможного, но нам нужны общепринятые стандарты, гарантирующие, что оно полностью раскрывает свой потенциал при сведенных к минимуму рисках», – цитирует Reuters европейского директора глобальных исследований и аналитики ЛК Марко Пройса (Marco Preuss).

В прошлом месяце принадлежащий Илону Маску стартап Neuralink продемонстрировал первые шаги по внедрению компьютерных чипов в мозг – явил миру свинью по кличке Гертруда, в мозг которой в течение двух месяцев был вживлен чип размером с монету.

Как показало исследование Opinium Research, большинство опрошенных хотели бы, чтобы улучшение человека любое работало только во благо человечества. Тем не менее, некоторые респонденты выразили опасения по поводу возможной эксплуатации чипов хакерами. Кроме того, по мнению большинства опрошенных, только состоятельные люди смогут получить доступ к технологиям улучшения человека…». ***(Европейцы готовы стать киборгами // SecurityLab.ru (https://www.securitylab.ru/news/512259.php). 18.09.2020).***

***

«Кибербезопасность – большая часть информационных технологий. Она направлена на защиту цифровых данных бизнеса от утечек, а также на сохранение работоспособности инфраструктуры.

На рынке таких услуг действует много игроков. Сам рынок растет двузначными темпами год к году и видится интересной инвестиционной возможностью. В статье рассмотрим:

- рынок и его сегменты;
- тенденции на рынке;
- отдельных игроков и их финансовые результаты.

Кибербезопасность – это про защиту данных и про устойчивость цифровой инфраструктуры

На сегодняшний день все – от небольших стартапов до холдингов и транснациональных корпораций – держат свои данные в цифровом виде.

Компании хранят информацию, которая имеет большую ценность, а в руках сторонних лиц может стать потерей конкурентного преимущества или вовсе навредить бизнесу. В цифровых данных может содержаться:

- интеллектуальная собственность (инновационные разработки, конструкторские решения и др.);

- данные о клиентах и поставщиках;
- планы/наработки по стратегиям расширения бизнеса;
- данные по приобретению других бизнесов и др.

Из-за их ценности за этими данными ведется охота подготовленными людьми — хакерами.

Кибербезопасность призвана ставить защиты там, где это возможно, и предотвращать утечку коммерчески чувствительной информации для сохранения своих конкурентных преимуществ.

Другими словами, кибербезопасность — это сфера предоставления сервисных услуг по цифровой защите данных.

Также, сервисы в области компьютерной защиты предотвращают выведение из строя серверов компаний и других цифровых хранилищ и поддерживают устойчивость сообщения между бизнес-юнитами, цепями поставок и т.д.

Размер рынка — около $185 млрд, и он постоянно растет

Существует много обзоров на рынок компьютерной безопасности. Оценки размеров и темпов роста значительно разнятся. Мы консервативно используем усредненные значения.

На конец 2018 г. объем рынка кибербезопасности оценивали в 152$ млрд со среднегодовым ростом в 10,5%. Соответственно, на данный момент рынок компьютерной безопасности составляет ~$180-190 млрд.

При сохранении текущих темпов роста к 2025 г. рынок вырастет выше $300 млрд.

Сегменты рынка компьютерной безопасности

Условно рынок можно разделить на несколько частей:

Цифровая защита (защита аккаунтов, виртуальных хранилищ, внутренней системы связи и др.);

Поддержка работоспособности серверов и физических хранилищ данных + коммуникационных элементов;

Прочие услуги…

Актуальные тренды на рынке кибербезопасности

На рынке существуют несколько тенденций, которые двигают рынок вперед в объемах.

Развитие программного обеспечения (софта) в области машинного обучения и искусственного интеллекта способствует совершенствованию информационных технологий. Это значит, что новые инструменты получают как "кибербезопасники", так и киберпреступники. В совокупности, автоматизация атак и расширение спектра действий злоумышленников действует на развитие новых направлений в компьютерной защите.

Также, развитие облачных технологий создает большой спрос на защиту этих данных. Соответственно, развитие рынка вокруг софта облачных сервисов будет порождать спрос на защиту информации в них.

На сегодняшний день существенно растет объем кибератак на мобильные устройства. С развитием технологий интернет-вещей (IoT) все чаще и чаще объектами для атак становятся также и другие персональные девайсы. Поэтому

важным трендом является защита мобильных устройств, их программных обеспечений и др.

Мобильные устройства становятся главным приоритетом в списке вероятных угроз для атак

В пандемию рост фишинговых атак превысил 660% г/г! Эти атаки направлены на установку вредоносного программного обеспечения на девайсы предполагаемой жертвы кибератаки для управления ее данными. Атаки проводятся так, что компьютер жертвы не распознает инородный софт и не дает сигналов владельцу об утечке. С этим сейчас стали бороться еще ожесточеннее. К примеру, Microsoft (NASDAQ:MSFT) делает свой продукт Office 365 адаптивным и устойчивым к таким атакам.

Внедрение искусственного интеллекта и блокчейн-технологий также является важным трендом в кибербезопасности. С их помощью можно предотвращать DDoS- и DoS-атаки на хранилища данных компаний.

Ожидается, что большое развитие получит азиатский рынок кибербезопасности из-за постепенного оформления там заинтересованных кругов в защите своей коммерческой информации и интеллектуальной собственности. Этому также будет способствовать развитие правового поля в рамках макротенденции улучшения инвестиционного климата азиатских стран.

Однако наряду с драйверами есть и «тормозы» рынка. Одним из рисков роста рынка является сокращение бюджетов компаний из-за влияния пандемии COVID-19. При сохранении слабой экономической обстановки низкие бюджеты могут стать краткосрочно-среднесрочной реальностью…

Топ-7 компаний на рынке кибербезопасности:

Cisco Systems Inc (NASDAQ:CSCO) ~9% (около постоянной планки);

Palo Alto Networks Inc (NYSE:PANW) ~7,8 (доля постепенно растет);

Fortinet Inc (NASDAQ:FTNT) ~5,5% (около постоянной планки);

Check Point Software Technologies Ltd (NASDAQ:CHKP) ~5,5% (доля постепенно снижается);

Semantec ~5%;

IBM (NYSE:IBM) ~4,5%;

McAfee (Intel Security) ~4%...

Резюме

Рынок кибребезопасности – это широкий спектр услуг по защите цифровых данных и предотвращению атак на физические хранилища данных. Рынок растет со средним темпом 11% и, вероятно, продолжит расти.

На рынке существует спрос на услуги IT-компаний в области безопасности, т.к. объемы атак злоумышленников только возрастают. Для удовлетворения этого спроса собрались игроки, которые имеют устойчивые фин. показатели и прогнозируют в рост своего бизнеса в будущем.

Мы считаем, что рынок кибербезопасности – это интересная возможность для инвестиций. Palo Alto Networks и компанию Okta видим как лидеров по темпам роста фин. показателей и бизнеса». ***(Сергей Пирогов. Рынок кибербезопасности растет двузначными темпами // Investing.com (https://ru.investing.com/analysis/article-200273805). 17.09.2020).***

***

«Новая цифровая парадигма для бизнеса — Индустрия X.0 — вместе с идеологией постоянных технологических изменений несет в себе и новые риски. Рассказываем об особенностях киберзащиты бизнеса, оперирующего в рамках Индустрии X.0.

Индустрия X.0 — цифровое переосмысление развития предприятия, использующее передовые технологии для преобразования основной деятельности, труда сотрудников и путей взаимодействия с клиентами.

Конечная цель этого подхода — трансформация бизнес-модели через достижение новых уровней эффективности разработок, инжиниринга, производства и поддержки с помощью новых взрывных технологий, таких как промышленный интернет вещей, роботизация, машинное обучение, искусственный интеллект, компьютерное зрение, AR/VR, блокчейн, большие данные, облака. Важным и неотъемлемым элементом Индустрии X.0 является кибербезопасность.

Несмотря на преимущества и новый горизонт возможностей развития бизнеса, усовершенствованная операционная модель несет в себе и дополнительные уязвимости, увеличивая пригодную для кибератак «площадь» ИТ-систем. Неспособность адекватно инвестировать в безопасность в нужных областях может привести к тому, что весь бизнес окажется под угрозой. Даже изначально закрытые промышленные ИТ-системы, которые не были предназначены для подключения к интернету, с наступлением эры всеобщей сетевой связанности стали доступны для удаленной атаки из любой точки мира в любое время.

«Цифровая трансформация несет промышленным предприятиям новые риски в сфере ИБ, — говорит Евгений Артюхин, директор департамента информационной безопасности, компания Biocad. — К ним относятся риски, которые не связаны с прямыми атаками на предприятие, но которые при этом могут нанести значительный ущерб, как репутационный, так и финансовый. Например, это угрозы для телекоммуникационного сектора, которые влекут за собой нарушения работоспособности сети Интернет. Кроме того, можно отметить участившиеся атаки на регистраторов доменных имен и, конечно, атаки на локальные системы фильтрации и блокировки трафика. В целом, можно сказать, что мотивация киберпреступников и кибергруппировок меняется стремительно, это затрудняет своевременную адаптацию систем защиты информации, однако, не отменяет такой необходимости».

«Нельзя обойти вниманием и пандемию COVID-19, которая повлекла за собой существенные изменения. Многие предприятия вышли если не на удаленный режим работы, то на смешанный, — продолжает Евгений Артюхин. — В связи этим для предприятий возросла необходимость расширять корпоративную сеть передачи данных и прорабатывать вопросы защиты пользователей не только в периметре предприятия, но и за его пределами, чтобы обеспечить максимальную защиту информационных активов. Отсюда возникает потребность предприятий во внедрении дополнительных средств защиты информации, дополнительных систем мониторинга, а также в более тонких настройках систем реагирования на инциденты ИБ».

Защита на уровне

Кибербезопасность в среде Индустрии Х.0 — это не просто абстрактная технологическая проблема, она разделяется на несколько вполне конкретных уровней.

Первый — физический. Устройства промышленного интернета вещей (датчики) часто устанавливаются в удаленных местах, которые могут находиться за пределами контроля оператора, поэтому важно учитывать их физическую безопасность. Она может реализовываться простыми методами в виде запираемых на замок шкафов с оборудованием, а может усиливаться за счет интеграции цифровых механизмов безопасности, таких как системы сигнализации на панели управления, которые сообщают о несанкционированном доступе, или видеонаблюдение с распознаванием лиц.

«Система информационной безопасности как живой организм, постоянно меняется в зависимости от внутренних и внешних факторов. Этим факторами являются изменения конъюнктуры рынка, изменения в требованиях законодательства РФ. Поэтому очень важно своевременно заметить эти изменения и в короткий срок отреагировать и перестроить систему информационной безопасности, — говорит Анатолий Маслов, директор по организационному развитию металлургического холдинга «Новосталь-М». — Появление Индустрии Х.0 не только расширит доступное злоумышленникам поле для маневра, но и сделает ущерб от кибератак более значимым для операционной деятельности Предприятия, из-за чего стоимость ущерба вырастет в абсолютных значениях».

Второй уровень — человеческий фактор. Любая кибербезопасность сильна настолько, насколько сильно ее самое слабое звено — человек. Хакеры научились использовать методы социальной инженерии, чтобы получать информацию от сотрудников, подрядчиков, заказчиков и других пользователей ИТ-систем предприятия. Злоумышленники эксплуатируют некомпетентных в области ИБ сотрудников, например, использующих один и тот же пароль для рабочих и личных аккаунтов.

Третий уровень — организационный. В прошлом защита промышленных процессов регулировалась различными командами и группами внутри организации. ИТ-безопасность в их ведение не включалась. В итоге сегодня на предприятиях, как правило, отсутствует комплексный подход к защите процессов и инфраструктуры, сочетающий практики кибербезопасности, обеспечения надежности систем и физической защиты.

Четвертый уровень — технологический. С одной стороны, более интеллектуальные технологии способны сдерживать, предотвращать и обнаруживать кибервторжения. С другой — киберугрозы тоже становятся «умнее и сложнее». Существующие технологические архитектуры и старые системы, которые были безопасны и надежны в течение многих лет, теперь могут обеспечить почти беспроблемный вход для хакеров в производственные системы компании.

При обеспечении кибербезопасности Предприятия Х.0, по мнению Анатолия Маслова, необходимо уделять равное внимание как операционной составляющей процесса (создавать продуманные реализации бизнес-процессов, составлять описания зон ответственности подразделений и каждого работника предприятия),

так и технологической, которая управлять призвана ликвидировать уязвимости систем, закрывать бреши в системе зашиты Предприятия.

«Случаи со Spectre и Meltdown иллюстрируют проблему ярче всего: 27 уязвимостей, которые были обнаружены в архитектурах процессоров AMD, ARM и Intel, использующихся в миллионах машин по всему миру. Они дают злоумышленникам дополнительные возможности по установлению контроля над практически каждым устройством, включая ноутбуки, мобильные устройства и промышленные системы, повышая риски их эксплуатации на порядок. Это аппаратные уязвимости и программными патчами их так просто не исправить», — отмечает серьезность вызовов руководитель практики информационной безопасности компании Accenture в России Андрей Тимошенко.

Тактика обороны в эпоху Индустрии X.0

Трудно добиться надлежащего уровня кибербезопасности, когда нарушения ИБ-периметра остаются незамеченными.

Поэтому первое, что необходимо сделать — повысить внутреннюю прозрачность ИТ-систем для понимания текущей ситуации. Это реализуется с помощью комплексного операционного, ИТ/ИБ и физического мониторинга критической инфраструктуры. Информация по всем этим направлениям должна стекаться в единый ситуационный центр мониторинга для совместного использования, корреляции и управления на комплексной основе в рамках всей организации.

По большому счету безопасность Индустрии X.0 — это вопрос интеграции ИТ и ОТ (операционных технологий) на современном уровне. Это подразумевает создание интегрированной системы безопасности ИТ-инфраструктуры как в ее локальной, так и облачной составляющей для защиты управления доступом и безопасности приложений.

Если разбить шаги по укреплению кибербезопасности в рамках парадигмы Индустрии X.0 на блоки в порядке срочности, то в раздел «реализовать немедленно» попадут:

- формирование единого органа управления безопасностью ИТ/ОТ;
- организация тренингов и повышение осведомленности персонала в вопросах ИБ;
- инвентаризация, классификация и категорирование ОТ-активов, включая оборудование, процессы, ПО, сети, людей и взаимосвязи;
- определение требований ИБ к различным категориям ОТ-активов;
- внедрение быстрых и практических мер защиты ОТ в соответствии с приоритетами;
- мониторинг рисков в соответствии с определенной методологией и измерение эффективности мер ИБ.

Цель — получить интегрированный Security Operations Center, охватывающий облачную и локальную ИТ-инфраструктуру, а также сферу операционных технологий, генерирующий продвинутую аналитику по безопасности с использованием Threat Intelligence — подхода к выявлению новых и наиболее актуальных киберугроз на базе реальных кейсов и отслеживания релизов новых типов угроз в реальном времени.

Главным отличием промышленного предприятия является необходимость обеспечивать безопасность автоматизированных систем управления технологическим процессом, уязвимость которых может повлечь за собой нарушения технологического процесса, считает Евгений Артюхин. Также он указывает, что нельзя забывать о работе с персоналом, причем речь не только об офисных сотрудниках. Необходимо повышение осведомленности работников в вопросах информационной безопасности, это поможет предприятию быть устойчивыми к атакам методами социальной инженерии, не только с использованием корпоративной техники, но и таргетированных атак через социальные сети.

Больше метрик

Главные ключи к успеху в ИБ для Индустрии Х.0 — превентивная оценка рисков и приоритет на безопасности в работе руководителей всех ключевых подразделений предприятия. Эти два аспекта следует «включать» от самых ранних стадий инсталляции любых технологических решений до окончания срока службы или вывода из эксплуатации.

Организациям необходимо применять подход «безопасность на уровне архитектуры», включающий анализ рисков и механизмы обеспечения безопасности конвергентных архитектур ИТ и ОТ. Для этого следует добавить метрики безопасности в аналитику.

Журнал событий межсетевых экранов и систем управления доступом, управление изменениями настроек ИТ платформ и средств защиты, статистика инцидентов и системы управления событиями ИБ (SIEM) могут помочь в совершенствовании этой работы.

Например, ошибки конфигурации могут привести к уязвимостям и киберинцидентам и вызвать простои. Добавление метрик и индикаторов (риска, компрометации) позволяет организациям отслеживать угрозы и действовать гибко и проактивно, чтобы различать операционные или кибер-проблемы. Это сократит время отклика и восстановления после сбоя в работе корпоративных и производственных систем или процессов.

Еще один важный момент — плотное сотрудничество с заинтересованными сторонами экосистемы Индустрии Х.0 (поставщики, клиенты, регуляторы, ИТ/ИБ вендоры), для оптимального понимания, какие показатели и меры безопасности наиболее полезны в данный период.

Внимание — людям, «физике», ИИ

Обучение и осведомленность сотрудников об угрозах ИБ должны быть встроены в любое управление безопасностью и быть доступным на постоянной основе.

В интервью с 4600 руководителями служб безопасности 71% респондентов указал, что кибератаки «все еще являются теневой областью; мы не совсем понимаем, как и когда они повлияют на нашу организацию».

Когда речь заходит о Индустрии Х.0, зачастую мало внимания уделяется тому, какую информацию могут получить хакеры или какие изменения они могут внести, если получат доступ к внутренней электронике: программируемым логическим контроллерам, блокам удаленных терминалов или датчикам.

Эффективность основных мер физической безопасности, таких как дверные замки, камеры наблюдения или системы контроля доступа, может быть повышена путем интеграции цифровой безопасности с обычными методами. Например, интеграция потоков видео с обычных камер видеонаблюдения с видеоаналитикой позволит обнаружить аномальное перемещение товаров, оборудования, людей и т.д.

Стратегии превентивной кибербезопасности, основанные на возможностях ИИ, также могут снизить подверженность возникающим угрозам. В то время как аналитика и машинное обучение могут использоваться для обнаружения аномалий, искусственный интеллект, оркестрация и автоматизация могут применяться для улучшения корреляции работы различных систем, ускорения обнаружения угроз и многократного сокращения времени реагирования». ***(Григорий Васюков. Кибербезопасность: как защитить предприятие в эпоху Индустрии X.0 // CNews (https://safe.cnews.ru/articles/2020-09-24_kiberbezopasnost_kak_zashchitit). 24 09.2020).***

***

«Компании по всему миру знают о киберугрозах больше, чем когда-либо. Но, по данным исследования, это не гарантирует максимальный уровень безопасности. Слабым звеном становятся сотрудники организаций, которые не понимают, как противостоять атакам и что делать в случае их возникновения.

В компаниях по всему миру признались в неготовности противостоять киберугрозам

Несмотря на то, что компании по всему миру все больше узнают об актуальных киберугрозах, сотрудники предприятий слабо верят в способность своих работодателей защитить критические для бизнеса данные. Такие результаты были получены в ходе исследования, проведенного аналитиками издания TechRadar Pro.

Согласно полученным данным, более 70% сотрудников считают, что кибербезопасность является ключевой головной болью руководителей компании, в которой они работают. Но половина из них (45%) признаются, что чувствуют себя плохо готовыми к борьбе с киберугрозами. При этом более 66% опрошенных заявили, что скептически относятся к готовности своих коллег адаптироваться к изменениям в тактике киберпреступников, в частности — к эволюции векторов атак и появлению новых видов вредоносных программ.

«Из-за того, что многие сотрудники теперь работают за пределами офисов, традиционный периметр безопасности значительно расширился за считанные месяцы. Добавление к нему теневой ИТ-среды сделало надзор за безопасностью практически невозможным. В связи с этим компании сталкиваются с целым рядом потенциальных последствий киберинцидентов, в том числе финансового, операционного и репутационного характера», — отмечают аналитики TechRadar Pro, напоминая о том, что только за последний месяц жертвами атак программ-вымогателей стали такие гиганты, как Garmin и Canon. В первом случае дело

закончилось уплатой выкупа, во втором — отказом от этого, с последующим сливом чувствительных данных в интернет.

Сотрудники предприятий не знаю, что делать в случае кибератаки

Среди проблем, способствующих повышению уровня угрозы, участники проведенного исследования назвали собственную недостаточную подготовку, а также отсутствие четкого порядка действий в случае возникновения угрозы и подчинения.

Каждый четвертый участник опроса (26%) заявил, что обучение по вопросам кибербезопасности в его компании не соответствует стандартам. Еще почти треть респондентов (29%) признались, что понятия не имеют, кто отвечает за решение вопросов кибербезопасности в их организации, что, по мнению аналитиков TechRadar Pro должно вызвать тревогу у директоров по информационной безопасности. Они делают вывод, что хотя уровень осведомленности о кибербезопасности выше, чем когда-либо, очевидно, что предприятиям необходимо предпринимать более реальные и существенные шаги для противостояния киберпреступникам.

Для этого у них есть понятные экономические стимулы, даже не учитывая угрозу финансовых штрафов со стороны регуляторов (а они могут достигать миллионов долларов в зависимости от серьезности инцидента и размера бизнеса). Почти половина (42%) опрошенных считает, что высокий уровень безопасности компании сделает ее экономически более эффективной и привлекательной для партнеров.

«За кибербезопасность отвечают не отдельные люди или команды. Каждый сотрудник организации должен сыграть свою роль в обеспечении безопасности и защиты данных и ресурсов компании. Работая вместе, каждый — от персонала фронт-офиса до менеджеров и высшего руководства — может внести свой вклад в общее дело обеспечения безопасности. Это требует усилий и постоянно действующей, хорошо спланированной программы кибер-обучения, соответствующего корпоративной культуре. Чтобы помочь в достижении поставленной Всемирным экономическим форумом цели создания более образованной рабочей силы, Fortinet и Salesforce недавно совместно запустили Центр обучения кибербезопасности, который предлагает организациям бесплатные ресурсы для повышения осведомленности о кибербезопасности и помощи в профильных инициативах. Среди прочего, речь идет о подготовке сотрудников к ситуациям, когда происходит взлом, помощи высшему руководству в повышении уровня киберустойчивости, изучении передовых ИБ-методик. Вовлекая всех своих сотрудников, прибегая к помощи сторонних организаций, компании могут разработать и поддерживать эффективную стратегию безопасности, дополненную передовыми технологиями с высоким уровнем автоматизации», — заключает Михаил Родионов, региональный директор Fortinet в России и странах СНГ». ***(В большинстве компаний мира не верят в возможность успешного противостояния хакерам // CNews (https://safe.cnews.ru/news/top/2020-09-22_v_bolshinstve_kompanij_mira). 24.09.2020).***

***

«Администрация Трампа выпустила уже пятую по счету Директиву по космической политике, направленную на защиту космических кораблей от киберугроз. Основная цель директивы состоит в том, что в новых ракетах необходимо использовать собственное программное обеспечение, шифровать данные, а также применять другие средства защиты.

Чиновники заявили, что сегодня следует больше внимания уделять кибербезопасности в космосе, поскольку риск кибератак со стороны вероятных противников растет.

Во время конференции, посвященной пятой директиве, на вопрос, какие именно типы угроз вызывают озабоченность у правительства США, представители властей ответили размыто, сославшись на достижения в области обороны и безопасности Китая за последний год. Усилия этой страны, как доложило Министерство обороны США, сосредоточены на разработке такого оружия, как спутниковые глушители и «наступательные кибернетические возможности».

Для борьбы с этими новыми угрозами в Директиве №5 прописаны основные принципы, которых следует придерживаться NASA и частным американским компаниям при запуске спутников и других кораблей в космос. Администрация президента рекомендует операторам использовать различные типы программного обеспечения и шифровать данные. Кроме того, следует отслеживать все цепочки поставок компонентов, необходимых для создания кораблей и ракет, а также следить за безопасностью своих наземных систем. Предусматривать следует и защиту от глушения сигналов.

Многие частные космические компании уже применяют те или иные стратегии для обеспечения кибербезопасности запускаемых ракет и аппаратов. Теперь среди них будут определены лучшие и наиболее эффективные. Как заявили в администрации, правительство не пытается навязать новые требования и стандарты, а предпочитает сотрудничать с частным сектором, используя его опыт и наработки». ***(Кирилл Панов. США нашли киберугрозы в космосе // Популярная мезханика (https://www.popmech.ru/technologies/news-617023-ssha-nashli-kiberugrozy-v-kosmose/). 07.09.2020).***

***

«Власти США при создании космических систем намерены уделять повышенное внимание вопросам кибербезопасности. Об этом говорится в распространенном в пятницу меморандуме Белого дома. США планируют создавать космические системы, способные «вести непрерывный мониторинг» и «противостоять вредоносным кибератакам».

Операторы таких систем должны предусмотреть защиту от несанкционированного доступа как к самим космическим аппаратам, так и к наземным элементам инфраструктуры.

Правила изложены в директиве космической политики 5 (SPD-5). Они предназначены для установления базовой кибербезопасности космических

аппаратов и систем, а также сетей связи, создаваемых и эксплуатируемых как государственными агентствами США, так и частными космическими компаниями.

«Владельцам и операторам космических систем следует сотрудничать с целью развития оптимальных методов [кибербезопасности] и делиться между собой информацией относительно угроз и данными об инцидентах в космической отрасли».

"Эти системы, сети и каналы могут быть уязвимы для злонамеренных действий, которые могут ухудшать или нарушать космические операции или даже уничтожать спутники", - говорится в меморандуме.

"Необходимо вести непрерывный мониторинг и осуществлять адаптацию для уменьшения вредоносной киберактивности, которая может быть направлена на манипулирование, разрушение или слежку за операциями космических систем", - говорится в документе.

Разработчиков таких систем обяжут продумать механизмы защиты от глушения сигнала с помощью проверенных шифровальных систем и новейших передатчиков.

Космические силы США были учреждены в феврале 2019 года, став шестым родом американских Вооруженных сил. В доктрине Космических сил сказано, что для защиты национальных интересов они могут прибегать не только к оборонительным, но и к наступательным действиям — в космосе, на земле и в киберпространстве.

Год назад Трамп официально объявил о начале работы космического командования США, назвав космос «следующей областью военных действий».

Согласно отчету экспертов лондонского аналитического центра «Королевский институт международных отношений» (Chatham House), звездные войны куда более реальны, чем может показаться. По мнению экспертов, киберпреступники, вражеские государства и даже террористы могут избрать в качестве вектора атак спутники. В настоящее время вопрос уязвимостей в спутниках и других искусственных космических объектах до конца не изучен, чем могут воспользоваться злоумышленники.

Ранее Американские военные чиновники выразили обеспокоенность уровнем кибербезопасности современных военных спутников США. По их словам, взломать спутники могут не только космические державы, такие как Россия и Китай, но и хакеры-любители. По словам заместителя председателя Объединенного комитета начальников штабов ВВС Пола Селвы (Paul Selva), США сильно уступают России и Китаю в области кибербезопасности в космическом пространстве». ***(Власти США выпустили директиву защиты космических систем от хакерских атак // SecurityLab.ru (https://www.securitylab.ru/news/511751.php). 05.09.2020).***

***

«Мичиганский университет объявил, что откроет новый колледж инноваций и технологий. Учебное подразделение откроется осенью 2021 для обучения и подготовки студентов к карьере в новых отраслях технологий.

Студенты школы смогут получить степень бакалавра в области технологий, готовясь к трудоустройству в автомобилестроении, производстве, искусственном

интеллекте, здравоохранении, аэрокосмической отрасли, кибербезопасности и других секторах, пишет edscoop.

Будущее, которое требует высоких технологий, требует от нас подготовки выпускников к разработке и применению новых технологий на пользу общества, – заявила в пресс-релизе канцлер UM-Flint Деба Дутта.

Прогнозируют, что за следующие десятилетия занятость в области компьютерных и информационных технологий значительно возрастет. Так, по данным Бюро статистики труда, к 2029 году откроется более 500 000 новых рабочих мест.

Чтобы создать кадровый резерв для талантов, который может подготовить студентов к этим работам, другие университеты по всей стране также запускают новые программы в областях, связанных с технологиями, в частности: Университет Бельвю, Университет Северного Техаса и Пенсильваньский университет». ***(Екатерина Сердюк. Мичиганский университет планирует открыть новую школу технологий и инноваций // Телеканал новостей «24» (https://innovation.24tv.ua/ru/novuju-shkolu-tehnologij-innovacij-otkroet-michiganskij-novosti-dnja_n1423475). 27.09.2020).***

***

Країни ЄС

«Европейский месяц кибербезопасности (ECSM) - это ежегодная информационная кампания ЕС, которая проводится каждый октябрь по всей Европе. Цель состоит в том, чтобы повысить осведомленность об угрозах кибербезопасности, продвигать кибербезопасность среди граждан и организаций; и предоставить ресурсы для защиты себя в сети посредством обучения и обмена передовым опытом.

Кампания ECSM координируется Европейской комиссией и Агентством по кибербезопасности Европейского союза (ENISA) и поддерживается государствами-членами ЕС и сотнями партнеров (правительства, университеты, аналитические центры, НПО, профессиональные ассоциации, частный бизнес) из Европы. и дальше.

Ежегодно с этой международной кампанией связаны десятки мероприятий и мероприятий.

Тема ECSM 2020 - цифровые навыки.

Мы можем обеспечить цифровую безопасность только в том случае, если у нас есть специалисты с нужными знаниями и навыками, а их в настоящее время недостаточно.

Острая нехватка профессионалов в области кибербезопасности в ЕС оценивается в более чем 300 000 сотрудников.

Навыки кибербезопасности входят в общую повестку дня Комиссии по цифровым навыкам. Комиссия инвестирует в навыки кибербезопасности, в том числе через программу Digital Europe Program и Horizon Europe.

Дополнительную информацию можно найти на нашем новом обновленном веб-сайте по кибербезопасности.

Следуйте наш твиттер аккаунт и внимательно прочитайте следующий информационный бюллетень, чтобы узнать больше о планируемых мероприятиях под эгидой ECSM 2020!» ***(Think Before U Click - the European Cybersecurity Month 2020 // European Commission (https://ec.europa.eu/digital-single-market/en/news/think-u-click-european-cybersecurity-month-2020). 08.09.2020).***

***

Російська Федерація та країни ЄАЕС

«Джерела DDoS-атак на державні органи Росії в період проведення голосування щодо поправок до конституції нібито "фіксувалися з території США, Великої Британії, України та ряду країн СНД". Про це заявив спецпредставник президента РФ з питань міжнародного співробітництва в сфері інформаційної безпеки Андрій Крутських в понеділок на конференції ОБСЄ з кібербезпеки…

Він повідомив, що в 2020 році звичайною справою стали атаки з метою впливу на критичну інфраструктуру і виборні процеси.

"Наприклад, в період проведення голосування щодо поправок до Конституції Російської Федерації (25 червня — 1 липня цього року) мали місце масштабні напади на інфраструктуру ЦВК та інші державні органи Росії. Джерела DDoS-атак потужністю до 240 тис. запитів в секунду фіксувалися з території США, Великої Британії, України та ряду країн СНД", — заявив спецпредставник президента РФ.

За словами Крутських, в 2020 році проблеми, з якими всі країни стикаються в інформаційному просторі, наростають як снігова куля. Так, збільшуються обсяги протиправного контенту, в тому числі терористичного спрямування, розповсюджуваного в мережі, нормою стає здійснення деструктивних дій держав в інформаційному просторі. "Не додають оптимізму прийняті в окремих країнах концепції з нанесення превентивних кіберударів, проведення наступальних дій в кіберсфере", — констатував він…». ***(Олексій Супрун. РФ заявила, що хакери з Британії, США та України нібито "здійснювали атаки під час голосування щодо конституції" // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1890189-rf-zayavila-scho-khakeri-z-britaniyi-ssha-ta-ukrayini-nibito-zdiysnyuvali-ataki-pid-chas-golosuvannya-schodo-konstitutsiyi). 07.09.2020).***

****

«Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК), которым регламентируется данная норма, направлен на «обеспечение технологической независимости и безопасности» критической информационной инфраструктуры (КИИ) РФ, а также «создание условий для продвижения российской продукции»

Подписан приказ ФСТЭК о внесении изменений в Требования по обеспечению безопасности значимых объектов КИИ РФ. Данные изменения направлены на использование в КИИ РФ преимущественно отечественного программного обеспечения и оборудования в целях обеспечения её технологической независимости и безопасности, а также создания условий для продвижения российской продукции.

Приказ уточняет условия выбора программного обеспечения и оборудования, используемого в составе значимых объектов критической информационной инфраструктуры, а также порядок его принятия к эксплуатации на таких объектах. Документ был разработан во исполнение поручений Президента РФ Владимира Путина по итогам специальной программы «Прямая линия с Владимиром Путиным» 20 июня 2019 года.

Во время «прямой линии» Путин сказал, что власти должны обеспечить рынок для российских программистов в чувствительных отраслях для безопасности и суверенитета, а также заявил, что в целях импортозамещения российские корпорации нужно «заставить» закупать именно отечественные [программные] продукты». ***(Критическую информационную инфраструктуру защитят импортозамещённым «железом» и ПО // РосКомСвобода (https://roskomsvoboda.org/63870/). 15.09.2020).***

***

«Глава президентского Совета по правам человека (СПЧ) Валерий Фадеев сообщил о намерении разработать «цифровой кодекс» России.

Совет привлечет к работе отечественных хакеров для создания доклада президенту РФ Владимиру Путину о проблемах, связанных с компьютерными технологиями,— от травли пользователей в соцсетях до кибершпионажа с помощью камер видеонаблюдения и утечек банковских данных.

СПЧ создаст рабочую группу «по защите прав граждан в цифровой среде», чтобы к декабрю подготовить доклад президенту России. Как сообщил газете «КоммерсантЪ» Валерий Фадеев, в группу войдут члены СПЧ, а также хакеры, «прекрасно разбирающиеся во взломах и различных манипуляциях в сети».

После доклада СПЧ намерен приступить к созданию «цифрового кодекса» и инициировать законопроект, призванный защитить российских пользователей от травли в соцсетях и слежки.

«Огромная проблема сегодня — это утечка данных, которую иллюстрирует, например, заметка об Анне Кузнецовой, заказавшей за 16 тыс. руб. слежку за собой с помощью камер видеонаблюдения, установленных в городе. Или травля в соцсетях, которой недавно подвергся доктор Леонид Рошаль», — отметил Фадеев.

Как отметил глава СПЧ, российское законодательство не обеспечивает должным образом защиту граждан в цифровой среде». ***(Хакеры помогут создать цифровой кодекс России // SecurityLab.ru (https://www.securitylab.ru/news/512270.php). 18.09.2020).***

***

«Президент Российской Федерации Владимир Путин озвучил целый ряд предложений о сотрудничестве в сфере кибербезопасности между Россией и Соединенными Штатами, а также во всем мире. Об этом сообщает пресс-служба Кремля.

Путин предложил Вашингтону обменяться гарантиями невмешательства во внутренние дела друг друга, включая избирательные процессы, в том числе с использованием высокотехнологичных методов.

Глава страны-агрессора отметил, что одним из основных стратегических вызовов современности является риск возникновения масштабной конфронтации в цифровой сфере.

Путин предложил восстановить полномасштабный двусторонний регулярный межведомственный диалог по ключевым вопросам обеспечения международной кибербезопасности на высоком уровне». ***(Путин хочет наладить с США диалог по кибербезопасности // Journalist (https://journalist.today/putin-hochet-naladit-s-ssha-dialog-po-kiberbezopasnosti/). 25.09.2020).***

***

Інші країни

«Израильская судоходная компания ZIM объявила о создании дочерней компании ZKCyberStar, которая будет специализироваться на оказании услуг по обеспечению кибербезопасности.

Как сообщила пресс-служба ZIM, проект реализуется в сотрудничестве с компанией Konfidas, экспертами в области кибербезопсаности. Новую структуру возглавит в должности CEO Ронен Мероз, в настоящее время занимающий в ZIM должность Global Intermodal Division Manager.

Новая компания будет оказывать широкий спектр услуг по поддержке киберготовности, включая разработку и внедрение планов безопасности, тренинги для специалистов, управление рисками, выявление угроз и меры по предотвращению последствий кибератак, специально разработанные для предприятий морской отрасли.

Как отмечают в ZIM, уровень киберрисков в морской индустрии в свете пандемии коронавируса повысился, при этом в силу продолжающейся цифровизации уязвимость отрасли для кибератак возросла. Потери мировой экономики из-за кибератак к 2021 г. оцениваются порядка $6 трлн. в год.

ZIM (штаб-квартира - Хайфа, Израиль) - одиннадцатая контейнерная линия мира. Согласно актуальным данным Alphaliner, компания контролирует 1,3% мирового рынка морских контейнерных перевозок. Активный флот перевозчика составляют 65 судов общей вместимостью 305354 TEU (в т.ч. одно собственное вместимостью 4992 TEU)». ***(СК ZIM создала компанию для обеспечения кибербезопасности // Транспортный бизнес (http://tbu.com.ua/news/sk_zim_sozdala_kompaniu_dlia_obespecheniia_kiberbezopasnosti.html). 04.09.2020).***

***

«Израильская фирма Candiru предлагает хакерские инструменты, используемые для взлома компьютеров и серверов, а также технологию для взлома мобильных устройств. У фирмы нет web-сайта, ее сотрудники не обновляют свои профили LinkedIn с указанием места работы. Как сообщает газета TheMarker, утекшие документы и судебные дела между компанией и бывшим старшим сотрудником, раскрыли некоторые подробности об ее внутренней деятельности.

Согласно документу, подписанному неназванным вице-президентом Candiru, фирма предлагает «высококлассную платформу киберразведки, предназначенную для проникновения в персональные компьютеры, сети и мобильные телефоны». Система позволяет тайно проводить эффективные и масштабируемые операции киберразведки на отдельных мобильных устройствах.

«После развертывания, неотслеживаемое ПО немедленно идентифицирует и отображают сети, к которым подключена цель. Система инициирует замаскированные процессы по кражи данных путем манипуляции и контроля над устройствами и локальными программами, включая социальные сети, коммуникационные программы или приложения, доступ к микрофону или камере телефона или компьютера», — сообщается в документах компании.

Как утверждает Candiru, ее система может работать по всему миру, но ее нельзя развернуть в США, Израиле, России и Китае.

Компания несколько раз меняла название: она начинала как Candiru, затем стала D.F. Associates, затем преобразовалась в Greenwick Solutions. В прошлом году ее также называли Tabatha Ltd., а теперь она известна как Saito Tech.

Компания помогает правоохранительным органам и спецслужбам в разных странах без разрешения взламывать компьютерные системы, вести наблюдение, похищать информацию и даже наносить ущерб». ***(Раскрыта деятельность израильского производителя шпионского ПО Candiru // SecurityLab.ru (https://www.securitylab.ru/news/511745.php). 04.09.2020).***

***

Протидія зовнішній кібернетичній агресії

«Президент Грузии Саломе Зурабишвили в специальном заявлении 4 сентября провела параллели между кибератакой на лабораторию имени сенатора Ричарда Лугара в Тбилиси и ситуацией вокруг блогера Алексея Навального…

Она назвала кибератаку «антигуманным актом», особенно в условиях пандемии, когда «роль лаборатории – важнейшая в деле спасения человеческих жизней».

По ее словам, это было «очередной попыткой устрашения Грузии».

Саломе Зурабишвили призвала обратить внимание на время кибератаки и «беспочвенные попытки, к которым прибегла российская сторона, чтобы отвести

от себя подозрения по поводу происхождения вещества, использованного для отравления Алексея Навального».

Она призвала как можно скорее расследовать обстоятельства этой кибератаки…» ***(Дмитрий Александров. Грузия связала кибератаку на лабораторию Лугара с ситуацией вокруг Навального // Деловая газета «Взгляд» (https://vz.ru/news/2020/9/4/1058664.html). 04.09.2020).***

***

«Парламент Норвегії заявляє, що став ціллю «значної» кібератаки впродовж останнього тижня. Електронні пошти кількох обранців та співробітників парламенту були зламані. Особи хакерів наразі не встановлені.

«Це була значна атака», – заявила головний адміністратор парламенту Маріан Андреассен 1 вересня.

Речник головної опозиційної Робітничої партії повідомив суспільному мовнику NRK, що постраждали кілька членів та співробітників.

Для протидії кібернападу залучили Норвезьку службу національної безпеки. Там заявили, що працювали впродовж кількох днів.

Андреассен розповіла, що спроби зупинити атаку мали «негайний ефект». ***(Парламент Норвегії заявляє, що став ціллю «значної» кібератаки // Радіо Свобода (https://www.radiosvoboda.org/a/news-norvehia-kibberataky/30815449.html). 01.09.2020).***

***

«Вчора Міністерство інформаційних технологій Індії наказало заблокувати 118 китайських додатків. За його словами, вони «завдають шкоди суверенітету і цілісності Індії, захисту, державній безпеці та громадському порядку». «Цей крок допоможе захистити інтереси десятків мільйонів індійських користувачів мобільного зв'язку та Інтернету. Це рішення є цілеспрямованим кроком для забезпечення безпеки і суверенітету індійського кіберпростору», – сказали в міністерстві.

Міністерство електроніки та інформаційних технологій отримало безліч скарг з різних джерел. Зокрема кілька повідомлень про неправомірні дії деяких мобільних додатків, доступних на платформах Android і iOS, з метою крадіжки і таємної передачі даних користувачів несанкціонованим чином на сервери, розташовані за межами Індії. В інтересах суверенітету і цілісності Індії, а також захисту та безпеки держави, уряд вирішив заблокувати певні програми, що використовуються як на мобільних, так і на інших пристроях з доступом в Інтернет». ***(Грицина Вікторія. Індія заблокувала ще 118 китайських додатків // Pingvin Pro (https://pingvin.pro/gadgets/news-gadgets/indiya-zablokuvala-shhe-118-kytajskyh-dodatkiv.html). 03.09.2020).***

***

«Минулого року стратегічна установа чеського уряду стала жертвою кібератаки, за якою, імовірно стоїть РФ.

До такого висновку дійшов чеський Національний офіс з кібер- і інформаційної безпеки…

Офіс заявив, що шпигунство проти чеської установи почалося з так званої фішингової атаки на електронні адреси установи. Користувач завантажував шкідливу програму в систему з вхідного листа. Згідно з аналізом офісу, група Sofacy, яку професійне співтовариство пов'язує з російською розвідкою ГРУ, ймовірно, стояла за цим інцидентом.

Яка саме установа зазнала кібератаки, офіс не уточнює.

У звіті відомства також згадано діяльність групи Winnti, яка займається в основному кібер-промисловим шпигунством. Офіс вважає, що ця група, яку експерти найчастіше пов'язують з Китаєм, хоча і не здійснювала кібератаки минулого року може з 50-відсотковою ймовірністю зробити таку спробу в майбутньому…». ***(У Чехії підозрюють Росію у кібератаках проти стратегічної держустанови // Європейська правда (https://www.eurointegration.com.ua/news/2020/09/2/7113890/). 02.09.2020).***

***

«Російські хакери атакували понад 200 організацій, що мають відношення до президентської кампанії у США.

Як передає Укрінформ, про це повідомляє DW з посиланням на доповідь експертів компанії Microsoft.

"Хакери, пов'язані з Росією, Китаєм та Іраном, все частіше атакують передвиборчі команди Дональда Трампа і його суперника-демократа Джо Байдена. Мета кібератак - отримати компрометувальну інформацію на людей і структури, близькі до обох кандидатів у президенти США", - йдеться в повідомленні.

Як зазначив віцепрезидент Microsoft із безпеки користувачів Том Берт, інтенсивність кібератак збільшується в міру наближення дати президентських виборів

За його словами, група російських хакерів, причетних до військової розвідки, вже прагнула вплинути на хід американських виборів у 2016 році. У 2019-му ця група намагалася отримати доступ до особистих даних політичних радників, які працюють як на Демократичну, так і на Республіканську партії, а також представників експертного співтовариства.

Загалом атаками були зачеплені понад 200 організацій, сказав Берт.

Він додав, що хакери з КНР без успіху пробували скомпрометувати довірену особу Джо Байдена. Також безрезультатною виявилася кібератака з Ірану. Про те, чи були успішні дії російських хакерів, Берт нічого не сказав, коментує DW…». ***(Microsoft: хакери з Росії, Китаю та Ірану атакують штаби і Трампа, і Байдена // Информационное агентство ЦК (http://expert.org.ua/armiya/2020/microsoft-hakeri-z-rosiyi-kitayu-ta-iranu-atakuyut-shtabi-i-trampa-i-baydena). 11.09.2020).***

***

Россия не вмешивалась, не вмешивается и не собирается вмешиваться ни в чьи электоральные процессы, заверил Дмитрий Песков.

Пресс-секретарь президента РФ Дмитрий Песков считает фобиями утверждения о вмешательстве российских хакеров в американские выборы. Об этом сообщает Интерфакс в пятницу, 11 сентября.

"По итогам (президентской кампании 2016 года в США – ред.) мы не видели каких-либо вразумительных аргументов, обоснований, которые бы говорили, что какие-то организации, имеющие отношение к РФ, занимались киберпреступностью", – сказал Песков, комментируя заявление компании Microsoft о том, что она обнаружила признаки вмешательства группы киберпреступников из России, Ирана и Китая в избирательный процесс в США накануне выборов президента 2020 года.

"Тогда, согласитесь, не было никакой вразумительной информации, были какие-то голословные утверждения, этакие фобии, что, когда происходит киберпреступление, то этим обязательно занимаются русские кибермонстры, – подчеркнул пресс-секретарь Путина. – Если (заявление Microsoft) выдержано в том же духе, то это низкая квалификация. Если там содержится профессиональная аргументация, то, конечно, стоит к ней прислушаться".

По словам Пескова, "разведка США неоднократно ошибалась, и это подтверждалось в ходе различных парламентских расследований, неоднократно она ошибалась, и это признано самими законодателями США на счет вмешательства РФ в выборы".

"Потом были сделаны официальные заключения комиссии, что Россия не вмешивалась в выборы", – продолжил Песков, отметив, что к такого рода заявлениям нужно относиться "с большой долей толерантности".

Он заявил, что "Россия не вмешивалась, не вмешивается и не собирается вмешиваться ни в чьи внутренние дела, ни в чьи электоральные процессы".

"И нам очень не нравится, когда другие пытаются вмешиваться в наши дела", – сказал пресс-секретарь Путина…». ***(Кремль назвал "фобиями" обвинение в кибератаках на выборы в США // Украина сегодня (https://ukr-today.com/news/russian/448671-kreml-nazval-fobijami-obvinenie-v-kiberatakah-na-vybory-v-ssha.html). 11.09.2020).***

***

«Британские власти расследуют взлом компьютерных систем Министерства иностранных дел страны, в результате которого неизвестные злоумышленники похитили сотни секретных документов, касающихся пропагандистских программ Великобритании в Сирии.

По информации издания Middle East Eye, речь идет о документах о финансовых и операционных связях Министерства иностранных дел и по делам Содружества с частными подрядчиками, скрыто управляющими сетью медиа-платформ в Сирии.

Об утечке стало известно на прошлой неделе после публикации активистами Anonymous в открытом доступе ряда документов, описывающих действия подрядчиков в рамках программы пропаганды, в том числе запуск радиостанций, англо- и арабоязычных журналов, газет и других печатных материалов для поддержки оппозиции в стране.

В настоящее время неизвестно, какая именно группировка стоит за взломом, но, исходя из сложности атаки, британские власти подозревают причастность спонсируемых государством хакеров, в частности из РФ.

Как отмечает Middle East Eye, министерство обеспокоено не столько содержанием утекших документов (о существовании программы известно уже несколько лет), сколько легкостью, с которой хакеры проникли в компьютерные системы. В самом же ведомстве отказались комментировать инцидент». ***(Хакеры украли пропагандистские материалы у британского МИД // SecurityLab.ru (https://www.securitylab.ru/news/512595.php). 30.09.2020).***

***

«Исследователи кибербезопасности из индийской фирмы Quick Heal обнаружили текущую кампанию по кибершпионажу, направленную против подразделений обороны и личного состава вооруженных сил Индии. Кампания продолжается по крайней мере с 2019 года, а целью киберпреступников является хищение конфиденциальной информации военных.

Вредоносная кампания, получившая название SideCopy, была организована киберпреступной группировкой, которая успешно остается незамеченной, «копируя» тактику других злоумышленников.

Атаки начинаются с отправки электронного письма со встроенным вредоносным вложением — либо ZIP-файл, содержащий LNK-файл, либо документ Microsoft Word. Помимо выявления трех различных цепочек заражения, примечателен тот факт, что одна из них использовала внедрение шаблона и критическую уязвимость редактора Microsoft Equation Editor (CVE-2017-11882) 20-летней давности. Ее эксплуатация позволяет злоумышленникам выполнить удаленный код на системе без вмешательства пользователя.

По словам исследователей, в документе Word якобы утверждается, что он посвящен теме политики оборонного производства правительства Индии. Более того, LNK-файлы имеют двойное расширение («Defense-Production-Policy-2020.docx.lnk») и содержат значки документов, тем самым вводя жертву в заблуждение и побуждая ее открыть файл.

После открытия LNK-файлы используют mshta.exe для выполнения вредоносных Microsoft HTML Applications (HTA). Файлы HTA содержат поддельный документ и вредоносный модуль.NET, который выполняет указанный документ и загружает файл HTA второго этапа. Последний, в свою очередь, проверяет наличие популярных антивирусных решений перед хищением учетных данных Microsoft.

После запуска файла также загружается вредоносная библиотека DUser.dll и RAT-модуль winms.exe. DUser.dll будет инициировать соединение через специальный IP-адрес через TCP-порт 6102.

«После успешного подключения злоумышленники смогут отправлять команды с C&C-сервера для выполнения различных операций. Например, если C&C-сервер отправит 0, то на системе жертве начнется сбор информации о технических данных компьютера, имени пользователя, версии ОС и пр.», — пояснили эксперты.

Хотя методы именования DLL-файлов имеют общие черты с группировкой SideWinder, использование набора инструментов с открытым исходным кодом и совершенно другая инфраструктура C&C-сервера привели исследователей к выводу, что злоумышленники имеют пакистанское происхождение и являются участниками группировки Transparent Tribe, которая ранее организовала несколько атак на индийских военных и правительственный персонал». ***(Раскрыта кампания по кибершпионажу против индийской армии // SecurityLab.ru (https://www.securitylab.ru/news/512531.php). 29.09.2020).***

***

Створення та функціонування кібервійськ

«Согласно общепринятому в западном мире мнению, с точки зрения военной мощи в киберпространстве США превосходят Китай, Великобританию, Иран, Северную Корею и Россию. Однако согласно новому исследованию специалистов Белферского центра науки и международных отношений при Гарвардском университете, Китаю удалось преодолеть отрыв и сравняться с США в таких вопросах, как слежение, кибероборона и строительство коммерческого сектора в киберпространстве.

«Многие, в особенности американцы, считают, что США, Великобритания, Франция и Израиль превосходят Китай с точки зрения кибермощности. Как показывает наше исследование, это не так – Китай очень продвинут и идет практически нога в ногу с США», – сообщил содиректор Белферского центра Эрик Розенбах (Eric Rosenbach).

В общем и целом, по кибермощности Китай занимает второе место в мире после США. Однако исследование также показало, что несколько стран, пока не считающиеся кибердержавами, растут на мировой арене.

Определение кибермощности – задача довольно трудная, поскольку информация по кибервооружению стран в основном засекречена. Участвовавшие в создании концепции определения киберпотенциала стран специалисты Google Threat Analysis Group и консультанты британского правительства в вопросах киберполитик задались целью предоставить метрику, отображающую более реалистичную картину экосистемы кибербезопасности. В рамках разработанной ими концепции для измерения киберпотенциала стран рассматриваются 27 показателей. Еще 32 показателя предназначены для определения намерений стран использовать свою кибермощность.

Для того чтобы получить полную картину кибермощности, исследователи разделили свои измерения на семь категорий: оборонительные возможности, наступательные кибероперации, сбор внешних разведданных, слежение, контроль над информационной средой, возможности и намерения стран, связанные с формированием международных кибернорм, и их усилия по развитию своего внутреннего киберсектора.

По результатам исследования, лидером на мировой киберарене являются США, возглавшие пять из семи категорий: контроль над информационной средой,

формирование международных кибернорм, сбор внешних разведданных, а также наступательные и разрушительные кибероперации. Вслед за США и Китаем в десятку мировых лидеров входят Великобритания, Россия, Нидерланды, Франция, Германия, Канада, Япония и Австралия.

Однако исследование также показывает, что есть ряд стран, наращивающих свои кибермощности, в том числе Объединенные Арабские Эмираты, Вьетнам и Сингапур. Такие страны, как Малайзия, Швеция и Швейцария также вошли в топ-10 в нескольких категориях, включая сбор разведданных, слежение, контроль над информацией и коммерческий рост»*. (По своей кибермощности Китай идет нога в ногу с США // SecurityLab.ru (https://www.securitylab.ru/news/511899.php). 09.09.2020).*

***

«Країни ЄС, Агентство ЄС із кібербезпеки (ENISA) та Єврокомісія розпочали сьогодні спільні навчання з кібербезпеки, головною метою яких є відпрацювання взаємодії в рамках нової Комунікаційної мережі організацій з протидії кібернетичним кризам (CyCLONe)…

«Нова Комунікаційна мережа організацій з протидії кібернетичним кризам є результатом відмінної співпраці між країнами ЄС і європейськими інституціями у зусиллях з кібернетичного захисту наших мереж та критично важливих систем. Кібербезпека є спільною відповідальністю, тож ми маємо спільно розробити та виконувати плани швидкої спільної відповіді на випадок масштабних кібернетичних інцидентів або криз», - зауважив з цього приводу Єврокомісар з питань внутрішнього ринку Террі Бретон.

За повідомленням, головним завданням спільного тренування, яке було організовано Нідерландами спільно з ENISA, є відпрацювання оперативних процедур та випробування стійкості європейських кібернетичних систем. В умовах кібернетичної кризи національні органи кібернетичного захисту мають бути заданими швидко приймати рішення на всіх рівнях та координувати їх одне з одним. Новостворена мережа CyCLONe (Cyber Crisis Liaison Organisation Network) дозволить усунути «слабкі місця» у системі такої взаємодії». *(Країни ЄС почали навчання з кібербезпеки // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (https://day.kyiv.ua/uk/news/290920-krayiny-yes-pochaly-navchannya-z-kiberbezpeky). 29.09.2020).*

***

«Английский генерал Патрик Сандерс заявил о том, что страна обладает кибероружием, способным нанести удар по критической инфраструктуре противника. Среди потенциальных противников Сандерс назвал Россию, Иран и Китай.

Атака по критической инфраструктуре

Министерство обороны Великобритании обладает кибероружием, которое способно вывести из строя энергосистемы и другие объекты инфраструктуры государств-противников. Об этом заявил глава Стратегического командования вооруженных сил Великобритании генерал (соответствует российскому званию

генерал-полковник) Патрик Сандерс (Patrick Sanders), выступая на разведывательной базе у города Коршем (Corsham) в Англии, пишет The Guardian. В качестве потенциальных противников Сандерс упомянул Россию, Иран и Китай, обвинив их во вмешательстве в демократические процессы на Западе.

Как отметил Сандерс, разрушение или уничтожение критической инфраструктуры теоретически может включать нанесение ударов по коммуникациям, телефонным или энергетическим сетям вражеской страны в условиях войны. Британские военные и раньше говорили о том, что они обладают наступательным кибернетическим потенциалом, однако до сих пор это не обсуждалось настолько открыто. Считается, что Великобритания провела хакерскую операцию против ИГИЛ в 2017 г., чтобы получить информацию о беспилотнике, управляемом исламистской террористической группировкой в Мосуле (Ирак).

По словам Сандерса, премьер-министр страны Борис Джонсон (Boris Johnson) считает исключительно важным, чтобы королевство обладало самыми передовыми возможностями для различных действий в киберпространстве. С этой целью военные тесно сотрудничают с Центром правительственной связи (Government Communications Headquarters, GCHQ), спецслужбой Великобритании, ответственной за ведение радиоэлектронной разведки и защиту правительственной и военной информации.

Сандерс сказал, что Великобритания испытывает до 60 серьезных хакерских атак в день, которые требуют вмешательства экспертов. Основными целями хакеров являются Центр управления безопасностью глобальных операций ВС страны и штаб-квартира организации Defence Digital.

В Британии могут появиться национальные кибервойска

Политтехнолог и главный советник премьер-министра Великобритании Доминик Каммингс (Dominic Cummings) с энтузиазмом поддерживает выделение дополнительных средств и внедрение военных технологий для проведения кибератак. Правительство Великобритании давно обсуждает возможность создания национальных кибервойск, которые объединят специалистов из Минобороны и британских спецслужб. По мнению The Guardian, увеличение расходов на создание кибероружия будет одним из главных пунктов пятилетнего плана оборонной политики Великобритании. Ожидается, что Джонсон может объявить о создании Национальных кибервойск уже в ноябре 2020 г., когда премьер-министр представит комплексный обзор вопросов безопасности, обороны и внешней политики страны…». ***(Англия создала кибероружие, способное разрушить телеком- и энергосистему России // CNews (https://www.cnews.ru/news/top/2020-09-28_angliya_sozdala_kiberoruzhie). 28.09.2020).***

***

«Фахівці міжнародного розробника антивірусного програмного забезпечення, експерта в області кіберзахисту - компанії ESET розповіли, чим можуть бути небезпечні неактивні профілі користувачів в соцмережах, і чому їх варто видаляти…

Як повідомляється на сайті ESET, коли ми видаляємо додаток соціальної мережі або будь-яку іншу програму з зареєстрованим особистим обліковим записом, більшість користувачів вважає, що оператор служби видалить їх особисту інформацію зі своїх систем. Однак, не всі програми дотримуються правил видалення інформації.

«Зокрема, нещодавно було виявлено, що Instagram зберігає фотографії і приватні повідомлення на своїх серверах ще тривалий час після нібито їх видалення. Однак Instagram не єдиний додаток, який порушував норми щодо зберігання конфіденційних даних користувачів. У минулому році один із дослідників виявив, що Twitter роками зберігав особисті повідомлення, а також дані з неактивних або заблокованих облікових записів», - йдеться в повідомленні.

Чому варто видаляти неактивні акаунти

Як відзначають фахівці з кібербезпеки, в разі видалення облікового запису ви обмежуєте використання своїх даних і відкликаєте згоду на відстеження геолокації ваших пристроїв. В іншому випадку, якщо компанія зіткнеться з витоком даних, ваша інформація може продаватися в даркнеті. Кіберзлочинці ніколи не перестануть атакувати сервери, тому якщо ваші дані будуть серед викрадених, вони можуть бути використані проти вас.

За даними ESET, подібна ситуація трапилася з користувачами Myspace. У 2016 році облікові дані для входу та відповідні дані 427 мільйонів профілів Myspace були виставлені на продаж в даркнеті, і, звичайно, не всі з них були активними в той час. Серед викрадених даних були паролі, тому користувачі, які повторно використовували комбінації, могли втратити доступ і до інших облікових записів.

Як захиститися від шахраїв

З метою запобігання подібних інцидентів фахівці ESET рекомендують вводити особисті дані тільки в разі потреби і при можливості включати VPN для програм, які використовують або навіть перепродають вашу інформацію. У Великобританії відповідно до Загального регламенту про захист даних (GDPR) діє заборона на продаж особистої інформації третім особам без згоди користувача, але все це не має значення в випадках витоку даних або їх викрадення зловмисниками.

Існує думка, що всі опубліковані дані в інтернеті залишаються там назавжди, тому ми можемо тільки зменшити ризики злому акаунтів. Для цього слід переглянути свій телефон, відкрити всі неактивні додакти і видалити саме обліковий запис, а потім вже додаток. Незважаючи на те, що інформація з соціальних мереж не здається занадто цінною, вона може бути використана в шахрайських схемах, пов'язаних із викраденням ваших банківських або інших важливих даних». ***(Фахівці розповіли про небезпеку неактивних профілів в***

соцмережах // Багнет (http://www.bagnet.org/news/tech/1290828/fahivtsi-rozpovili-pro-nebezpeku-neaktivnih-profiliv-v-sotsmerezhah). 04.09.2020).

***

«Отсутствие защиты базы данных форума веб-мастеров Digital Point привело к утечке данных 800 тыс. пользователей.

Калифорнийский форум Digital Point описывает себя как «крупнейшее сообщество веб-мастеров в мире». Его пользователями являются фрилансеры, маркетологи, разработчики и представители других специальностей.

1 июля нынешнего года исследовательская команда WebsitePlanet и эксперт в области безопасности Джеремайя Фаулер (Jeremiah Fowler) обнаружили незащищенную базу данных Elasticsearch, содержащую более 62 млн записей, в том числе данные 863 412 пользователей Digital Point (имена, электронные адреса и внутренние идентификационные номера). Кроме того, в БД содержались внутренние записи и публикации пользователей.

Изучая БД с целью выяснить ее владельца, исследователи наткнулись на наборы данных, относящиеся к участникам форума, пожаловавшимся на сообщения, с указанием причин жалоб, таких как «плохие деловые отношения», спам и т.д. Другими словами, эти наборы данных являются весьма личными.

Помимо хищения данных и фишинга, незащищенная БД может стать жертвой Meow Bot – автоматизированного скрипта, скомпрометировавшего тысячи баз данных MongoDB и Elasticsearch в июле нынешнего года. После развертывания скрипт подменяет данные числами и словом «meow».

Фаулер уведомил Digital Point о проблеме в тот же день, когда она была обнаружена, - 1 июля. Примечательно, что нужный электронный адрес исследователь обнаружил там же, в незащищенной БД. В течение считанных часов после уведомления администрация Digital Point закрыла базу данных». ***(Крупнейшее сообщество веб-мастеров в мире допустило утечку данных // SecurityLab.ru (https://www.securitylab.ru/news/511795.php). 08.09.2020).***

***

«Facebook подала судебный иск против Ирландской комиссии по защите данных… Компания призвала регулятора соразмерно подходить к вопросу передачи данных из ЕС в США, пока по нему не будет достигнуто устойчивое долгосрочное решение.

В конце августа Ирландская комиссия по защите данных направила Facebook требование прекратить передачу данных европейских пользователей в США. Это первый случай, когда регулятор из ЕС потребовал от крупной технологической компании выполнить принятое в июле решение Европейского суда ЕС.

В 2019 году Европейский суд в Люксембурге году начал рассматривать жалобу австрийца Макса Шремса против передачи персональных данных Facebook спецслужбам США, которые якобы прибегают к массовой слежке за пользователями. Перед этим Шремс пожаловался в Комиссию по защите персональных данных Ирландии и потребовал прекратить оборот информации между ирландским и американским офисами компании Facebook. Регулятор,

решив, не обладает нужными полномочиями, обратился с этим запросом в Высокий суд Ирландии, а тот — в суд ЕС. Последний позднее приостановил действие соглашения между ЕС и США о передаче данных пользователей.

Дело может стать прецедентом для американских технологических корпораций, заставив их теперь либо выделять данные граждан ЕС из всех остальных и хранить их отдельно, либо ограничивать свои операции в ЕС, говорят аналитики. Вслед за Facebook такие требования могут быть направлены и другим технологическим компаниям». ***(Facebook идёт в суд из-за запрета передавать данные из ЕС в США // РосКомСвобода (https://roskomsvoboda.org/63774/). 11.09.2020).***

***

«Связанная с военными и разведывательными сетями компания Zhenhua Data собрала в единую базу подробные данные, включая дату рождения, адрес, профессиональные достижения, банковские записи и другие сведения — все это могло быть взято как из открытых источников, так и приобретено в даркнете

Китайский оппозиционный активист прислал разведывательному альянсу «Пять глаз» базу с данными 2,4 миллиона граждан США, Великобритании, Австралии, Канады, Индии и Японии, которую собрала связанная с китайской разведкой компания Zhenhua Data. По словам аналитиков, большинство данных собрано из открытых источников, таких как профили в социальных сетях, куда входят дата рождения, семейное положение, фотографии, список родственников, аккаунты в соцсетях, образование, профессиональные достижения и список правонарушений. Однако там присутствуют и сугубо конфиденциальные данные, например, банковские записи и заявления о приёме на работу.

Среди людей, на которых китайская компания собрала данные, — высокопоставленные политики, члены королевской семьи и командующие армиями. Internet 2.0, консалтинговая компания по кибербезопасности, базирующаяся в Канберре и клиентами которой являются правительства США и Австралии, заявила, что смогла восстановить записи примерно 250 000 человек из утекшего набора данных, в том числе около 52 000 американцев, 35 000 австралийцев и почти 10 000 британцев. В числе тех, чьи данные обнаружены в базе, автралийский премьер-министр Скотт Моррисон. Предполагается, что часть информации Zhenhua Data нашла в даркнете.

Аналитик американской разведки в разговоре с ABC назвал эту базу «Cambridge Analytica на стероидах». Источники The Age в британской разведке посчитали «пугающим» масштаб такой утечки. Американский учёный и эксперт по кибербезопасности Кристофер Болдинг заявил, что утечка похожа на «открытие Святого Грааля»:

«Мир находится только на начальном этапе понимания того, сколько Китай инвестирует в разведку».

На удалённом сайте Zhenhua Data утверждалось, что компания предоставляла услуги для «военной, охранной и иностранной пропаганды», а свою миссию она описывала как влияние на «великое омоложение китайской нации».

Когда Guardian обратилась к Zhenhua за комментарием, там ответили: «Сообщения об инциденте не соответствуют действительности».

«Все наши данные являются общедоступными в Интернете. Мы их не собираем. Это просто интеграция данных. Наша бизнес-модель и партнеры — наша коммерческая тайна. Нет никакой базы данных о двух миллионах человек», — сказала представительница компании по фамилии Сун, также назвавшаяся главой Zhenhua Data.

«Мы частная компания, — сказала она, отрицая какие-либо связи с китайским правительством или военными. — Наши клиенты — исследовательские организации и бизнес-группы». ***(Данные миллионов граждан Австралии, Великобритании и США попали в руки китайской разведки // РосКомСвобода (https://roskomsvoboda.org/63824/). 14.09.2020).***

***

«В США пользователь соцсетями Британи Кондити подала в федеральный суд Сан-Франциско иск против Facebook. В нем женщина обвинила компанию в шпионаже за людьми через камеру телефона.

Британи Кондити считает, что Facebook сознательно использует камеру смартфонов при пользовании приложением Instagram. По ее словам, компании это выгодно, ведь это «дает возможность собирать выгодную и ценную информацию о своих пользователях, не имея доступа к этому иначе», сообщает Голос Америки.

Согласно иску, основным мотивом таких действий Facebook может быть увеличение доходов от рекламы, которая должна стать еще более целевой для пользователей. В частности, с помощью такого шпионажа можно увидеть, как пользователи реагируют на рекламу в Instagram и понять, нашла ли реклама своего потенциального покупателя.

Компания Facebook опровергла эти заявления и заявила о программной ошибке, из-за которой телефон сам получал доступ к камере.

Как защититься от шпионажа Facebook, рассказал специалист по кибербезопасности и советник секретаря СНБО Юрий Мелащенко.

Он советует держать постоянно выключенным микрофон, а также не давать Facebook доступ к вашим контактам и запретить ему использовать геолокацию.

Также для защиты от слежки со стороны Facebook могут помочь сторонние приложения. Мелащенко советует Ghostery (позволяет отключить трекеры на сайтах, которые вы посещаете) и The Fondom Project (шифрует все сообщения в Messenger)». ***(Facebook снова обвинили в слежке за пользователями. Теперь они используют камеру смартфонов при работе приложения Instagram // KOMA.Life (https://koma.life/novosti/facebook-snova-obvinili-v-slezhke-za-polzovatelyami-teper-oni-ispolzuyut-kameru-smartfonov-pri-rabote-prilozheniya-instagram/). 20.09.2020).***

***

«ИБ-специалист компании WizCase Ата Хакчил (Ata Hakcil) обнаружил, что сотрудники Microsoft по ошибке оставили один из бэкэнд-серверов Bing доступным для любого желающего.

Исследователь пишет, что сервер хранил более 6,5 Тб логов мобильный приложений, содержащих 13 000 000 000 записей, полученных из поисковика. Свою теорию на этот счет специалист проверил очень просто – нашел в логах свои поисковые запросы, которые выполнял в приложении Bing для Android.

Хакчил пишет, что сервер был доступен через интернет в период с 10 по 16 сентября 2020 года, а когда специалист уведомил о проблеме инженеров Microsoft Security Response Center (MSRC), сервер вновь защитили паролем.

Журналисты издания ZDNet получили комментарий о случившемся от представителей Microsoft. В компании заверили, что исправили неправильную конфигурацию сразу же после получения уведомления от Хакчила, а также подчеркнули, что утекло весьма ограниченное количество данных, которые не были персонализированы.

В компании даже пошли навстречу изданию и предоставили журналистам доступ к тому самому Elasticsearch-серверу, чтобы те убедились сами – на сервере нет и не было никаких личных пользовательских данных. ZDNet пишет, что сервер действительно содержал лишь технические детали: поисковые запросы, сведения о системе пользователя (устройство, ОС, браузер и так далее), сведения о географическом местоположении (если доступны), а также различные токены, хэши и коды купонов». ***(Мария Нефёдова. Microsoft оставила открытым один из внутренних серверов Bing // Хакер (https://xakep.ru/2020/09/22/bing-leak/). 22.09.2020).***

***

«Издание Bleeping Computer, ссылаясь на известного ИБ-эксперта Боба Дьяченко, предупредило о том, что компания Razer недавно оставила базу данных своего интернет-магазина незащищенной. Из-за этой оплошности производителя игровых девайсов данные примерно 100 000 человек, покупавших продукты в интернет-магазине компании, могли попасть в руки посторонних.

Дьяченко обнаружил незащищенную базу Razer, доступную любому желающему, 19 августа 2020 года. …БД содержала имя клиента, адрес электронной почты, номер телефона, номера заказов, детали заказов, а также биллинговые адреса и адреса доставки.

Исследователь рассказывает, что на протяжении нескольких недель он не мог выйти с компанией на контакт, и лишь 9 сентября 2020 года сотрудники Razer все же обратили внимание на проблему и обезопасили проблемную БД. При этом в итоге в компании подчеркнули, что номера банковских карт пользователей и их пароли утечка не затрагивала.

Дьяченко и специалисты Bleeping Computer отмечают, что даже без паролей и платежных данных злоумышленники могут использовать утекшую информацию о пользователях в фишинговых атаках, для сбора более конфиденциальной информации (включая финансовые данные)». ***(Мария Нефёдова. Компания Razer допустила утечку данных // Хакер (https://xakep.ru/2020/09/14/razer-leak/). 14.09.2020).***

***

«Крупная е-коммерческая компания Shopify при участии ФБР и других правоохранительных органов расследует утечку данных, спровоцированных двумя ее сотрудниками.

Как сообщают представители Shopify, двое сотрудников отдела техподдержки получили доступ и попытались похитить у продавцов данные о транзакциях покупателей. Инцидент безопасности предположительно затронул порядка двухсот магазинов. По данным отчета за прошлый квартал, платформа Shopify насчитывает более 1 млн зарегистрированных продавцов.

Как подчеркивают в компании, утечка произошла не из-за уязвимости в платформе, а по вине недобросовестных инсайдеров. Злоумышленники могли получить доступ к таким данным покупателей, как электронные адреса, имена, адреса проживания, а также сведения о заказах (товарах и услугах). Данные банковских карт и другая финансовая информация не были затронуты утечкой. Обнаружив несанкционированный доступ к данным пользователей, компания заблокировала его и заявила о случившемся в правоохранительные органы.

В настоящее время расследование находится на ранних стадиях. Shopify намерена в скором времени уведомить всех затронутых продавцов и покупателей». ***(Недобросовестные сотрудники Shopify получили доступ к данным покупателей // SecurityLab.ru (https://www.securitylab.ru/news/512400.php). 23.09.2020).***

***

«Компания ArbiterSports, предоставляющая программное обеспечение для спортивных лиг, сообщила об инциденте безопасности, затронувшем порядка 540 тыс. зарегистрированных членов, в том числе спортивных судей и высокопоставленных представителей спортивных лиг и школ.

В частности, ArbiterSports является официальным поставщиком ПО для Национальной ассоциации студенческого спорта (National Collegiate Athletic Association, NCAA) – американской университетской спортивной ассоциации, в которую входят более 1,2 тыс. организаций, устраивающих спортивные соревнования в колледжах и университетах США и Канады.

Согласно уведомлению ArbiterSports, в июле нынешнего года компании удалось отразить атаку вымогательского ПО. Хотя злоумышленникам и не удалось зашифровать ее системы, они все-таки смогли похитить резервные копии файлов.

В резервных копиях содержались данные из web-приложений ArbiterGame, ArbiterOne и ArbiterWorks, используемых спортивными лигами и школами для назначения и управления расписаниями судей и официальных лиц. В результате инцидента злоумышленники похитили данные пользователей, зарегистрировавшихся в вышеупомянутых приложениях, в том числе их имена пользователя, настоящие имена, пароли, домашние и электронные адреса, даты рождения и номера социального страхования.

После того, как ArbiterSports удалось отразить атаку вымогательского ПО, злоумышленники связались с ней и потребовали выкуп за удаление похищенных ими файлов. Компания заплатила нужную сумму и получила от киберпреступников подтверждение, что данные действительно были удалены. Правда, никакой

гарантии того, что злоумышленники не сохранили себе копии похищенных данных, нет». ***(Хакеры похитили данные 540 тыс. спортивных судей и представителей спортивных лиг // SecurityLab.ru (https://www.securitylab.ru/news/512317.php). 22.09.2020).***

***

«Мошенники нападают на ваши учетные записи в социальных сетях с помощью фишинговых писем, которые якобы нарушают авторские права или обещают поставить блестящую «синюю галочку» рядом с вашим именем.

Социальные сети, такие как Twitter, Facebook, Instagram и TikTok, становятся важным компонентом жизни людей, и злоумышленники нацелены на них со злонамеренными целями

Эти украденные учетные записи затем используются для кампаний дезинформации, мошенничества с криптовалютой, такого как недавние взломы Twitter, или продаются на подпольных рынках.

В связи с этим социальные счета следует рассматривать как ценный товар и защищать как таковые.

Фишинговые атаки социальных сетей, на которые следует обратить внимание

За последний месяц команда MalwareHunterTeam отслеживала многочисленные фишинговые кампании, нацеленные на ваши учетные записи в социальных сетях, и делилась ими с BleepingComputer.

Ниже мы описываем два наиболее распространенных фишинговых мошенничества в социальных сетях, с которыми вы можете столкнуться, чтобы вы знали, как их избежать.

Поддельные проверочные фишинговые страницы

Первая фишинговая кампания стала популярной в последнее время, поскольку она обещает поставить вам проверенную галочку в социальных сетях, таких как TikTok, Instagram и Twitter.

Наиболее распространенными социальными сетями, на которые распространяется это мошенничество, являются Twitter и Instagram, и пользователям предлагается ввести логин и пароль для проверки.

Не так часто, как Instagram или Twitter, также создаются фишинговые страницы TikTok, которые обещают пользователям блестящий значок проверки.

Почти на всех целевых страницах, которые мы видели, подталкивая эти мошенничества с проверкой, есть слово «проверить» или «значок», поэтому будьте осторожны с любыми URL-адресами, содержащими эти строки и утверждающими, что вы можете проверить вашу учетную запись.

Поддельные страницы с нарушением авторских прав

Еще одна широко распространенная фишинговая кампания в социальных сетях претендует на нарушение авторских прав на опубликованный вами пост.

На этих фишинговых страницах указано, что ваша учетная запись Twitter или Instagram будет приостановлена в течение 24 часов, если вы не войдете в систему и не оспорите иск о нарушении авторских прав.

Ниже вы можете увидеть пример недавних фишинговых страниц Twitter и Instagram, посвященных нарушению авторских прав…

Что делает фишинговую страницу Instagram интересной, так это то, что она отображает ваше фактическое изображение профиля на фишинговой странице, чтобы оно выглядело более законным, как показано на изображении Дуэйна Джонсона выше.

Следует отметить, что приведенная выше фишинговая страница Instagram также нацелена на пароль вашей учетной записи электронной почты, поскольку захват учетной записи электронной почты дает широкий спектр доступа к другим учетным записям.

Эти веб-сайты для этих фишинговых страниц с нарушением авторских прав обычно содержат слова «авторское право» или «нарушение» в URL-адресе, что упрощает их обнаружение.

Что делать, если вы попались на эту аферу

Этих мошенничества не было бы, если бы люди не попадались на них.

Может быть, недосыпание, стресс на работе или вы только что поссорились со своим партнером; попадание в сеть фишинговых атак может произойти случайно.

Если вы по ошибке попались на одну из этих афер и введете свой логин и пароль, вам следует немедленно войти в сервис и изменить свой пароль.

Вы также должны включить 2FA / MFA в своих учетных записях в социальных сетях, чтобы мошенники не могли украсть ваши учетные записи, не имея доступа к вашему мобильному телефону.

Кроме того, в вашей учетной записи электронной почты должна быть включена многофакторная аутентификация, поскольку, как только злоумышленники получают доступ, это значительно упрощает кражу других учетных записей, которыми вы владеете». ***(Lawrence Abrams. Phishing attacks are targeting your social network accounts // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/phishing-attacks-are-targeting-your-social-network-accounts/). 24.09.2020).***

***

«В свободном доступе была обнаружена база данных, не защищенная паролем и шифрованием, содержащая огромное количество информации, относящейся к пользователям сайтов знакомств по всему миру. База, развернутая на Elastcisearch, принадлежала компании Mailfire, базирующейся на Кипре и разрабатывающей маркетинговые инструменты. Обнаруженная база использовалась для работы инструмента отправки уведомлений о получении новых сообщений в приватных чатах сайтов знакомств.

На данный момент оценивается, что пострадало более 100 000 пользователей. База весила 882 ГБ и содержала более 370 миллионов записей. Среди раскрытой информации были содержимое уведомлений, имена, возраст и даты рождения, пол, адреса электронной почты, местонахождение отправителей сообщений, IP-адреса, изображения и описания профилей. Также были обнаружены переписки между пользователями.

В базе оказались данные с более чем 70 сайтов знакомств. Среди них были как самые известные, так и более специфичные, как например для знакомства с

азиатками или колумбийками, или премиальный сайт для людей старшего возраста». ***(Крупная утечка данных с более 70 сайтов знакомств // SecureNews (https://securenews.ru/major-data-breach-from-over-70-dating-sites/). 14.09.2020).***

***

«Исследователи информационной безопасности обнаружили несколько уязвимостей в государственной системе слежения за COVID-19, из-за которых данные более 8 миллионов индийцев оказались под угрозой.

Проблемы в системе наблюдения за обстановкой с COVID-19 индийского штата Уттар-Прадеш были обнаружены специалистами из vpnMentor 1 августа 2020 года. 10 августа специалисты связались с представителями правительства штата, в том числе с органами защиты от киберпреступлений. Устранить недостатки получилось к 10 сентября.

Обнаружилось две большие уязвимости. Первая — незащищенный git репозиторий с исходным кодом системы и незашифрованными доступами к админке. Пароли хранились зашифрованными по MD5, но отдельной колонкой шли в открытом виде. Вторая — собрание CSV файлов, не защищенных паролями, с ежедневными отчетами о состоянии пациентов и их данными.

Персональные данные пациентов из файлов содержали имена, адреса, номера телефонов, диагнозы, симптомы и некоторые медицинские записи». ***(Данные миллионов индийцев, больных COVID, пострадали из-за утечки // SecureNews (https://securenews.ru/data-of-millions-of-indians-with-covid-affected-by-leak/). 24.09.2020).***

***

«В этом году компания Warner Music Group стала жертвой утечки информации. В период с 25 апреля по 5 августа персональные данные клиентов компании находились в открытом доступе, включая имена, адреса электронной почты, телефонные номера, адреса выставления счета, адреса доставки, номера кредитных карт, их даты истечения и CVC и CVV коды.

Юридическая компания Morgan & Morgan подала в суд групповой иск на Warner Music Group. Истцами стали Леви Комбс из Огайо и Эстебан Трухильо из Флориды, которые приобретали продукцию компании в Июле и Мае этого года. В начале сентября они оба получили уведомление от WMG, сообщающее об утечке персональных данных. При этом в августе данные карт, которые истцы использовали для оплаты, были дважды использованы неизвестными неавторизованными лицами для оплаты неких покупок. Одну из попыток банк отклонил как подозрительную. Истцы обвиняют компанию в ненадлежащем обеспечении безопасности персональных данных клиентов». ***(На компанию Warner Music Group подали групповой иск // SecureNews (https://securenews.ru/class-action-filed-against-warner-music-group/). 17.09.2020).***

***

«…Незащищенная база данных предоставила пользователям мобильного приложения поисковой системы Microsoft Bing

конфиденциальные данные, включая их координаты местоположения, условия поиска в виде открытого текста и многое другое.

Хотя никакая личная информация, такая как имена, не была раскрыта, исследователи с Wizcase утверждали, что было доступно достаточно данных, чтобы можно было связать эти поисковые запросы и местоположения с идентификаторами пользователей, что дает злоумышленникам информацию, готовую для атак шантажа, фишинга и многого другого.

Данные относились к версии Microsoft Bing для мобильных приложений, размещенной на сервере размером 6,5 терабайт (ТБ), принадлежащем Microsoft. Исследователи полагают, что сервер был защищен паролем до 10 сентября, за два дня до того, как они обнаружили проблему 12 сентября. Microsoft была предупреждена об обнаруженных данных 13 сентября и обеспечила безопасность сервера 16 сентября.

Хотя они не подсчитали, сколько пользователей конкретно пострадали, исследователи отметили, что только в Google Play было загружено более 10 миллионов приложений Bing, при этом миллионы мобильных поисковых запросов выполнялись ежедневно.

«Основываясь на огромном количестве данных, можно с уверенностью предположить, что любой, кто выполнил поиск в Bing с помощью мобильного приложения, когда сервер был открыт, подвергается риску», - сказал Чейз Уильямс, исследователь Wizcase, в понедельник. «Мы видели записи о поисках людей из более чем 70 стран».

Но когда Threatpost обратился в Microsoft за комментариями, компания заявила, что объем предоставленных данных был «небольшим».

«Мы исправили неверную конфигурацию, из-за которой открывался небольшой объем данных поискового запроса», - сказал представитель Microsoft. «После анализа мы определили, что раскрытые данные были ограничены и не идентифицированы».

В дополнение к поисковым запросам пользователей, которые были в виде открытого текста, сервер также показал время выполнения поиска, токены уведомлений Firebase (позволяющие разработчикам отправлять уведомления на определенные устройства), модели устройств, частичный список URL-адресов, посещенных с результаты поиска, данные купона, которые включали информацию о том, когда был скопирован код купона, данные операционной системы и уникальные идентификационные номера (включая ADID, который является уникальным идентификатором для учетной записи Microsoft, deviceID и devicehash).

Исследователи также обнаружили, что были раскрыты точные данные о местоположении (в пределах 500 метров) - если разрешение на определение местоположения разрешено пользователями в приложении.

«Хотя отображаемые координаты неточны, они все же дают относительно небольшой периметр того, где находится пользователь», - заявили исследователи. «Просто скопировав их на Google Maps, можно будет использовать их, чтобы найти владельца телефона».

Следует отметить, что личная информация пользователей Bing, включая их имена, не была раскрыта; По словам исследователей, пользователи, которые вводили поисковые запросы в приватном режиме, были в безопасности от инцидента.

Исследователи также утверждают, что в период с 10 по 12 сентября по 14 сентября сервер подвергся атаке «Мяу». Атака Meow - это продолжающиеся атаки, которые начались ранее в июле и привели к безвозвратному удалению 1000 незащищенных баз данных. По словам исследователя Боба Дайченко, в результате нападения слово «мяу» стало его единственной визитной карточкой. Хакеры Meow также недавно атаковали сервер Mailfire, который был неправильно настроен и оставлен открытым.

«Из того, что мы видели, в период с 10 по 12 сентября сервер подвергся атаке Meow, в результате которой была удалена почти вся база данных», - сказали исследователи Wizcase. «Когда мы обнаружили сервер 12-го числа, с момента атаки было собрано 100 миллионов записей. 14 сентября на сервер произошла вторая атака Meow».

Threatpost обратился к Wizcase и Microsoft за дальнейшими комментариями по поводу этой атаки.

Исследователи предупредили, что помимо хакеров Meow, эти данные потенциально могут быть доступны другим типам хакеров и мошенников, что может привести к различным шантажистским и фишинговым атакам на пользователей мобильного приложения Bing, особенно когда речь идет о поисковых запросах.

«Будь то поиск контента для взрослых, обман другого значимого человека, крайние политические взгляды или сотни неприятных вещей, которые люди ищут в Bing, - говорят исследователи, - как только хакер получит поисковый запрос, можно будет узнать его идентичность благодаря всей информации, доступной на сервере, что делает их легкой целью для шантажа».

По словам исследователей, раскрытие данных о местоположении также может открыть жертвам физические нападения или ограбления.

«Киберпреступник будет не только знать распорядок дня пользователей, но и на основе поисковых запросов может получить информацию о том, есть ли у вас при себе деньги или дорогие вещи», - заявили они. «Например, если кто-то будет искать, где купить дорогой предмет или где можно найти магазин, злоумышленник может быть готов украсть этот предмет». ***(Lindsey O'Donnell. Unsecured Microsoft Bing Server Leaks Search Queries, Location Data // Threatpost (https://threatpost.com/microsoft-bing-search-queries/159407/). 21.09.2020).***

***

«Социальная инженерия и ошибки сотрудников приводят к нарушениям в работе Администрации ветеранов и Национальной службы здравоохранения.

Пара случаев утечки данных, связанных со здравоохранением, в крупных государственных учреждениях затронула десятки тысяч людей.

Во-первых, кибератака на Департамент по делам ветеранов США (VA) затронула около 46 000 ветеранов, раскрывая их финансовую информацию. И еще один инцидент, произошедший в Национальной службе здравоохранения Великобритании, раскрыл личную информацию 18 105 граждан Уэльса.

Ветеринары поймали на финансовых нарушениях

В первом случае внутренний инструмент, используемый Центром финансовых услуг VA (FSC), был взломан и использовался для перехвата и кражи средств, которые были зарезервированы в качестве платежей местным поставщикам медицинских услуг, говорится в сообщении. Покрытие VA этими платежами обрабатывается программным инструментом, который содержит финансовые данные ветеранов, номера социального страхования и многое другое.

«Воздействие могло быть намного больше. Скорее всего, была применена технология безопасности, которая обнаружила большое количество изменений записей в этом событии, поскольку злоумышленник редактировал отдельные финансовые записи, чтобы отклонить платежи», - сказал Илья Сотников, вице-президент по управлению продуктами в Netwrix по электронной почте. «Каждый раз, когда наблюдается интенсивная, необычная деятельность, вероятность нарушения высока».

FSC отключил приложение после обнаружения несанкционированного доступа - сроки, когда произошло нарушение, не указаны.

«Предварительная проверка показывает, что эти неавторизованные пользователи получили доступ… с помощью методов социальной инженерии и использования протоколов аутентификации», - говорится в пресс-релизе агентства. «Чтобы предотвратить любой неправомерный доступ к информации и ее изменение в будущем, доступ к системе не будет возобновлен до тех пор, пока Управление информационных технологий VA не завершит всестороннюю проверку безопасности».

FSC уведомляет затронутых ветеринаров, а также ближайших родственников умерших.

«Слишком рано говорить, сыграли ли новые конфигурации, связанные с переходом на работу из дома, роль в взломе VA, но это может быть хорошим напоминанием для других компаний о необходимости пересмотреть решения, принятые в марте и апреле, поскольку они быстро переходили на новые способы оставаться продуктивными», - сказал Сотников. «Поскольку это всего лишь одно из множества нарушений, затрагивающих данные ветеранов, VA необходимо убедиться, что они предпринимают все меры безопасности, необходимые не только для защиты финансовых данных, но и конфиденциальных личных и медицинских данных ветеранов, которых он обслуживает».

Обнаружены пациенты с COVID-19

Между тем, отделение Национальной службы здравоохранения Уэльса объявило, что информация, позволяющая установить личность (PII) жителей Уэльса с положительным результатом на COVID-19, была раскрыта в результате «индивидуальной человеческой ошибки».

Инцидент произошел 30 августа, когда положительные данные о пациентах с коронавирусом были случайно загружены на общедоступный сервер, а не на

правильный сервер, где они были доступны для поиска любым пользователем сайта. Ситуация была исправлена менее чем через 24 часа - и за 20 часов, когда он был в сети, его просмотрели 56 раз, говорится в объявлении Национальной службы здравоохранения Уэльса.

«В большинстве случаев (16 179 человек) информация состояла из их инициалов, даты рождения, географического района и пола, что означает, что риск их установления невысок», - говорится в заявлении. «Однако для 1926 человек, живущих в домах престарелых или других закрытых помещениях, таких как поддерживаемое жилье, или жителей, которые имеют тот же почтовый индекс, что и эти настройки, информация также включала название учреждения. Таким образом, риск идентификации для этих людей выше, но все еще считается низким».

На данном этапе нет доказательств того, что данные были использованы не по назначению, но Национальная служба здравоохранения Уэльса начала расследование. Он также изучает меры по предотвращению подобного рода ошибок в будущем.

«Хотя недавняя утечка данных, позволяющих установить личность жителей Уэльса, как было обнаружено Службой общественного здравоохранения Уэльса, не является необычным эксплойтом или злонамеренной уловкой, заявление о раскрытии информации примечательно», - сказал Майк Кайзер, старший стратег по безопасности и евангелист SailPoint. «Он ясен, своевременен и принимает на себя ответственность за сбой: редкая тройка уведомлений о нарушениях. Часто задаваемые вопросы особенно полезны, поскольку многие люди могут не иметь склонности разбирать официальные заявления».

Он добавил: «В записке даже есть прямая ссылка на общедоступную систему, через которую данные были разглашены по ошибке. Демонстрация прозрачности и подотчетности посредством четкой и честной коммуникации необходима для того, чтобы общественность могла доверять организациям свои личные данные. Раскрытие информации, подобное этому, демонстрирующее приверженность этическому подходу, заслуживает похвалы». ***(Tara Seals. Data Breaches Expose Vets, COVID-19 Patients // Threatpost (https://threatpost.com/data-breach-duo-vets-covid-19-patients/159283/). 15.09.2020).***

***

«Житель Великобритании Дэнни Холл (Danny Hall) встретил не в самом лучшем расположении духа — приложение Instagram на его смартфоне перестало принимать привычный пароль. Попытки восстановить доступ к учетной записи не привели к успеху, а позднее выяснилось, что аккаунт принадлежит другому человеку из Лос-Анджелеса.

«На 99,9% уверен, что я не попался на фишинг. К тому же я не получал запрос на подтверждение двухфакторной аутентификации. Instagram тоже не присылал никаких уведомлений об изменении адреса электронной почты», — написал Холл.

Холл зарегистрировался в Instagram 10 лет назад, когда сервис только начал работать, и успел получить профиль с адресом @danny. Он отметил, что регулярно получал спам и письма о попытках зайти в профиль или сбросить пароль, поэтому

аккаунт был защищён «сильным случайным паролем» и двухфакторной аутентификацией

Его девушка связалась с новым владельцем страницы. Тот сообщил, что заполучил аккаунт с помощью друга, который работает в Facebook. Затем он удалил переписку. «Да, звучит как бред, но я не представляю другого способа получить доступ к учётной записи. Даже если у вас есть мой пароль, я получу уведомление о попытке входа», — отметил Холл.

По словам пострадавшего, обращения в службу поддержки Instagram и Facebook ни к чему не привели. На очередной запрос ему ответили, что проблема решена, хотя аккаунт с архивом фотографий и переписок за десять лет все еще находился в руках неизвестного жителя Лос-Анджелеса.

На тред Холла откликнулся глава Instagram Адам Моссери, он попросил написать ему в личные сообщения. 28 сентября Холл написал, что ему вернули страницу, все его публикации сохранились». ***(Глава Instagram помог вернуть пользователю аккаунт, украденный сотрудником Facebook // SecurityLab.ru (https://www.securitylab.ru/news/512525.php). 28.09.2020).***

***

Кібербезпека Інтернету речей

«Современные технологии улучшают и упрощают нам жизнь. Это удобно, когда можно дать голосовую команду аудиосистеме и она выберет и воспроизведет любимый трек, заказать что-нибудь в Интернете, используя только голос или попросить холодильник сообщить, когда закончатся запасы еды, а также настроить офисный принтер, чтобы он сам диагностировал и автоматически запрашивал обслуживание у поставщика. Еще каких-то 10-15 лет назад, все вышеперечисленное можно было наблюдать только в фантастических фильмах. Сейчас – это реальность.

Подобные функции стимулируют спрос на умные офисы, умные дома, умную технику, умные здания и умные города - все они связаны через Интернет вещей (IoT).

Интернет вещей - это сеть физических объектов, оснащенных датчиками, программным обеспечением и другими технологиями для обмена данными с другими устройствами и системами через Интернет. К ним относятся встроенные системы, беспроводные сенсорные сети, системы управления, системы автоматизации дома и зданий, а также устройства для умного дома, смартфоны и интеллектуальные колонки.

По данным Transforma Insights, исследовательской компании по цифровой трансформации, в конце 2019 года в мире было 7,6 миллиарда активных устройств Интернета вещей, а к 2030 году их будет 24,1 миллиарда.

Плюшевые мишки тоже подключены к Интернету?

Безусловно, побуждаемые необходимостью работы на дому в 2020 году, люди подключили к своим корпоративным сетям множество некоммерческих

устройств. Некоторые из них предсказуемы, а другие могут вызывать удивление и улыбку. Например, плюшевые мишки и другие игрушки, спортивное оборудование, такое как тренажеры, игровые устройства и автомобили, согласно отчету международной компании Palo Alto Networks по безопасности Интернета вещей за 2020 год.

Растущее количество и разнообразие устройств, подключенных к сетям IoT, постепенно усложняют реализацию кибербезопасности, поскольку каждое устройство является потенциальным слабым местом.

Например, можно взломать большое количество подключенных автомобилей, чтобы закрыть города, вызвав затор.

Умные дома и даже целые города могут быть взломаны посредством проникновения в автоматизированные системы, управляющие системами отопления, вентиляции и кондиционирования, пожарной сигнализацией и другой важной инфраструктурой.

Сообщается, что киберпреступники проникали в дома через различные интелектуальные устройства, например, умные термостаты, чтобы терроризировать семьи, дистанционно включая отопление; или несанкционированный доступ к домашним камерам видеонаблюдения и умным колонкам, подключенным к Интернету.

Последствия взлома, вероятно, будут наиболее серьезными в сфере здравоохранения, где отказ оборудования или потеря контроля над ним представляют опасность для жизни.

«Подключенные медицинские устройства - от инфузионных насосов с поддержкой Wi-Fi до интеллектуальных машин МРТ - увеличивают площадь атак на устройства, обменивающихся информацией, и создают проблемы безопасности, включая риски конфиденциальности и возможное нарушение правил защиты данных», - пишет Анастасиос Арампацис, представитель поставщика средств безопасности Tripwire.

За кибербезопасность в IoT отвечают руководители

Итак, кто будет отвечать за кибербезопасность в сети IoT? Продавцы индивидуальной техники или оборудования? Тот, кто владеет или управляет сетью? Компания или организация, использующие сеть IoT?

Глобальная исследовательская и консалтинговая компания Gartner прогнозирует, что к 2024 году 75% руководителей будут нести персональную ответственность за атаки на то, что Gartner называет киберфизическими системами (CPS).

Gartner определяет CPS как «системы, которые спроектированы для координации измерений, вычислений, управления, сетей и аналитики для взаимодействия с физическим миром, включая людей».

Эти системы «лежат в основе всех подключенных ИТ, операционных технологий (OT) и Интернета вещей (IoT), где решения по безопасности охватывают как кибернетический, так и физический мир, такой как ресурсоемкие, критически важные инфраструктуры и среды клинического здравоохранения».

OT состоит из аппаратного и программного обеспечения, которое обнаруживает или вызывает изменения в промышленном оборудовании, активах, процессах и событиях посредством прямого мониторинга и/или контроля.

Другими словами, к 2024 году 75% руководителей могут нести ответственность за сбои в безопасности Интернета вещей.

Почему генеральные директора? Как написала вице-президент по исследованиям Gartner Кателл Тилеманн, регулирующие органы и правительства резко ужесточат правила и нормы, регулирующие CPS в ответ на рост серьезных инцидентов, возникающих из-за неспособности защитить CPS. «Скоро генеральные директора не смогут сослаться на незнание или прятаться за страховыми полисами».

Привлечение генеральных директоров к ответственности «является вполне вероятной возможностью и согласуется с тем, как они несут ответственность за точность и законность своих финансовых операций», - говорит Перри Карпентер, директор по стратегии на тренинге по вопросам безопасности KnowBe4.

Национальная ассоциация корпоративных директоров (NACD) «понимает, что безопасность IoT, а в более широком смысле, кибербезопасность, должны быть проблемой, которая поднимается даже до уровня Совета директоров», - сказал Карпентер.

Компании могут покупать киберстрахование, но полисы киберстрахования «печально известны тем, что не выплачивают страховые выплаты, если компания не соответствует высоким стандартам безопасности», - отметил Карпентер.

Кроме того, «регулирующие органы не будут торопиться предлагать легкие выходы для руководителей и компаний, которые могут проявить явную халатность».

Возможен ли подход, основанный на оценке риска?

Глобальная консалтинговая компания McKinsey&Co обнаружила, что предприятия стремятся принять подход к кибербезопасности, основанный на оценке рисков, но он не может обеспечить общую защиту руководителей.

Подходы к информационной безопасности, основанные на оценке рисков, позволяют организациям применять стратегии, адаптированные к их уникальной операционной среде, ландшафту угроз и бизнес-целям, согласно CDW, которая предоставляет технологические решения для бизнеса, правительства, образования и здравоохранения в США, Великобритании и Канаде.

Они позволяют пользователям «понять влияние действий по снижению рисков, обеспечивая всестороннее представление о рисках и заполняя пробелы, которые могут быть в альтернативных подходах к безопасности. Использование подхода, основанного на оценке рисков, четко вписывается в стратегии управления рисками предприятия (ERM), что приемлимо для большинства организаций».

Широко признано, что полностью защищенной системы не существует, так что не будет ли правльным решением возлагать ответственность на генерального директора за отказ CPS?

«Дело не в 100% защите, - сказал Карпентер, - а в том, чтобы обеспечить должную осторожность при проектировании систем. Руководители не могут просто разводить руками и использовать [тот факт, что 100% безопасности не существует]

в качестве оправдания, они должны строить стратегию с учетом безопасности и устойчивости».

Как сделать сети Интернета вещей более безопасными

Palo Alto Networks рекомендует следующие шаги для защиты сетей IoT:

Используйте обнаружение устройств, чтобы получить подробную и актуальную инвентаризацию количества и типов устройств, подключенных к вашей сети IoT, их профилей риска и их доверенного поведения;

Сегментируйте свою сеть, чтобы устройства Интернета вещей находились в их собственных строго контролируемых зонах безопасности, отделяя их от IT-активов;

Принять методы защиты паролей, заменив пароль по умолчанию для вновь подключенных устройств IoT на безопасные, соответствующие корпоративным политикам пароли;

Продолжайте исправлять и обновлять прошивку, когда это возможно;

Активно отслеживайте устройства IoT в любое время.

«Защита сетей IoT требует сочетания покупки продуктов, которые являются безопасными по своей конструкции, и применения целостного подхода к безопасности», - заявила Андреа Каркано, соучредитель операционных технологий (OT) и фирмы по обеспечению безопасности Интернета вещей Nozomi Networks.

«IT-специалисты больше не могут просто беспокоиться о безопасности и возможности подключения своих IT-сетей, - сказал Каркано. «Теперь они должны думать о безопасности своих кибер и физических систем». ***(Романов Роман. В ближайшем будущем за кибербезопасность Интернета вещей будут нести ответственность руководители компаний // Internetua (https://internetua.com/v-blizjayshem-buduschem-za-kiberbezopasnost-interneta-vesxei-budut-nesti-otvetstvennost-rukovoditeli-kompaniy). 25.09.2020).***

***

Кіберзлочинність та кібертероризм

«Основні тенденції розвитку кіберзлочинності в наступному десятилітті…

На сьогодні у світі налічується близько шести тисяч тіньових ринків, де продають 45 тисяч продуктів або послуг у сфері кіберзлочинності. І один із найшвидше зростаючих ринків — послуги зі зламу. Популярні шкідливі програми в мережі включають веб-ін'єкції (набори інструментів і інфраструктуру), куленепробивний хостинг, оренду ботнетів тощо. Крадіжка інтелектуальної власності, зокрема й військових розробок, — це як мінімум чверть усіх кіберзлочинів. Але це нині. А погляньмо, що буде в майбутньому.

От деякі прогнози щодо розвитку технологій до 2025 року:

- розумний транспорт стане повсякденням до 2025 року. Він включатиме не тільки автомобілі, але й цілісну транспортну систему, яка поєднуватиме засоби пересування, інфраструктуру та людей;

- технології штучного інтелекту зможуть ліпше реагувати на ситуації на дорогах і допомагатимуть мінімізувати міські затори й оптимізувати трафік;
- мобільний Інтернет 5G буде стандартом. Global Industry Vision прогнозує, що 58% населення світу матиме доступ до мереж 5G до 2025 року;
- поліпшений погляд. Окуляри віртуальної реальності. Звіт Global Industry Vision припускає, що 10% компаній використовуватимуть окуляри віртуальної реальності до 2025 року;
- поява робочих роботів. Прогнозується, що на 10 тисяч працівників до 2025 року припадатиме 103 роботи. Поки що це небагато, але в певних професіях заміщення людей роботами неминуче;
- використання розумних чат-ботів, які розмовляють багатьма мовами. 86% великих організацій перейдуть до їхнього використання вже через п’ять років;
- хмарні бізнес-сервіси. Передбачається, що до 2025 року 85% сервісів перейдуть у хмару;
- 90% користувачів, які користуються «розумними» гаджетами, зможуть використовувати персональних помічників, оснащених штучним інтелектом;
- трафік обміну інформацією до 2025 року зросте більш як у шість разів.

Що всі ці тенденції означають? Якщо в 2000-х основним проявом кіберзлочинності були віруси, передані через комп’ютери користувачів, а в 2010-х, крім пристроїв користувачів, уже активно атакували сервери та програмне забезпечення, то 2020-ті роки будуть справжнім Клондайком для хакерів. Спектр уразливості або точок входу буде просто величезним!

Атаки на автомобілі й системи керування пересувними апаратами, GPS-навігацію, мобільний Інтернет, міські системи у керування інфраструктурою і транспортом, станції передачі трафіку, супутники, планшети. Атаки на мобільні пристрої користувачів, окуляри віртуальної реальності та інші «розумні» і не дуже побутові й переносні пристрої. Впроваджуватимуться шкідливі програми в сервіси керування роботами або чат-ботами, що може завдати суттєвої шкоди репутації компаній. Ну й, звичайно, неминучі атаки на дата-центри, канали передачі даних і сервіси, які дозволять одразу одержати дані величезної кількості користувачів. Окремо тут можна також виділити атаки на державні реєстри.

До додаткових загроз можна віднести крадіжку персональних даних із «розумних» пристроїв, використання гаджетів для зламу інших пристроїв власника та, звичайно ж, усе зростаючий обсяг інформаційного спаму з усіх боків.

При цьому ми всі маємо розуміти, що кількість пристроїв збільшиться в кілька разів у найближчі два-три роки. А ціновий чинник зробить масовими саме слабко захищені пристрої. Тобто дані персональних користувачів будуть уразливими як ніколи. Тим більше що вже успішно випробувано технології і формування відбитків пальців, і підміни обличчя.

Є ще один дуже важливий аспект — кількість сервісів, якими ми користуємося. Вона зростає з кожним днем. При цьому більшість стартапів використовують украй простий процес реєстрації у своїх сервісах: логін і пароль. І, гадаю, більшість із вас не використовують для реєстрації багато email-адрес, як і різні паролі. Скільки у вас паролів для входу у ваші численні сервіси? Один-два, максимум три. Тобто, зламавши один із ваших облікових записів, хакер із великою

ймовірністю одержить доступ і до інших ваших облікових записів, зокрема й до фінансових даних. З урахуванням того, що багато сервісів зберігають базові елементи оплати всередині систем, то під загрозою опиняться й усі банківські картки, які ви використовуєте в мережі.

До цього треба додати ще кілька важливих складових. По-перше, мотивація хакерів зазвичай сильна, оскільки можливий приз може бути дуже цінним. По-друге, хакери теж поліпшують технології штучного інтелекту й використовують свої напрацювання, найчастіше навіть раніше, ніж фахівці з кібербезпеки. По-третє, уже зараз на ринку спостерігається дефіцит кадрів із кібербезпеки, і цей дефіцит через великі технологічні складнощі в цій сфері легко не заповниться. По-четверте, як відомо, тактика нападу завжди більш виграшна, ніж тактика чистого захисту.

Тут, звичайно ж, постає конкретне запитання: що робити? Відповідь відрізнятиметься для різних потенційних об'єктів атак: урядів, корпорацій і персональних користувачів.

Урядам потрібне зростання зусиль із впровадження суворих правил для обмеження обсягу даних, які збирають пристрої IoT (Інтернету речей), у таких галузях, як банківська сфера, фінансові сервіси, охорона здоров'я та роздрібна торгівля. Це як стимулюватиме зростання ринку рішень для кібербезпеки, так і мінімізуватиме зростаючі загрози від низько захищених пристроїв. Треба також підвищити вимоги до безпеки об'єктів критичної інфраструктури й посилити покарання за кіберзлочини.

Організаціям треба формувати центри забезпечення безпеки. Причому нині в тренді формування таких центрів не на майданчиках замовника, а в хмарних сховищах. Дедалі більше великих і середніх організацій відкривають для себе керовані послуги, які надають сервіс-провайдери, з надання сервісів інформаційної безпеки на комерційній основі. Загалом через брак якісних фахівців з кібербезпеки та їхню дорожнечу це розумне рішення, зокрема і з економічного погляду. Слід використовувати машинне навчання, яке дає змогу вибудовувати більш гнучкі й адаптивні методики виявлення загроз. Водночас не варто забувати про те, що машинне навчання можна використати і з погляду роботи з алгоритмами організації. Щойно в шахраїв з'явиться розуміння про те, яким чином алгоритм було навчено, в них одразу ж з'являться важелі маніпуляції ним.

Персональним користувачам мережі треба передусім усвідомлювати загрози безпеки та мінімізувати ризики. Якщо ви платите з допомогою телефону, придумайте складний пароль для свого мобільного пристрою. Аналіз, проведений Монобанком, показав, що 45% користувачів узагалі не мали паролів на телефон! Це просто катастрофічний результат. Для мінімізації ризиків також слід мати вхід у банківську систему або інші фінансові сервіси як мінімум з окремим паролем, що не використовується в соціальних мережах або інших електронних сервісах. Ну й за можливості в мережу не виставляти карток, на які заходять гроші. Ліпше мати ще одну картку, на яку можна перерахувати суму для оплати й поповнювати її за потреби, виставляючи на ній кредитний ліміт, що дорівнює нулю. Крім того, попри те, що основна маса сучасних мобільних банківських додатків дозволяють використовувати біометрію (відбиток пальця, обличчя, зліпок голосу) для входу, це спрощена автентифікація як для користувача, так і для зловмисників. Додаток у

цьому разі змушений зберігати всі автентифікаційні зліпки даних на самому пристрої…». ***(Данило Монін. Ризики й виклики нового часу // Дзеркало тижня. Україна (https://zn.ua/ukr/macrolevel/riziki-j-vikliki-novoho-chasu.html). 05.09.2020).***

***

«Компания «Elcore Украина», официальный дистрибьютор Trend Micro, сообщила о том, что вендор представил новый отчет о глобальной теневой инфраструктуре.

Опубликованы обнаруженные Trend Micro сведения о сложном цикле монетизации преступных действий, связанных со взломом, использованием и сдачей в аренду локальных и облачных серверов организаций. Эти данные были получены в ходе работы над вторым из трёх докладов компании об инфраструктуре киберпреступности, посвящённым тому, как работает рынок нелегального хостинга.

Кроме этого, исследователи Trend Micro выявили, например, такой факт: одним из сигналов для специалистов по ИТ-безопасности, говорящим об активности киберпреступников, должно стать обнаружение операций майнинга криптовалюты с использованием инфраструктуры организации. Хотя криптомайнинг сам по себе не нарушает бизнес-процессы и не приводит к финансовым потерям, ПО для него обычно используется хакерами для получения прибыли от скомпрометированных серверов организации, которые «простаивают», пока киберпреступники разрабатывают более перспективные с точки зрения заработков схемы. К числу таковых относятся, например, кража ценных данных, продажа доступа к серверам другим хакерам и подготовка к целевым атакам с использованием программ-вымогателей. Любые серверы, на которых обнаружены криптомайнеры, рекомендуется немедленно отключить от инфраструктуры и обследовать на предмет возможных противозаконных действий.

«Рынок нелегального хостинга предлагает своим клиентам широкий спектр инфраструктурных решений для разного рода кампаний, включая абьюзоустойчивый хостинг, услуги анонимизации, предоставление доменных имён и предварительно скомпрометированные корпоративные ресурсы, — отметил Боб Макардл (Bob McArdle), директор направления перспективного исследования угроз в Trend Micro. — Наша цель — повысить уровень осведомлённости об инфраструктуре, которую используют киберпреступники, чтобы помочь правоохранительным органам, нашим клиентам и другим исследователям в этой области лишить злоумышленников инструментов совершения правонарушений и увеличить их операционные расходы».

В докладе перечислены доступные на сегодняшний день услуги рынка нелегального хостинга, а также приведены технические подробности того, как они функционируют и как киберпреступники используют их для ведения своей деятельности. Также в нём содержится подробное описание типичного жизненного цикла скомпрометированного сервера — от первоначального взлома до финальной атаки.

Облачные серверы особенно уязвимы для компрометации и использования в инфраструктуре нелегального хостинга, так как они часто защищены хуже локальных.

Боб Макардл также отметил: «Взломав локальные или облачные корпоративные активы, хакеры смогут в дальнейшем свободно их использовать. Поэтому на практике в первую очередь стоит обратить внимание именно на те активы, которые проще всего скомпрометировать».

Киберпреступники используют уязвимости в серверном ПО, атаки методом перебора для взлома учётных данных или кражу этих учётных данных при помощи фишинга, чтобы развернуть в сети организации вредоносное ПО. Также они могут взломать программное обеспечение для управления инфраструктурой, похитив ключи облачного API, что предоставит им доступ к ресурсам и возможность создания новых виртуальных машин.

После взлома доступ к этим облачным серверам будет продан на подпольных форумах, специализированных торговых площадках и даже в социальных сетях для использования в разнообразных атаках…». ***(Trend Micro представила исследование о скомпрометированных хакерами локальных и облачных серверах // Компьютерное Обозрение (https://ko.com.ua/trend_micro_predstavila_issledovanie_o_skomprometirovannyh_hakerami_lokalnyh_i_oblachnyh_serverah_134420). 08.09.2020).***

***

«Фирма Defiant, разработчик межсетевого экрана Wordfence, сообщила о внезапной активизации хакеров, которые на прошлой неделе атаковали миллионы сайтов WordPress.

Эти атаки использовали незакрытую уязвимость в File Manager, популярном подключаемом модуле для WordPress, установленном более чем на 700 тыс. сайтов.

Данная уязвимость открывает возможность неавторизованной загрузки файлов, в том числе вредоносных, на сайты, работающие со старой версией File Manager.

В случае если начальная атака оказалась успешной, и сайт с устаревшим плагином обнаружен, хакеры загружают на сервер жертвы веб-оболочку, замаскированную под файл изображения. Действуя через эту веб-оболочку они могут захватить управление над уязвимым веб-сайтом и добавить его в ботнет.

В общем с 1 сентября, когда эти атаки были впервые обнаружены, брандмауэр Defiant блокировал диверсии против более 1,7 млн сайтов, в том числе 1 млн атак только в пятницу, 4 сентября.

Число 1,7 млн это более половины сайтов WordPress, защищённых Wordfence, реальный же размах атак по мнению представителей Defiance, должен быть ещё больше.

Команда разработчиков File Manager подготовила программный патч в тот же день, когда узнала об атаках, однако, как это бывает обычно, далеко не все владельцы сайтов устанавливают обновления безопасности своевременно. Поэтому, начиная с версии WordPress 5.5, вышедшей в августе, этот движок управления контентом дополнен функцией автоматической установки обновлений

для тем и подключаемых модулей». ***(Ошибка в плагине WordPress стала причиной атак на миллионы веб-сайтов // Компьютерное Обозрение (https://ko.com.ua/oshibka_v_plagine_wordpress_stala_prichinoj_atak_na_milliony_veb-sajtov_134402). 07.09.2020).***

***

«В течение прошлой недели более десятка европейских интернет-провайдеров (ISP) подверглись DDoS-атакам, нацеленным на их инфраструктуру.

Среди пострадавших ISP, бельгийский EDP, французские Bouygues Télécom, FDN, K-net, SFR, и голландские Caiway, Delta, FreedomNet, Online.nl, Signet и Tweak.nl.

Атаки продолжались не более суток и в конце-концов были отражены, но до тех пор службы ISP были парализованы.

Подробности этих инцидентов сообщила NBIP, некоммерческая организация, основанная голландскими ISP для борьбы с DDoS-атаками и попытками прослушивания коммуникаций со стороны правительства.

«Множественные атаки были нацелены на маршрутизаторы и DNS-инфраструктуру провайдеров из Бенилюкса, — сказал представитель NBIP. — Большинство из них были атаками усилением DNS и LDAP. Некоторые длились более 4 часов и по интенсивности приближались к 300 Гб/с.»

ZDNet отмечает тот факт, что 28 августа, когда началась эта серия атак, была обнародована информация о преступной группе, занимавшейся вымогательством путём DDoS-атак финансовых учреждений по всему миру, включая MoneyGram, YesBank India, Worldpay, PayPal, Braintree и Venmo.

Возможно это лишь совпадение, однако атаки на финансовые сервисы прекратились с началом атак европейских ISP. Кроме того, источники, следившие за этой преступной группировкой, информировали, что среди её жертв было несколько ISP из Юго-Восточной Азии». ***(В Европе прошла волна DDoS-атак на интернет-провайдеров // Компьютерное Обозрение (https://ko.com.ua/v_evrope_proshla_volna_ddos-atak_na_internet-provajderov_134392). 04.09.2020).***

***

«Компания Check Point Softw are Technologies изучила домены, связанные со школьной тематикой и выявила всплеск интереса хакеров. Так, за последние три месяца исследователи обнаружили более 35149 новых доменов, связанных с темой возвращения в школу. Из них 512 классифицированы как вредоносные, а 3401 – подозрительные. Среднее число подозрительных доменов в пиковое время достигло 356, в то время как среднее значение в апреле-мае составляло 115. Рост активности мошенников пришелся на конец июля начало августа. В этот период количество подозрительных доменов увеличилось почти на 30% за неделю в сравнении с тем же показателем в июне-июле.

Также исследователи Check Point в первом полугодии изучили LMS (Learning Management Systems) – программные решения для организации дистанционного обучения. Некоторые популярные системы используют в качестве дополнительного ПО WordPress. В результате были выявлены недостатки безопасности в трех самых популярных плагинах WordPress: LearnPress, LearnDash и LifterLMS.

Несмотря на то, что уязвимости плагинов уже исправлены, исследователи Check Point предостерегают пользователей от стремления хакеров использовать детей, обучающихся дистанционно, в своих интересах.

Среди основных угроз, которым подвержены школьники, можно выделить следующие:

Zoombombing – незваное присоединение постороннего человека к встрече Zoom с целью ее саботирования. Подобные участники зачатую прибегают к оскорблениям и использованию ненормативного контента, что в свою очередь может травмировать детей.

Кибербуллинг – компрометирование пользователей сети личной информацией и прочими злонамеренными данными. Часто жертвами подобных махинаций становятся пользователи популярных социальных сетей. По данным «Центра исследования случаев кибербуллинга» 37% молодых людей в возрасте от 12 до 17 лет подвергались издевательствам в интернете, из них 30% стали жертвами мошенников более одного раза.

Программы-вымогатели. В большинстве случаев подобные программы распространится с помощью фишинговых писем, которые содержат вредоносный файл или зараженную ссылку. После установки вредоносного ПО на компьютер жертвы программа шифрует данные и требует за них выкуп. Так, в 2019 г. более 1000 школ в США были атакованы программами-вымогателями, которые блокировали доступ к компьютерной системе или отдельным файлам до уплаты выкупа.

Фишинг – вид мошеннической активности, направленный на получение конфиденциальной информации, с помощью рассылки электронных писем с зараженной ссылкой или вложением, в том числе и от лица проверенного отправителя.

Советы учащимся:

Выключайте или блокируйте камеры и микрофоны вне урока. Также убедитесь, что в поле зрения камеры не попадает личная информация;

Переходите по ссылкам, присланным из надежных источников;

Осуществляйте вход в системы напрямую. Например, для входа в школьный портал вбейте его название в поисковой сети и перейдите по официальной ссылке;

Используйте надежные и сложные пароли;

Никогда не делитесь конфиденциальной информацией в сети. Также не рекомендуется хранить личные данные в облачных платформах.

Советы для родителей:

Расскажите детям о фишинге. Объясните им, что не стоит самостоятельно переходить по подозрительным ссылкам, присланным по электронной почте;

Объясните своим детям, что оскорбительные комментарии или шутки в Интернете – это не нормально. В случае, если ребенок стал жертвой кибербуллинга, ему следует немедленно сообщить об этом взрослым;

Донесите до ребенка, что оставлять без присмотра личные устройства – небезопасно. Так повышается шанс стать жертвой мошенников;

Установите параметры конфиденциальности и безопасности на веб-сайтах, доступ к которым не желателен для ребенка;

Повышение информированности. Грамотность в области кибербезопасности – это важный навык, в том числе и для самых маленьких школьников. Инвестируйте время, деньги и прочие ресурсы, чтобы ваш ребенок был осведомлен о потенциальных угрозах и мерах предосторожности.

Советы школам:

Установите антивирусное ПО, а также не забудьте включить автоматическое обновление программы;

Используйте мощные пограничные брандмауэры и интернет-шлюзы для защиты школьных сетей от деятельности мошенников;

Тщательно проверяйте поставщиков платформ для дистанционного обучения;

Постоянно контролируйте все свои системы и анализируйте их на предмет нетипичной активности;

Информируйте сотрудников, а также учащихся об актуальных киберугрозах и мерах предосторожности». ***(Число подозрительных доменов на школьную тематику выросло на 30% // Компьютерное Обозрение (https://ko.com.ua/chislo_podozritelnyh_domenov_na_shkolnuyu_tematiku_vyroslo_na_30_134350). 02.09.2020).***

***

«Шестнадцатилетний школьник из Флориды парализовал на три дня онлайн-школы округа Майами-Дейд с помощью простейшей DDoS-атаки.

Власти арестовали юного хакера, который, по их словам, совершил восемь DDoS-атак на сайты школ My School Online округа Майами-Дейд. Мотивов злоумышленник не назвал. Школьник использовал Low Orbit Ion Cannon (LOIC) — устаревший инструмент DDoS, популярный в прошлом десятилетии среди хакеров.

В расследовании инцидента приняли участие Департамент правоохранительных органов Флориды и ФБР. Найти школьника оказалось просто — он не скрывал реальный IP-адрес. Ученику предъявлены обвинения в совершении преступления с использованием компьютера в попытке мошенничества и вмешательства в деятельность учебного заведения. Хакер признался только в восьми атаках, но власти сообщают о, по меньшей мере, двадцати. Расследование продолжается.

Серия распределенных кибератак типа «отказ в обслуживании» парализовала школьную систему округа и привела к тому, что около 170 тысяч учителей и учеников не смогли выйти на онлайн-занятия. Майами-Дейд — самый густонаселенный округ во Флориде…». ***(Виталий Маршак. Школьник из США парализовал школы простейшей кибератакой // Популярная мезханика***

(https://www.popmech.ru/technologies/news-617033-shkolnik-iz-ssha-paralizoval-shkoly-prosteyshey-kiberatakoy/). 07.09.2020).

***

«Израильская фирма "Tower Semiconductor" (ранее – "TowerJazz"), специализирующаяся на создании чипов, сообщила о том, что её сервера подверглись атаке кибернетического характера…

Пострадавшая компания добавляет, что тесно сотрудничает с правоохранительными органами и экспертами, а также пытается поскорее восстановить работу всех своих систем, ставших целью атаки кибернетических злоумышленников. Между тем, пока что использование некоторых серверов пришлось приостановить, что привело к сворачиванию части операций.

Оценка ущерба, причиненного фирме "Tower Semiconductor", пока что проведена на была. Также представители компании, в прошлом сотрудничавшей даже с НАСА, воздержались от подробностей в связи с осуществленной кибератакой». ***(Производитель чипов подвергся кибератаке // ISRAland Online (http://www.isra.com/news/249997). 07.09.2020).***

****

«Федеральное бюро расследований США выпустило срочное оповещение, предупреждающее предприятия о вымогательской кампании, направленной на организации из разных сфер деятельности по всему миру.

В рамках кампании злоумышленники под видом известных хакерских группировок, таких как Fancy Bear, Cozy Bear, Lazarus Group или Armada Collective, угрожают организациям массивными DDoS-атаками, если те не заплатят выкуп в биткойнах в шестидневный срок. Об этом пишет securitylab.ru.

По данным бюро, атаки начались 12 августа 2020 года, их целью являлись компании в финансовой и туристической сферах, а также предприятия, занимающиеся ретейлом и электронной коммерцией.

В предупреждении ФБР не указывается, какие страны охватывает вредоносная кампания, но, специалисты ИБ-компании Radware говорят, что атаки наблюдаются в странах Северной Америки, Азиатско-Тихоокеанского региона, Европы, Ближнего Востока и Африки.

По данным Radware, размер выкупа варьируется от 10 биткойнов (примерно $102 тыс по текущему курсу) до 20 биткойнов (порядка $205 тыс), причем для каждой жертвы существует отдельный адрес криптовалютного кошелька. Как указывается в требовании выкупа, если компания не заплатит, на нее будет осуществлена DDoS-атака мощностью до 2 Тбит/с.

В ФБР отмечают, что после получения требования некоторые компании действительно подверглись небольшим DDoS-атакам, но в большинстве случаев злоумышленники не выполнили угрозу, если организация не заплатила деньги в срок.

По словам специалистов Akamai, мощность этих демо-атак достигала почти 200 Гбит/с, а сами они были различных типов — ARMS, DNS Flood, GRE Protocol Flood, SNMP Flood, SYN Flood и WSDiscovery Flood.

ФБР советует организациям не платить вымогателям, поскольку это будет только стимулировать дальнейшие атаки. В качестве меры защиты от данной угрозы компаниям рекомендуется использовать сервисы по предотвращению DDoS-атак». ***(ФБР предупреждает о волне кибератак на компании по всему миру // cursorinfo.co.il (https://cursorinfo.co.il/all-news/world-news/world/fbr-preduprezhdaet-o-volne-kiberatak-na-kompanii-po-vsemu-miru/). 07.09.2020).***

***

«Artech Information Systems, одна из крупнейших ИТ-кадровых компаний США, раскрыла утечку данных, вызванную атакой программы-вымогателя, которая затронула некоторые из ее систем в начале января 2020 года.

Artech - это частная фирма с годовой выручкой в 810 миллионов долларов в 2019 году и более чем 10 500 сотрудниками и консультантами в 40 штатах США, Канаде, Индии и Китае.

Компания предоставляет кадровые и кадровые решения, управление программами и государственные услуги, а в ее список клиентов входят более 80 клиентов из списка Fortune 500 и федеральные правительственные учреждения США.

Программа-вымогатель развернута через три дня после первого взлома

Атака вымогателей была обнаружена Artech после обнаружения вымогателей в некоторых системах после сообщений о необычной активности, связанной с одной из учетных записей ее сотрудников.

«В тот же день Artech привлекла ведущую стороннюю фирму по судебным расследованиям для оценки безопасности ее систем и подтверждения характера и масштабов инцидента», - поясняется в письме с уведомлением об утечке данных, отправленном пострадавшим лицам [1, 2].

«15 января 2020 года расследование установило, что неавторизованный субъект имел доступ к определенным системам Artech в период с 5 января 2020 года по 8 января 2020 года».

BleepingComputer узнал об атаке на серверы Artech 11 января 2020 года, когда банда вымогателей REvil (Sodinokibi) утекла 337 МБ файлов, которые, по их утверждениям, были украденными с серверов компании.

«Это небольшая часть того, что у нас есть», - заявили тогда операторы REvil. «Если никаких перемещений не будет, мы продадим оставшиеся, более важные и интересные коммерческие и личные данные третьим сторонам, включая финансовые детали».

BleepingComputer связалась с Artech, чтобы узнать, знают ли они об атаке и заявлениях группы вымогателей, но наши электронные письма были проигнорированы и не получили ответа, пока мы не опубликовали эту статью.

Однако в электронном письме, отправленном BleepingComputer сотрудником Artech, говорилось, что компании пришлось отключить все системы, но она смогла восстановить критически важные службы и серверы из резервных копий.

REvil - это программа-вымогатель как услуга (RaaS), которая взламывает корпоративные сети через открытые службы удаленных рабочих столов и

скомпрометированных поставщиков управляемых услуг, а также с помощью эксплойтов и спама.

Как только они получат доступ к сети жертвы, операторы REvil будут распространять латеральную кражу конфиденциальных данных, чтобы использовать их в качестве рычага давления на жертв, чтобы они заплатили выкуп под угрозой публичной утечки информации.

После получения административного доступа к контроллеру домена и кражи данных с серверов и рабочих станций REvil развертывает полезные нагрузки вымогателей на всех компьютерах в скомпрометированной сети компании.

Личная, финансовая и медицинская информация, раскрытая в результате атаки

В ходе расследования инцидента компания Artech обнаружила личную информацию, информацию о состоянии здоровья и финансовую информацию нескольких лиц, хранящуюся в скомпрометированных системах.

Примерно 25 июня 2020 года, когда компания завершила расследование атаки, она смогла определить лиц, информация которых была затронута во время атаки программы-вымогателя.

«Расследование установило, что на момент происшествия соответствующие файлы могли содержать информацию, включая имя, номер социального страхования, медицинскую информацию, информацию о медицинском страховании, финансовую информацию, информацию о платежной карте, водительские права / государственный идентификационный номер, удостоверение личности государственного образца. номер, номер паспорта, номер визы, электронная / цифровая подпись, имя пользователя и пароль», - сообщает Artech.

Комбинация раскрываемой информации различается для каждого пострадавшего человека в соответствии с письмом компании с уведомлением о нарушении.

После обнаружения атаки Artech изменил учетные данные системы, чтобы защитить свои системы, и начал работать с внешними экспертами по безопасности для улучшения существующих процессов и протоколов безопасности компании.

Artech призывает затронутых лиц, получивших уведомление об утечке данных, следить за выписками по своим счетам на предмет подозрительной активности и проявлять бдительность в отношении попыток мошенничества и кражи личных данных. Компания также предоставляет им бесплатный кредитный мониторинг и услуги по защите личности через Kroll». ***(Sergiu Gatlan. US staffing firm Artech discloses ransomware attack, data breach // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/us-staffing-firm-artech-discloses-ransomware-attack-data-breach/). 11.09.2020).***

***

«Команда исследователей из Comparitech решила расследовать недавний всплеск числа дефейс-атак (тип хакерской атаки, в результате которой веб-страница заменяется на другую, либо меняется ее внешний вид). Рост числа подобных атак стал неожиданностью, так как в последние годы наблюдался

устойчивый тренд к снижению их числа. Но если в июле 2019 их было зафиксировано 300 000 за год, то к маю 2020 — 700 000.

В ходе расследования специалисты Comparitech обнаружили также большое число уязвимостей в популярных CMS — WordPress, Joomla, Drupal и Opencart. Было найдено 89 уязвимостей нулевого дня. По оценкам, на данный момент около 100 000 сайтов используют плагины, имеющие эти уязвимости. Причем большинство из них работают на WordPress (78 430) и Joomla (16 360), меньше на Opencart (6 240) и Drupal (300). Анализ 5 популярных ботов для масс-хакинга показал, что каждый из них мог использовать от 40 до 80 обнаруженных уязвимостей. Причем большое число обнаруженных уязвимостей не зарегистрированы ни в одной соответствующей базе данных. У 5 проанализированных ботов 154 из 280 эксплойтов не имели индекса CVE». ***(Обнаружено 89 критических уязвимостей в CMS платформах // SecureNews (https://securenews.ru/89-critical-vulnerabilities-found-in-cms-platforms/). 09.09.2020).***

***

«Компания Fortinet представляет выводы свежего исследования FortiGuard Labs Global Threat Landscape Report, публикующегося каждые полгода.

«Первые шесть месяцев 2020 года ознаменовались формированием беспрецедентного ландшафта киберугроз. Драматический масштаб и стремительная эволюция методов атаки демонстрируют оперативность противников в изменении своих стратегий с целью максимизации выгоды от текущих событий: усилия сосредоточены вокруг последствий пандемии COVID-19 по всему миру. Никогда еще не существовало такой четкой картины, как сейчас, демонстрирующей необходимость корректировать защитные стратегии организаций в будущем, чтобы в полной мере учитывать периметр сети, распространившийся на дома сотрудников. Для организаций очень важно принять меры по защите своих удаленных работников, помочь им обезопасить свои устройства и домашние сети на длительный период. Разумно было бы рассмотреть возможность принятия такой же стратегии, как та, что мы используем в реальном мире, в отношении и кибервирусов. Киберсоциальное дистанцирование – это в первую очередь осознание рисков и сохранение безопасного расстояния», – Дерек Мэнки, руководитель отдела безопасности и глобальных угроз, FortiGuard Labs.

Анализ угроз, проведенный лабораторией FortiGuard Labs в первой половине 2020 года, демонстрирует драматические масштабы, в которых киберпреступники и субъекты национальных государств использовали глобальную пандемию как возможность для осуществления различных кибератак по всему миру.

Приспосабливаемость противников позволила создать волны атак, нацеленные на страх и неопределенность, обусловленные текущими событиями. Кроме того, внезапный рост количества удаленных сотрудников вне корпоративной сети в одночасье расширил поверхность цифровых атак.

Хотя многие важные тренды ландшафта киберугроз были связаны с пандемией, некоторые из них развивались благодаря собственным движущим

силам. Например, вирусы-вымогатели, направленные на устройства Internet-of-Things (IoT), а также операционные технологии (OT), не ослабевают, а наоборот, развиваются, становясь более целенаправленными и изощренными.

На глобальном уровне большинство угроз прослеживается во всем мире и в различных отраслях промышленности с некоторыми региональными или вертикальными вариациями. Подобно пандемии COVID-19, определенная угроза могла появиться в одной области, но в конечном итоге распространиться почти везде, что означает, что большинство организаций могут рано или поздно с ней столкнуться. Конечно, существуют региональные различия в показателях инфицированности, основанные на таких факторах, как политики, практики или методы реагирования.

Ключевые выводы исследования:

Использование возможностей, открывающихся вследствие глобальных событий. Злоумышленники и раньше использовали новостную повестку как приманку для социальной инженерии, но в первой половине 2020 года это перешло на следующий уровень. От фишеров-опортунистов до интригующих субъектов национального государства – киберпротивники нашли множество способов использовать глобальную пандемию в своих интересах в огромных масштабах. К ним относятся схемы фишинга и компрометации деловой почты, кампании, поддерживаемые на государственном уровне и атаки с целью получения выкупа. Они работали над тем, чтобы максимизировать глобальный характер пандемии, поразившей всех в мире, в сочетании с немедленным расширением площади цифровых атак. Эти тенденции были замечены в других новостях и продемонстрировали, как быстро злоумышленники могут воспользоваться основными событиями с широким социальным влиянием на глобальном уровне.

Периметр становится более личным. Увеличение количества удаленных рабочих мест обусловило драматическое изменение корпоративных сетей почти в одночасье, и киберпреступники сразу же начали использовать эти события как возможность. В первой половине 2020 года попытки эксплойтов против нескольких маршрутизаторов потребительского класса и устройств IoT были на первом месте по обнаружению IPS. Кроме того, Mirai и Gh0st доминировали в наиболее распространенных детекторах бот-сетей, что было вызвано очевидным ростом интереса злоумышленников к старым и новым уязвимостям в продуктах IoT. Эти тенденции примечательны тем, что они демонстрируют, как периметр сети распространился на дом, где злоумышленники пытаются закрепиться в корпоративных сетях, используя устройства, которые удаленные сотрудники могут использовать для подключения к сетям своих организаций.

Браузеры тоже под прицелом. Для злоумышленников переход к удаленной работе стал беспрецедентной возможностью атаковать ничего не подозревающих людей разными способами. Например, вредоносное веб-ПО, используемое в фишинговых кампаниях и других видах мошенничества, превзошло более традиционную электронную почту в качестве пути доставки вредоносов. Фактически, семейство вредоносных программ, которое включает в себя все варианты веб-фишинговых приманок и мошенничества, занимало первое место среди всех вредоносов в январе и феврале и выпало из первой пятерки только в

июне. Это может свидетельствовать о стараниях киберпреступников осуществлять свои атаки в момент, когда люди наиболее уязвимы и легковерны – во время серфинга по сети дома. Веб-браузеры, а не только устройства, также являются основными целями для киберпреступников, возможно, в большей степени, чем обычно, поскольку злоумышленники продолжают атаковать удаленных сотрудников.

Вымогатели никуда не исчезли. Хорошо известные угрозы, такие как вредоносы, нацеленные на получение выкупа, не стали менее заметными в течение последних шести месяцев. Тематические сообщения и вложения по теме COVID-19 использовались в качестве приманки в различных кампаниях по выкупу. Другие вымогатели были обнаружены при перезаписи главной загрузочной записи компьютера (MBR) перед шифрованием данных. Кроме того, участились случаи, когда злоумышленники не только блокировали данные организации-жертвы, но и, в качестве дополнительного рычага воздействия, похищали их, затем угрожая обнародованием. Эта тенденция значительно увеличивает риск того, что организации потеряют бесценную информацию или другие конфиденциальные данные в будущих атаках с применением вымогателей. Ни одна отрасль в мире не избежала подобных атак, и данные демонстрируют, что пятью направлениями, в наибольшей степени подверженными атакам с целью получения выкупа, являются телекоммуникации, Интернет-провайдеры, образовательные учреждения, правительственные и технологические организации. К сожалению, рост числа таких вредоносов, продаваемых в качестве услуги (RaaS), и эволюция определенных вариантов указывает на то, что ситуация с вымогателями не становится менее острой.

OT-угрозы после Stuxnet. В июне исполнилось 10 лет со дня появления Stuxnet, который сыграл важную роль в эволюции угроз для операционных технологий и в обеспечении их безопасности. Сейчас, много лет спустя, сети OT остаются мишенью для преступников. Вирус-вымогатель EKANS, выпущенный в начале этого года, демонстрирует, как злоумышленники продолжают расширять фокус атак с целью получения выкупа и на OT-среды. Кроме того, шпионский фреймворк Ramsay, предназначенный для сбора и эксфильтрации конфиденциальных файлов в сетях с воздушной ловушкой или сетях с ограниченным доступом, является примером того, как злоумышленники ищут новые способы проникновения в такие типы сетей. Распространенность угроз, направленных на системы диспетчерского контроля и сбора данных (SCADA) и другие типы промышленных систем контроля (ICS), меньше по объему, чем те, которые затрагивают IT-сети, но это не умаляет важность данного тренда.

Сопоставление трендов вредоносов. Обзор списка CVE показывает, что количество опубликованных уязвимостей увеличилось за последние несколько лет, что вызвало дискуссию о приоритезации исправлений. Несмотря на то, что количество опубликованных в 2020 году угроз, по всей видимости, приближается к рекорду, сами уязвимости этого года имеют самый низкий уровень распространенности использования, когда-либо зарегистрированный за 20-летнюю историю списка CVE. Между тем, уязвимости 2018 года продемонстрировали 65% распространенность использования – более четверти организаций

зарегистрировали попытки использования 15-летних CVE. Масштабная разработка и распространение эксплойтов с помощью законных и вредоносных хакерских инструментов по-прежнему отнимают значительное время у преступников.

Необходимо срочно обезопасить периметр сети, распространившийся на дома сотрудников

С ростом количества подключений, устройств и постоянной потребности в удаленной работе расширяется поверхность цифровых атак. В связи с распространением периметра корпоративной сети на дом злоумышленники ищут самое слабое звено и новые возможности для атак. Организациям необходимо готовиться, предпринимая конкретные шаги для защиты своих пользователей, устройств и информации таким же образом, как и в корпоративной сети. Компании, занимающиеся анализом угроз и исследованиями в данной сфере, могут помочь в этом, предоставив широкую экспертизу о специфике угроз по мере их развития, а также проведя углубленный анализ методов атак, их участников и новых тактик, что позволит дополнить знания организаций. Потребность в безопасных решениях для удаленных сотрудников, обеспечивающих безопасный доступ к критически важным ресурсам при одновременном масштабировании для удовлетворения потребностей всего персонала, никогда еще не была столь велика. Только платформа кибербезопасности, разработанная для обеспечения комплексной видимости и защиты всей поверхности цифровых атак, включая сети, приложения, многооблачные или мобильные среды, способна обеспечить безопасность современных быстро развивающихся сетей». ***(Киберпреступники активно используют возможности, возникшие вследствие глобальной пандемии // SecureNews (ttp://www.iksmedia.ru/news/5689389-Kiberprestupniki-aktivno-ispolzuyut.html). 03.09.2020).***

***

«Издание ZDNet сообщает, что на прошлой неделе более десятка европейских интернет-провайдеров подверглись вымогательским DDoS-атаками, нацеленным на их DNS-инфраструктуру. Среди пострадавших числятся: бельгийский EDP, французские Bouygues Télécom, FDN, K-net, SFR и нидерландские Caiway, Delta, FreedomNet, Online.nl, Signet и Tweak.nl.

Все атаки длились не более суток, и в итоге с ними удалось справиться, хотя у многих провайдеров были зафиксированы перебои в работе, пока DDoS был активен.

Представители некоммерческой организации NBIP, основанной голландскими интернет-провайдерами для борьбы с DDoS-атаками и попытками перехвата телефонных переговоров, предоставили журналистам издания дополнительную информацию об инцидентах.

«Множественные атаки были нацелены на маршрутизаторы и DNS-инфраструктуру провайдеров стран Бенилюкса. Большинство [атак] использовали DNS амплификацию и относились к типу LDAP-атак, — рассказали в NBIP. — Некоторые атаки длились более 4 часов и достигали мощности около 300 Гбит/сек».

Голландское агентство кибербезопасности (NCSC) так же подтвердило, что интернет-провайдеры страны подверглись вымогательским атакам. За прекращение DDoS злоумышленники требовали большие суммы денег в биткоинах.

ZDNet отмечает, что все атаки произошли 28 августа 2020 года, на следующий день после того, как стало известно о вымогательских DDoS-атаках на крупных поставщиков финансовых услуг. Напомню, что тогда пострадали сервис денежных переводов MoneyGram, индийский YesBank, PayPal, Braintree и Venmo. Более того, жертвой злоумышленников стала и новозеландская фондовая биржа, которая из-за атак была вынуждена несколько дня подряд приостанавливать торги.

Хотя у журналистов нет доказательств связи между этими сериями инцидентов, DDoS-атаки на поставщиков финансовых услуг прекратились сразу же после того, как начались атаки на европейских провайдеров. Кроме того, по информации собственных источников издания, за несколько недель до первой волны вымогательских DDoS-атак та же хакерская группировка атаковала нескольких интернет-провайдеров в Юго-Восточной Азии.

Некоторые эксперты считают, что недавний сбой в работе американского интернет-провайдера CenturyLink, из-за которого произошло снижение глобального трафика на 3,5%, тоже мог быть результатом DDoS-атаки. Впрочем, специалисты Cloudflare и Cisco придерживаются иного мнения и связывают инцидент с некорректным анонсом Flowspec». ***(Мария Нефёдова. Европейские интернет-провайдеры подверглись DDoS-атакам // Xakep (https://xakep.ru/2020/09/04/isp-ddos/). 04.09.2020).***

***

«Один из крупнейших мировых поставщиков услуг межсетевого соединения и обработки данных компания Equinix сообщила о кибератаке с использованием вымогательского ПО. Согласно краткому пресс-релизу, опубликованному на сайте Equinix, вредонос заразил внутренние системы компании.

В компании не раскрывают масштаб атаки или информацию, о каком вымогательском ПО идет речь. Отмечается, что инцидент не затронул дата-центры и сервисы Equinix.

«Поскольку большинство клиентов используют собственное оборудование в дата-центрах Equinix, данный инцидент не оказал влияние на их операции или данные, хранящиеся на их оборудовании», - отметили в компании.

В настоящее время расследование инцидента продолжается…». ***(Equinix расследует вымогательскую атаку на внутренние системы // SecurityLab.ru (https://www.securitylab.ru/news/511971.php). 10.09.2020).***

***

«В настоящее время ищущие жертв операторы вымогательского ПО все чаще обращаются посредникам – брокерам, продающим в даркнете доступ ко взломанным сетям различных организаций. Как сообщается в отчете ИБ-компании Digital Shadows, за последние два года спрос на подобные услуги существенно увеличился в связи с ростом популярности бизнес-модели

«вымогательское ПО как услуга» (ransomware-as-a-service, RaaS). Большой всплеск обращений RaaS к брокерам, продающим доступ ко взломанным сетям, наблюдается последние шесть месяцев.

Задачей брокеров является обеспечить все необходимые для осуществления кибератаки условия и оптимизировать процесс таким образом, чтобы оператор мог успешно внедрить свою вымогательскую программу в атакуемую сеть.

«Перед партнерами разработчиков вымогательского ПО стоит нелегкая задача по непрерывном поиску жертв для них, чтобы обеспечивать поток прибыли. Если партнер не удовлетворяет требованиям разработчика, его исключают из партнерской программы, и он теряет деньги», – пояснил руководитель исследовательской группы Digital Shadows Плек Алварадо (Alec Alvarado).

Процесс начинается с выявления уязвимых целей. Как правило, брокеры просто без разбора сканируют Сеть с помощью Shodan или Masscan в поисках открытых портов. Также они могут использовать сканеры уязвимостей для обнаружения потенциальных точек входа.

Во многих случаях брокеры выявляют жертв с открытыми портами Remote Desktop Protocol (RDP). Кроме того, они предлагают доступ к сетям атакуемых организаций через шлюзы Citrix и контроллеры доменов. Доступ через шлюзы обеспечивается с помощью брутфорс-атаки и последующей эксплуатации известных уязвимостей в продуктах Citrix.

Укрепившись во взломанной сети, брокеры внимательно изучают ее. Они могут повышать свои привилегии или с помощью боковых перемещений по сети определять, к каким данным у них есть доступ. Затем полученные сведения структурируются, упаковываются в презентабельный продукт, оцениваются и выставляются на продажу.

Стоимость каждого такого продукта варьируется от $500 до $10 тыс. Чем выше доход атакуемой организации, тем дороже стоит доступ к ее сетям. В то же время, чем выше доход, тем больше сумма требуемого выкупа.

Покупатели доступа к сетям могут гораздо больше, чем просто развертывать в них вымогательское ПО. Они могут заниматься промышленным шпионажем, похищать важные разработки, интеллектуальную собственность и другие конфиденциальные данные, повышать свои привилегии в сети, перемещаться и оставаться в ней продолжительное время, используя легитимные подручные инструменты». ***(Операторы вымогательского ПО покупают доступ ко взломанным сетям у посредников // SecurityLab.ru (https://www.securitylab.ru/news/511994.php). 11.09.2020).***

***

«Хакеры ежегодно получают более миллиона долларов, продавая на подпольных форумах взломанные учетные записи в популярной видеоигре Fortnite.

В связи с тем, что за последние несколько лет популярность Fortnite стремительно выросла, игра является прибыльной целью для киберпреступников. Подсчитав аукционные продажи нескольких продавцов аккаунтов в Fortnite за

трехмесячный период, исследователи из Night Lion Security обнаружили, что продавцы в среднем зарабатывали $25 тыс. в неделю и примерно $1,2 млн в год.

Ценность взломанной учетной записи сосредоточена вокруг внутриигровых образов персонажа (по сути, цифрового костюма). Игроки могут приобрести внутриигровые аксессуары за валюту Fortnite — V-Bucks. Некоторые скины являются редкими и стоят больших денег; например, скин Recon Expert — один из самых ценных и в среднем стоит около $2,5 тыс. на аккаунт.

Учетные записи в Fortnite изначально взламываются с помощью брутфорса, но у киберпреступников есть инструменты, которые могут сделать эти методы еще проще. По словам одного известного в подпольных кругах хакера, использующего псевдоним DonJuji, высокопроизводительные инструменты для взлома Fortnite могут в среднем осуществлять от 15 тыс. до 25 тыс. проверок аккаунта в минуту.

Epic Games ограничивает количество разрешенных входов для каждого IP-адреса, пытаясь ограничить попытки взлома пароля. Однако киберпреступники обходят это путем использования автоматической ротации прокси, которая создает новый IP-адрес для каждого запроса. Например, программа проверки учетных записей Fortnite под названием Axenta обеспечивает автоматическую ротацию прокси, а также ряд других встроенных инструментов, позволяющих проверять и автоматически менять пароли.

Затем киберпреступники создают «логи» этих различных скомпрометированных учетных записей и продают их. Коллекции, содержащие несколько тысяч украденных аккаунтов, продаются на аукционах в частных каналах Telegram по цене от $10 тыс. до $50 тыс. Затем учетные записи по отдельности выставляются на продажу». ***(Взломанные аккаунты в Fortnite ежегодно приносят хакерам миллионы долларов // SecurityLab.ru (https://www.securitylab.ru/news/511652.php). 02.09.2020).***

***

«Люди часто підключають невідомі USB-накопичувачі до своїх комп'ютерів, свідчать результати досліджень

Підключення невідомих USB-накопичувачів може призвести до проникнення на комп'ютер жертви різних видів загроз, які здатні заблокувати й викрасти важливі конфіденційні дані, повідомляє unian.ua.

Фахівці міжнародного розробника антивірусного програмного забезпечення, експерта в галузі кіберзахисту попереджають, що підключення невідомих USB-накопичувачів може призвести до викрадення хакерами важливих персональних або корпоративних даних, а також до зараження шкідливим програмним забезпеченням.

«За результатами дослідження, люди часто підключають невідомі USB-накопичувачі до своїх комп'ютерів з метою допомогти власнику знайти втрачену флешку або просто з цікавості. При цьому користувачі не замислюються про можливий шкідливий вміст носія і ризики підключення. На жаль, саме на таку поведінку часто розраховують кіберзлочинці, використовуючи методи соціальної інженерії для здійснення своєї шкідливої діяльності», - повідомляється на сайті відомої антивірусної компанії.

Потенційні ризики

Згідно з повідомленням, підключення невідомих USB-накопичувачів може призвести до проникнення на комп'ютер жертви різних видів загроз, наприклад, програм-вимагачів, які здатні заблокувати важливі конфіденційні дані. В іншому випадку, можливе зараження програмами для зчитування натискань клавіатури, які дозволять хакерам отримати облікові дані для доступу до різних облікових записів жертви — від соціальних мереж до фінансових установ.

Більш того, при підключенні зараженого USB-накопичувача до робочого комп'ютера під загрозою може опинитися вся корпоративна мережа, оскільки певні типи шкідливих програм можуть поширюватися по всій системі компанії.

"Серед відомих прикладів подібних атак загроза Stuxnet, яка поширюється безпосередньо за допомогою зараженого USB-накопичувача. Крім цього, варто згадати шкідливі програми BadUSB, які дозволяли зловмисникам отримати повний контроль над пристроєм, шпигувати за користувачами й навіть викрадати дані», - додали експерти з кібербезпеки.

Як забезпечити захист пристрою

Для зниження ризиків зараження пристрою при підключенні невідомого USB-накопичувача фахівці рекомендують дотримуватися таких правил:

- Завжди оновлювати операційну систему і програмне забезпечення до актуальних версій.

- Як правило, при підключенні зовнішнього носія до одного з USB-портів комп'ютера, запуск відбувається автоматично. Тому для безпеки пристрою рекомендується відключити функцію "Автозапуск", щоб система автоматично не відкривала USB-накопичувач з потенційно шкідливим кодом.

- Використовувати надійне рішення з безпеки для захисту робочих станцій від загроз, пов'язаних із зараженими USB-накопичувачами, а також від інших шкідливих програм. Крім того, рішення для захисту робочих станцій надає можливість сканування підключених зовнішніх носіїв на наявність будь-якого шкідливого ПЗ і повідомляє в разі виявлення підозрілих програм». ***(Фахівці розповіли, що може наробити невідома "флешка" // Багнет (http://www.bagnet.org/news/tech/1292039/fahivtsi-rozpovili-shcho-mozhe-narobiti-nevidoma-fleshka). 19.09.2020).***

***

«Хакерська атака на університетську клініку в Дюссельдорфі, ймовірно, була здійснена з території Росії.

Про це заявили в Міністерстві юстиції землі Північний Рейн-Вестфалія…

Хакери застосували вірус-шифрувальник DoppelPaymer. За даними приватних фірм, що спеціалізуються на питаннях комп'ютерної безпеки, подібний тип вірусу неодноразово застосовувався проти компаній і установ по всьому світу хакерською групою, що працює з Росії.

Кібератака на університетську клініку Дюссельдорфа сталася 17 вересня і через неї померла 78-річна жінка.

Хакерам вдалося відключити 30 серверів клініки разом з програмним забезпеченням приймального відділення. Унаслідок цього машина "швидкої

допомоги", в якій перебувала пацієнтка з підозрою на розрив аорти, змушена була їхати в більш віддалену клініку в місті Вуппераль. Згодом жінка померла в лікарні.

Німецька прокуратура веде розслідування проти невідомих осіб за фактом ненавмисного вбивства.

Вірус-шифрувальник зазвичай використовується хакерами з метою вимагання. Потрапивши в систему, вірус зашифровує призначені для користувача файли, вимагаючи викуп за ключ розшифрування.

За даними ЗМІ, справжньою метою атаки був університет у Дюссельдорфі. Після того як поліція повідомила хакерам, що їхній кібернапад зупинив діяльність медичного закладу, вони прислали ключ розшифрування. Утім, комп'ютерна мережа клініки досі не може працювати в нормальному режимі». ***(У Німеччині підозрюють російських хакерів у кібератаці на клініку в Дюссельдорфі // Європейська правда (https://www.eurointegration.com.ua/news/2020/09/22/7114586/). 22.09.2020).***

***

«Аналитики «Лаборатории Касперского» подсчитали, что в первой половине 2020 года количество атак на образовательные ресурсы в России резко возросло. Так, в период с января по июнь 2020 года этот показатель был выше значений предыдущего года на 350% и более.

Самый большой разрыв специалисты отметили в январе: количество DDoS-атак на образовательные порталы выросло на 550% по сравнению с январем 2019 года. В конце учебного года, в мае, на образовательный сектор была направлена каждая вторая DDoS-атака (49%), а уже в июне показатель закономерно снизился, но все равно оставаясь довольно высоким — 19%.

Кроме того, в первом полугодии 2020 года эксперты зафиксировали рост числа фишинговых страниц, имитирующих популярные платформы для обучения, и фейковых приложений для видеоконференций. С января по июнь с подобными вредоносными ресурсами столкнулись 168 500 уникальных пользователей продуктов «Лаборатории Касперского».

«Обычно злоумышленники, мишенью которых являются образовательные порталы, “уходят на каникулы” до сентября. В этот раз на ситуацию повлияла пандемия: все студенты и школьники перешли на дистанционное обучение, начав пользоваться цифровыми ресурсами еще активнее. В итоге увеличилось количество возможных целей для DDoS-атак, а организаторы фишинговых кампаний “пошли в науку”, держа в уме возросшую популярность различных интернет-сервисов для обучения. Пока прогнозов по снижению мошеннической активности в этой сфере мы не делаем — осень традиционно отличается высокими цифрами. К тому же многие школы и институты планируют сохранить практику онлайн-занятий», — комментирует Александр Гутников, эксперт по кибербезопасности в «Лаборатории Касперского». ***(Мария Нефёдова. Количество DDoS-атак на образовательный сектор возросло на 350% // Xakep (https://xakep.ru/2020/09/11/educational-ddos/). 11.09.2020).***

***

«Крупнейший итальянский производитель очков Luxottica и владелец бренда Ray-Ban подвергся кибератаке, которая привела к остановке производства продукции в Италии и Китае. Порталы Luxottica one.luxotrica.com и University.luxottica.com демонстрируют сообщения о техническом обслуживании сайтов:

«Портал OneLuxottica временно недоступен. Мы работаем над тем, чтобы запустить его как можно скорее», — говорится в сообщении.

Кибератака вызвала сбой в работе IT-систем офисов Luxottica в Агордо и Седико (Италия). Поскольку сотрудники не могли выполнять свою работу, им было сказано идти домой.

Как сообщили специалисты Bad Packets изданию BleepingComputer, компания Luxottica использует программно-аппаратное обеспечение Citrix ADX, содержащее критическую уязвимость (CVE-2019-19781). Уязвимость популярна среди злоумышленников-вымогателей. Эксплуатация уязвимости позволяет получить к сети и похитить учетные данные, которые можно использовать для дальнейшего перемещения по сети». ***(Крупнейший производитель очков Luxottica подвергся кибератаке // SecurityLab.ru (https://www.securitylab.ru/news/512364.php). 22.09.20200.***

***

«Эксперты из компании Cisco изучили базы данных MITER ATT&CK и рассказали о векторах угроз, на которых сотрудники служб кибербезопасности предприятий должны сосредоточить свои усилия.

Как сообщили специалисты, в первой половине 2020 года бесфайловые взломы были наиболее распространенным вектором атак на предприятия. Бесфайловые атаки включают внедрение процессов, подделку реестра и использование таких вредоносов, как бесфайловый троян Kovter, внедритель кода на основе легитимных процессов Poweliks и бесфайловое вредоносное ПО Divergent.

На втором месте находятся инструменты двойного назначения, включая Metasploit, PowerShell, CobaltStrike и Powersploit. Легальные инструменты тестирования на проникновение, такие как Metasploit, приносят пользу кибербезопасности в целом, но, к сожалению, преступники могут использовать эти решения в незаконных целях.

Легитимная система аутентификации и управления учетными данными Mimikatz заняла третье место, поскольку злоумышленники начали использовать ее для хищения учетных данных.

По данным Cisco, в первой половине 2020 года вышеперечисленные векторы атак составляют примерно 75% наблюдаемых индикаторов компрометации.

Общее количество предупреждений о выполнении кода достигло 55%, поставив данную тактику на первое место. Частота обхода защитных решений упала на 12% до 45%, в то время как достижение персистентности, перемещение по сети и доступ к учетным данным выросли на 27%, 18% и 17% соответственно.

Кроме того, некоторые классификации полностью исчезли из списка или составляли менее одного процента предупреждений об индикаторах

компрометации, включая начальный доступ, повышение привилегий и обнаружение, что свидетельствует о смещении фокуса, когда дело доходит до серьезных атак.

Для защиты от угроз высокого уровня Cisco рекомендует администраторам использовать групповые политики или белые списки для выполнения файлов, а если организации требуются инструменты двойного использования, следует реализовать временные политики доступа. Кроме того, также следует периодически проверять соединения между конечными точками». ***(Cisco рассказала об основных векторах угроз и тактиках киберпреступников // SecurityLab.ru (https://www.securitylab.ru/news/512359.php). 22.09.2020).***

***

«Компания Tyler Technologies, ведущий поставщик государственных технологических услуг, подверглась атаке программы-вымогателя, которая нарушила его работу.

Tyler Technologies - одна из крупнейших в США компаний по разработке программного обеспечения и технологических услуг для государственного сектора.

С прогнозируемым доходом в 1,2 миллиарда долларов на 2020 год и 5 500 сотрудниками Tyler Technologies предоставляет технические услуги местным органам власти во многих штатах США.

С сегодняшнего дня на веб - сайте Tyler Technologies появилось сообщение о техническом обслуживании, а в их аккаунте в Твиттере было написано в Твиттере, что у них возникли технические проблемы.

В электронном письме, увиденном BleepingComputer, ИТ-директор Tyler Technologies Мэтт Биери отправил клиентам электронное письмо, в котором сообщалось, что они расследуют кибератаку и уведомили правоохранительные органы.

"Я пишу, чтобы сообщить вам об инциденте безопасности, связанном с несанкционированным доступом к нашим внутренним телефонным и информационным системам со стороны неизвестной третьей стороны. Мы рассматриваем этот вопрос с наивысшим приоритетом и работаем с независимыми ИТ-экспертами для проведения тщательного расследования ответ."

«Сегодня рано утром мы узнали, что неавторизованный злоумышленник нарушил доступ к некоторым нашим внутренним системам. После обнаружения и из мер предосторожности мы закрыли точки доступа к внешним системам и немедленно приступили к исследованию и устранению проблемы. С тех пор мы привлекли внешних экспертов по ИТ-безопасности и судебной экспертизе для проведения подробного анализа и помощи в безопасном восстановлении поврежденного оборудования. Мы внедряем усовершенствованные системы мониторинга и уведомили правоохранительные органы », - заявил Биери в электронном письме клиентам.

Биери также заявил, что текущие расследования показывают, что атака была ограничена локальной сетью Tyler Technologies.

В сообщениях на форуме Ассоциации муниципальных информационных систем Калифорнии (MISAC), опубликованных для BleepingComputer, служащие

местных органов власти сообщили, что Tyler Technologies подверглась атаке программы-вымогателя, затронувшей их систему продажи телефонных билетов и системы поддержки.

«Сегодня утром нам сообщил один из технических специалистов службы поддержки, что они рано утром столкнулись с программой-вымогателем в их корпоративных сетях. У меня нет никаких других подробностей на данный момент, кроме того, что поддержка не работает, пока они не получат доступ к своим системам», - сказал один местный житель Сотрудник муниципалитета разместил сообщение на форуме MISAC.

Другой пользователь MISAC заявил, что он слышал, что атака была ограничена внутренней сетью Tyler Technologies и не затронула клиентов.

Технологии Tyler, пораженные вымогателем RansomExx

Источники кибербезопасности, знакомые с атакой, сообщили BleepingComputer, что Tyler Technologies подверглась атаке со стороны программы-вымогателя RansomExx.

RansomExx - это переименованная версия вымогателя Defray777, активность которого возросла с июня, когда они атаковали Департамент транспорта Техаса (TxDOT), Konica Minolta и совсем недавно IPG Photonics.

Хотя BleepingComputer не получил записки о выкупе, мы обнаружили зашифрованный файл, загруженный сегодня на VirusTotal, связанный с этой атакой.

Этот зашифрованный файл имеет расширение.tylertech911-f1e1a2ac, которое включает имя Tyler Technologies и имеет тот же формат, что и другие атаки RansomExx.

RansomExx не имеет сайта утечки данных программ-вымогателей, но это не означает, что они не крадут незашифрованные файлы перед развертыванием своих программ-вымогателей.

BleepingComputer связался с Tyler Technologies с дополнительными вопросами, но не получил ответа». ***(Lawrence Abrams. Government software provider Tyler Technologies hit by ransomware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/government-software-provider-tyler-technologies-hit-by-ransomware/). 23.09.2020).***

***

«Банда программ-вымогателей LockBit запустила новый сайт утечки данных, который будет использоваться в рамках их стратегии двойного вымогательства, чтобы запугать жертв и заставить их заплатить выкуп.

С конца 2019 года банды программ-вымогателей применяют тактику двойного вымогательства: кража незашифрованных файлов перед шифрованием компьютеров в сети.

Затем банды вымогателей используют украденные файлы и угрозу того, что они будут опубликованы на сайтах утечки данных, в качестве рычага, чтобы заставить жертв заплатить выкуп.

Сайт утечки данных Lockbit

По данным компании Kela, занимающейся кибербезопасностью, вымогатель LockBit разместил вчера на русскоязычном хакерском форуме ссылку на свой новый сайт утечки данных.

На сайте утечки данных в настоящее время находятся две жертвы; производитель деталей автоматики и судоходная компания.

LockBit ранее запускал сайт утечки, но закрыл его примерно в то время, когда они присоединились к «Картелю лабиринта», и начал использовать сайт Maze для публикации украденных файлов.

С открытием их сайта утечки данных неизвестно, выходят ли они из этого «картеля» или просто хотят, чтобы специальный сайт находился под их контролем.

Все атаки программ-вымогателей следует рассматривать как утечки данных, поскольку операторы программ-вымогателей не только крадут данные, но и просматривают документы, чтобы увидеть, что в них содержится.

В связи с этим компании должны быть прозрачными в отношении атак, чтобы сотрудники и клиенты могли адекватно защитить себя от риска раскрытия данных.

С выпуском сайта LockBit теперь в общей сложности семнадцать сайтов утечки данных программ-вымогателей, используемых в тактике двойного вымогательства». ***(Lawrence Abrams. LockBit ransomware launches data leak site to double-extort victims // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/lockbit-ransomware-launches-data-leak-site-to-double-extort-victims/). 16.09.2020).***

***

«Креативная фишинговая кампания использует шаблон электронной почты, который притворяется напоминанием о прохождении тренинга по безопасности, проводимого известной охранной компанией.

По мере того, как пользователи компьютеров становятся все более осведомленными и осведомленными о стандартных методах и шаблонах фишинга, злоумышленникам необходимо постоянно совершенствовать свои методы для разработки инновационных способов обманным путем заставить пользователей предоставить свои учетные данные.

Так обстоит дело с новой фишинговой кампанией, обнаруженной фирмой Cofense, занимающейся защитой электронной почты, которая претендует на то, чтобы быть «обучением безопасности» от KnowBe4.

Новая кампания прикидывается напоминанием о фишинге

С ростом фишинговых атак компании, занимающиеся кибербезопасностью, предлагают обучение фишингу и имитационные тесты, чтобы проверить, насколько хорошо сотрудники могут обнаруживать вредоносные электронные письма.

Одна известная компания по обеспечению безопасности электронной почты - KnowBe4, которая предлагает обучение фишингу и имитационные тесты.

В новой фишинговой кампании, проанализированной Cofense и первоначально обнаруженной KnowBe4, злоумышленники рассылают электронные письма, которые якобы исходят от KnowBe4, с напоминанием им войти в систему и пройти обучение фишингу.

В этих электронных письмах используется тема «Напоминание об обучении: срок выполнения», а получателю предлагается войти в систему «Обучение по вопросам безопасности», прежде чем оно истечет в течение 24 часов.

Интересным аспектом фишингового письма является то, что оно предупреждает, что ссылка будет не на стандартной платформе обучения фишингу, а на внешнем сайте.

Злоумышленники предоставляют это предупреждение, чтобы успокоить жертв, если они видят подозрительный URL-адрес, предлагающий ввести свои учетные данные.

Если пользователь щелкает URL-адрес, он будет перенаправлен на URL-адрес с использованием TLD Russia.ru, который просит его войти в систему с учетными данными Outlook, чтобы предположительно начать обучение.

После входа в систему им будет предложено ввести дополнительную информацию, такую как имя пользователя, адрес электронной почты, имя, день рождения, адрес и еще раз пароль.

Теперь, когда злоумышленники собрали адрес электронной почты, пароль и личную информацию жертвы, они могут использовать ее в дальнейших целевых атаках, таких как мошенничество с BEC, или для доступа к сети жертвы.

Фишинговые мошенничества с каждым днем становятся все более изощренными, и даже тем, кто разбирается в фишинговых атаках, может быть сложно понять, во что верить.

В связи с этим каждый должен уделять пристальное внимание URL-адресам, прежде чем отправлять какую-либо информацию. Если что-то выглядит подозрительно, сотрудники должны связаться со своими сетевыми администраторами, чтобы подтвердить подлинность электронного письма.

Если бы эта фишинговая афера была частью реальной программы обучения осведомленности о безопасности, подозрительность к URL-адресам и уведомление ваших администраторов прошли бы проверку». ***(Lawrence Abrams. This security awareness training email is actually a phishing scam // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/this-security-awareness-training-email-is-actually-a-phishing-scam/). 16.09.2020).***

***

«Ландшафт кибербезопасности меняется каждый день: в то время как злоумышленники разрабатывают сотни способов атаковать бизнес, специалисты по кибербезопасности находят тысячи стратегий защиты предприятий.

По данным организации Online Trust Alliance (OTA), только в 2018 году бизнес подвергся более 2 млн хакерских атак и потерял из-за них $45 млрд. Эта сумма на 60% больше той, что приводилась годом ранее. При этом рынок кибербезопасности тоже растет и будет расти – если в 2019 году он составлял $121,1 млрд, то уже к 2027 году превысит $281,74 млрд со среднегодовым темпом роста в 12,6%, прогнозирует Fortune Business Insights. Во многом это связано с повсеместной диджитализацией: чем больше информации в цифровом формате, тем выше риски ее утечки.

По мере того, как кибератаки становятся все более распространенными и изощренными, предприятиям необходимо совершенствовать свою защиту. Rusbase поговорил со специалистами компании Fortinet и узнал, какие тенденции в области кибербезопасности формируются прямо сейчас, что изменилось из-за пандемии коронавируса и отличается ли подход к безопасности российских компаний от зарубежных.

В 2020 году вероятность того, что вы столкнетесь с простым компьютерным вирусом, крайне мала – сегодняшние вредоносные программы фокусируются на том, чтобы хакеры смогли заработать как можно больше. На традиционных же вредоносных программах особо не заработаешь. Поэтому, скорее всего, вы будете поражены вымогателями, троянами, которые украдут данные, или ботом, позволяющим сдавать в аренду ваши вычислительные мощности. Только в 2019 году было обнаружено 439 тысяч новых вариантов вредоносных программ, что на 12,3% больше, чем годом ранее. Современные «вредители» эффективнее прежних, распространявшихся через нелегальные копии программного обеспечения. Они могут воровать пароли и конфиденциальную информацию, шифровать и удалять данные и так далее. Обнаружить вирусы тоже стало сложнее – например, их скрывают среди легальных программ (скажем, PDF или Word) или обновлений программного обеспечения.

Зловредная активность постоянно растет и эволюционирует, подтверждает технический директор Fortinet в России Алексей Андрияшин. По его словам, в последнее время злоумышленники задействуют новые технологии, которые часто рекламируются и используются в продуктах безопасности: например, искусственный интеллект, обработку больших данных, технологии машинного обучения.

Действительно, тренд на применение в кибербезопасности искусственного интеллекта и машинного обучения набирает популярность. По данным Capgemini Research Institute, искусственный интеллект быстрее обнаруживает угрозы и вредоносные действия, чем любой специалист, что позволяет более оперативно реагировать на внешние вмешательства в работу компании. Руководители служб кибербезопасности 69% компаний, которых опрашивали Capgemini Research Institute, подтвердили, что в их работе искусственный интеллект «жизненно важен». Спрос на ИИ в кибербезопасности превысил $8,8 млрд в 2019 году и достигнет $38,2 млрд к 2026.

Но преступники тоже не отстают и активно осваивают эти методы. Как только это войдет в постоянную практику, бороться с киберпреступностью станет еще тяжелее, говорит Алексей Андрияшин.

Кроме того, что вирусы эволюционируют сами, меняются и технические возможности их распространения. Так, нарастает популярность интернета вещей, что делает уязвимым для вирусов не только компьютер и телефон, но и всю остальную технику в доме, офисе или на производстве. Каналы связи IoT-гаджетов с облаками – слабое звено в системе безопасности, а преступники уже научились запускать вирусы через сети 5G и проникать во все IoT-устройства. Чтобы найти подобные слабые места, злоумышленники начали использовать инструменты их автоматического обнаружения в любой системе.

Одновременно с этим все больше компаний используют для аутентификации биометрические данные, но надежность этого метода до сих пор остается под вопросом. Так, еще в 2015 из американского Управления кадровой службой (управляет персоналом на государственной службе федерального правительства США) был похищен файл с более 5,6 млн отпечатков пальцев. И так как, в отличие от паролей, отпечатки пальцев нельзя изменить, этот вид биометрии навсегда перестал быть надежным способом аутентификации для пострадавших госслужащих. Есть и другая проблема – отпечатки можно подобрать. В 2018 году исследователи из Университета Нью-Йорка создали искусственный интеллект, который смог взломать аутентификацию отпечатков пальцев в 20% случаев путем подбора. Легко обмануть и некоторые сканеры радужной оболочки глаза – достаточно сфотографировать радужку в ночном режиме, распечатать изображение на бумаге и поместить сверху влажную контактную линзу, чтобы имитировать форму глаза.

Несмотря на то, что 100-процентную безопасность данных в интернете гарантировать никто не может, все больше компаний и государств требуют авторизации пользователей на всех ресурсах, причем под настоящими именами.

Задача государства заключается в том, чтобы обеспечивать безопасность своих граждан и исключать возможности использования персональных данных злоумышленниками, считает Алексей Андрияшин: «Какие средства допустимы, каждый решает самостоятельно. Но то, что вовлеченность государства и всех служб в интернет повышается – неизбежный факт, нам с этим жить и адаптировать действия в интернете».

Что изменил коронавирус

Сегодня во всем мире около 2,8 млн специалистов по кибербезопасности, но этого недостаточно – по данным Международного консорциума по сертификации в области безопасности информационных систем ((ISC)2), компаниям и госучреждениям не хватает примерно 4,07 млн таких специалистов. То есть рабочая сила в области кибербезопасности должна вырасти на 145%, только чтобы покрыть существующий спрос. Опрос, проведенный среди компаний в ноябре 2019 года, показал, что 65% респондентов испытывают нехватку специалистов по кибербезопасности. При этом уже работающие специалисты вынуждены отражать все больше атак.

Чтобы повысить устойчивость к кибератакам, компаниям необходимо отслеживать осведомленность своих IT-специалистов и рядовых сотрудников. Помочь в этом могут бесплатные тренинги по кибербезопасности от Fortinet, ориентированные как на профессионалов, так и на обычных пользователей.

Киберпреступники, которые решили воспользоваться пандемией для своих целей, начали появляться еще в конце января и распространились так же быстро, как и болезнь, указывают эксперты PwC в обзоре, посвященном кибербезопасности во время COVID-2019. Обычно злоумышленники выдают себя за доверенное лицо (банки, торговых партнеров) или рядового сотрудника (например, IT-администратора, менеджера). Прежде всего, такие атаки осуществляются для того, чтобы получить доступ к электронной почте компании, украсть личные данные

сотрудников и информацию о бизнесе, проникнуть в корпоративные платежные системы, пишет PwC.

Агентство по кибербезопасности и инфраструктурной безопасности (CISA) рассказало, что киберпреступники находят все больше уязвимостей в VPN, при этом на их обновления у компаний не хватает времени, так как VPN работают круглосуточно. Кроме того, возрастает количество фишинговых писем и атак на организации без многофакторной аутентификации.

Но самое главное – во время коронавируса активно атакуют и ключевые государственные организации. Тренд не новый – еще в декабре 2015 года в Ивано-Франковске на западе Украины хакеры одновременно атаковали три электростанции, выведя из строя 60 подстанций и оставив почти четверть миллиона человек без света на несколько часов. Это был первый взлом для отключения электростанций, но лишь начало кибератак на жизненно важную инфраструктуру и ключевые организации.

В марте, уже после того, как Всемирная организация здравоохранения (ВОЗ) объявила о пандемии, ее главный сотрудник по информационной безопасности Флавио Аггио объявил, что попыток взлома серверов организации и ее партнеров стало как минимум в два раза больше. Например, по данным Reuters, 13 марта группа хакеров, известная как DarkHotel, которая занимается кибершпионажем по крайней мере с 2007 года, активировала вредоносный сайт, имитирующий внутреннюю почтовую систему ВОЗ, и пыталась украсть пароли у нескольких сотрудников агентства. Атаки во время пандемии совершались и на государственных служащих и руководителей предприятий в Китае, Северной Корее, Японии, США – и официальные лица, и эксперты по кибербезопасности этих стран неоднократно предупреждали, что злоумышленники всеми силами стремятся извлечь выгоду из международной обеспокоенности из-за коронавируса. По данным Reuters, во время пандемии ежедневно создается около 2 тысяч вредоносных сайтов, чего никогда не наблюдалось раньше.

Бизнес видит эти тренды и уже готов инвестировать больше: по данным исследования Fortinet 2020 Remote Workforce Cybersecurity Report, почти все опрошенные организации уже так или иначе инвестировали дополнительные средства в кибербезопасность в связи с пандемией COVID-19. Почти половина респондентов отметили вложения дополнительных средств в VPN и облачную безопасность, в то время как почти 40% вложили дополнительные средства в квалифицированных IT-специалистов или в контроль сетевого доступа (NAC). Причем 60% опрошенных предприятий планируют потратить более $250 тысяч на инвестиции в данную сферу в течение следующих 24 месяцев.

После того, как многие компании перевели сотрудников на удаленку, резко вырос спрос на системы и решения, которые обеспечивают защищенную удаленную работу, подтверждает Алексей Андрияшин. Сейчас этот фактор несколько сглаживается, и многие компании уже перестроили свои процессы под удаленный доступ и продолжают работать в комбинированном режиме – кто-то в офисе, кто-то из дома.

Возросла активность и менее крупных злоумышленников, которые воруют данные с карт, просят заплатить штраф из-за нарушения режима самоизоляции или

перевести деньги на телефон. По данным МВД, в I квартале 2020 года число IT-преступлений возросло на 83,9%, мошенничеств — на 48,5%, мошенничеств с использованием электронных средств платежа — на 150,5%, преступлений с использованием или применением расчетных (пластиковых) карт — на рекордные 457,2%.

«Но на крупных ресурсах этот риск маловероятен. Выше вероятность того, что какой-то ресурс будет подделан злоумышленниками и пользователь попадет именно на зловредный сайт и оставит там свои данные. Поэтому так важно не терять бдительности, следить за тем, какую информацию вы вводите и разглашаете, и читать новости о современных методах преступников, чтобы быть подготовленным», – советует эксперт.

Россия и мир

Все продукты для обеспечения информационной безопасности уже известны, и на рынке нет ограничений доступа к ним. Но некоторые компании, например, близкие к государству, законодательно ограничены в использовании иностранных решений, рассказывает Андрияшин. Остальным же следует внимательно следить за тенденциями во всем мире – часто у западных игроков есть чему поучиться.

Например, в России многие с недоверием относятся к облакам, хотя за рубежом технология широко используется. Многие российские компании (те же госорганы и бизнес, обеспечивающий работу критически важной инфраструктуры) вовсе не могут их использовать, но остальным организациям ничего не мешает это делать. Облачные технологии удобны для доступа к данным, обмена информацией, в качестве площадок коммуникации, а применение различных методов защиты делает эту технологию надежной, говорит Андрияшин. На российском рынке это направление будет активно развиваться.

В начале июля стало известно, что Amazon заключил соглашение с Mail.ru Group о создании совместного облачного сервиса. Так крупнейший в мире облачный бизнес полноценно выйдет в Россию. «Вслед за ним, наверняка, подтянутся и другие, и облачные технологии будут активно развиваться и на нашем рынке. Современным компаниям нужно быть готовыми к тому, что применение облаков в будущем – необходимый фактор развития бизнеса, так как облачные технологии существенно снижают издержки на IT», – заключает он». ***(Вирусный фон: как хакеры используют пандемию в своих целях, и другие тренды кибербезопасности // Rusbase (https://rb.ru/longread/virus-and-cyber-security/). 15.09.2020).***

***

«Компания Group-IB рассказала, что в первом полугодии 2020 года хакерами в кибератаках наиболее часто использовался фишинг. Через него распространялись программы-шпионы, программы для загрузки вредоносного ПО и банковские трояны. Об этом сообщает РИА «Новости» со ссылкой на исследование Group-IB.

«Ожидаемо фишинг под различные онлайн-сервисы вырос более чем вдвое во время пандемии коронавируса: на него пришлось 46% от общего числа фейковых веб-страниц», — говорится в сообщении.

Топ-4 выявленных киберугроз:

- вложения с программами-шпионами или ссылки, ведущие на их скачивание — в 43% вредоносных писем;
- загрузчики — в 17%;
- бэкдоры, открывающие удаленный доступ к компьютерам жертв, — в 16%;
- банковские трояны — в 15%.

Отмечается, что программы-шифровальщики, которые в прошлом полугодии были в каждой второй вредоносной рассылке, практически исчезли. На них приходится менее 1%.

«Операторы шифровальщиков сфокусировались на целевых атаках, выбирая себе крупные жертвы, и требуя от них значительно большие суммы. Точечная проработка таких атак снизила их объем в антирейтинге угроз», — поясняют эксперты.

Наиболее часто используемые инструменты кибератак: троян RTM, шпионское ПО LOKI PWS, AgentTesla, Hawkeye, и Azorult, а также бэкдоры Formbook, Nanocore, Adwind, Emotet и Netwire.

Также были обнаружены новые вредоносные программы:

- ПО для удаленного управления ПК Quasar,
- программа-шпион, извлекающая данные учетных записей пользователей из различных программ, Gomorrah,
- ПО для сбора пользовательских данных 404 Keylogger.

Большинство вредоносных файлов попадали на компьютер жертвы с помощью архивов». ***(Екатерина Кочкина. Эксперты назвали самые распространенные киберугрозы текущего года // Rusbase (https://rb.ru/news/cyberthreats-2020/). 18.09.2020).***

***

«На прошедших выходных около 2000 сайтов, работающих на движке Magento, были атакованы в ходе крупнейшей кибератаки.

Группа исследователей из Sansec зафиксировала 1904 MageCart атаки на онлайн-магазины: 10 в пятницу, 1058 в субботу, 603 в воскресенье и 233 в понедельник. По оценкам специалистов могли быть украдены платежные данные десятков тысяч покупателей. Sansec отмечает, что это крупнейшая атака, зарегистрированная с тех пор, как компания начала вести наблюдение в 2015 году. Предыдущий рекорд составил 962 онлайн-магазина, атакованных за день в июле 2019 года.

Растущее число атак подобного рода говорит о том, что злоумышленники усложняют свои методы. Также вызывает опасение тот факт, что многие из атакованных сервисов в прошлом не имели проблем с безопасностью. Это может означать, что хакеры обнаружили новую уязвимость. Предположительно она находится в версии Magento 1. Версия на данный момент не актуальна и перестала поддерживаться разработчиками 30 июня этого года, но тем не менее используется многими сайтами до сих пор. Если предположение верно, это означает, что еще около 95 000 онлайн магазинов находятся под угрозой». ***(Крупнейшая кибератака***

на интернет-магазины // SecureNews (https://securenews.ru/the-largest-cyberattack-on-online-stores/). 15.09.2020).

***

«Ожидаемо фишинг под различные онлайн-сервисы вырос более чем вдвое во время пандемии коронавируса: на него пришлось 46% от общего числа фейковых веб-страниц. Со сцены фактически ушли лидеры прошлого полугодия – вирусы-шифровальщики, веерно распространяемые в почтовых рассылках, на них пришелся всего 1%. Зато каждое третье вредоносное письмо содержало программу-шпиона, цель установки которого – кража платежных данных или иной чувствительной информации с целью продажи в даркнете или шантажа.

По данным Центра реагирования на инциденты кибербезопасности CERT-GIB, в первой половине 2020 вложения с программами-шпионами или ссылки, ведущие на их скачивание, содержались в 43% проанализированных Group-IB вредоносных писем. Еще 17% содержали загрузчики, третье место разделили бэкдоры и банковские трояны — они скрывались в 16% и 15% вредоносных рассылок, соответственно. Шифровальщики, которые в прошлом полугодии детектировались в каждой второй вредоносной рассылке, в первой половине этого года практически исчезли — на них приходится менее 1%.

Эта статистика подтверждает тренд, сформулированный в недавнем исследовании Group-IB «Программы-вымогатели: новейшие методы атак шифровальщиков»: операторы сместили фокус атак с индивидуальных пользователей на крупные корпоративные сети. Так, вместо того, чтобы шифровать компьютер отдельной жертвы после компрометации, атакующие используют зараженную машину для дальнейшего продвижения по сети, повышения привилегий в системе и распространения шифровальщика по максимально возможному числу хостов.

В Топ-10 инструментов, использовавшихся злоумышленниками в атаках, зафиксированных CERT-GIB за этот период, вошли троян RTM (30%); шпионское ПО LOKI PWS (24%), AgentTesla (10%), Hawkeye (5%), и Azorult (1%); и бэкдоры Formbook (12%), Nanocore (7%), Adwind (3%), Emotet (1%), и Netwire (1%). Среди новых инструментов, выявленных в первом полугодии, Quasar – ПО для удаленного управления на базе открытого исходного кода, Gomorrah — программа-шпион, извлекающая данные учетных записей пользователей из различных программ, и 404 Keylogger — ПО для сбора пользовательских данных, получившее широкое распространение в первом квартале 2020 года.

Почти 70% вредоносных файлов попадали на компьютер жертвы с помощью архивов, порядка 18% были замаскированы под офисные документы (с расширениями.doc,.xls и.pdf), еще 14% — под исполняемые файлы и скрипты.

В первой половине 2020, CERT-GIB заблокировал 9 304 фишинговых ресурса, что на 9% выше, чем полугодием ранее. Главным трендом этого периода стало более чем двукратное увеличение числа ресурсов, использующих безопасное SSL/TLS соединение — их количество за полгода возросло с 33% до 69%. Это объясняется желанием злоумышленников удержать пул жертв — большинство

популярных браузеров отмечают сайты без SSL/TLS соединения как по умолчанию небезопасные, что негативно сказывается на эффективности фишинговых кампаний. По прогнозам экспертов Group-IB, доля веб-фишинга с небезопасным соединением продолжит сокращаться, а сайты, не поддерживающие протоколы SSL/TLS, станут исключением.

Как и во второй половине 2019 года, в текущем периоде лидером по количеству фишинговых страниц стали онлайн-сервисы. На фоне пандемии и перехода бизнеса в онлайн, их доля возросла до рекордных 46%. Привлекательность онлайн-сервисов обусловлена тем, что, похищая данные учетной записи пользователя, злоумышленники также могут получить доступ к данным банковской карты, привязанной к аккаунту. Чаще всего злоумышленники создают поддельные страницы, требующие обновления данных банковской карты для продолжения пользования сервисом, но в некоторых случаях, похищая данные учетной записи, они получают доступ и к данным самой карты.

Следом за онлайн-сервисами — почтовые агенты (24%), чья доля после спада в 2019 возобновила рост в 2020 году, и финансовые организации (11%). В топ целевых категорий по веб-фишингу также вошли платежные сервисы, облачные хранилища, социальные сети, и сайты знакомств.

Согласно результатам работ по обнаружению и нейтрализации угроз CERT-GIB, лидерство в топе доменных зон по регистрации фишинга уверенно держит зона.com, согласно на нее приходится почти половина проанализированных за отчетный период фишинговых ресурсов — 44%. За ней следуют доменные зоны.ru (9%),.br (6%),.net (3%) и.org (2%).

«Год начался с изменений в топе актуальных угроз, распространяющихся с помощью вредоносных рассылок, — комментирует заместитель руководителя CERT-GIB Ярослав Каргалев. — Операторы шифровальщиков сфокусировались на целевых атаках, выбирая себе крупные жертвы, и требуя от них значительно большие суммы. Точечная проработка таких атак снизила их объем в антирейтинге угроз, а на их место пришли программы-шпионы и бэкдоры, с помощью которых злоумышленники сначала похищают чувствительную информацию, а затем шантажируют жертву, требуя выкуп, и, в случае отказа, продают ее на хакерских форумах или выставляют в паблик. Вероятнее всего, стремление операторов шифровальщиков сорвать большой куш постепенно приведет к росту таргетированных атак, при этом почта по-прежнему будет главным источником их распространения, что повышает требования к обеспечению ее кибербезопасности». ***(Эксперты фиксируют изменение ландшафта угроз по итогам первого полугодия 2020г. // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5691854-Eksperty-fiksiruyut-izmenenie-lands.html). 21.09.2020).***

***

«…Федеральное агентство пострадало от успешной кибератаки, связанной со шпионажем, в результате которой в его сети был сброшен бэкдор и многоступенчатое вредоносное ПО.

Агентство по кибербезопасности и безопасности инфраструктуры США (CISA) в четверг опубликовало предупреждение, в котором не назвало агентство, а

предоставило технические детали атаки. В нем говорилось, что хакеры получали первоначальный доступ, используя легитимные учетные данные сотрудников Microsoft Office 365 для удаленного входа на компьютер агентства.

«У злоумышленника были действующие учетные данные для доступа к учетным записям Microsoft Office 365 (O365) нескольких пользователей и учетным записям администратора домена», - сообщает CISA. «Сначала злоумышленник вошел в учетную запись пользователя O365 с IP-адреса 91.219.236 [.] 166, а затем просмотрел страницы на сайте SharePoint и загрузил файл. Злоумышленник киберугроз несколько раз подключался по протоколу управления передачей (TCP) с IP-адреса 185.86.151 [.] 223 к серверу виртуальной частной сети (VPN) организации-жертвы».

Что касается того, как злоумышленникам вообще удалось заполучить учетные данные, расследование CISA не дало окончательного ответа, однако предполагалось, что это могло быть результатом эксплойта уязвимости, который, по его словам, широко распространен в правительственных сетях.

«Возможно, кибер-злоумышленник получил учетные данные с незащищенного VPN-сервера агентства, используя известную уязвимость - CVE-2019-11510 - в Pulse Secure», - говорится в предупреждении. «CVE-2019-11510… позволяет удаленное извлечение файлов без аутентификации, включая пароли. CISA зафиксировала широкое использование CVE-2019-11510 в федеральном правительстве».

Патч был выпущен в апреле 2019 года, но Министерство внутренней безопасности (DHS) в апреле этого года отметило, что до развертывания исправлений злоумышленники могли скомпрометировать учетные записи Active Directory с помощью уязвимости - так что даже те, кто исправлены ошибки, все еще могут быть скомпрометированы и уязвимы для атак.

После первоначального доступа группа приступила к разведке сети. Сначала они вошли в учетную запись электронной почты агентства O365, чтобы просмотреть и загрузить вложения электронной почты службы поддержки с «доступом к интрасети» и «паролями VPN» в строке темы - и они обнаружили ключ Active Directory и групповой политики, изменив ключ реестра для группы Политика.

«Сразу после этого злоумышленник использовал стандартные процессы командной строки Microsoft Windows - conhost, ipconfig, net, query, netstat, ping и whoami, plink.exe - для перечисления скомпрометированной системы и сети», - сообщает CISA.

Следующим шагом было подключение к виртуальному частному серверу (VPS) через клиент Windows Server Message Block (SMB), используя псевдоним безопасного идентификатора учетной записи, который группа ранее создала для входа в нее; затем они запустили plink.exe, утилиту удаленного администрирования.

После этого они подключились к системе управления и контроля (C2) и установили специальную вредоносную программу с именем файла «inetinfo.exe». Злоумышленники также создали локально смонтированный удаленный общий ресурс, который «позволял злоумышленнику свободно перемещаться во время

своих операций, оставляя меньше артефактов для судебного анализа», - отмечает CISA.

Киберпреступники, войдя в систему как администратор, создали запланированное задание для запуска вредоносного ПО, которое оказалось дроппером для дополнительных полезных нагрузок.

«Inetinfo.exe - это уникальное многоэтапное вредоносное ПО, используемое для удаления файлов», - пояснил CISA. «Он удалил system.dll и 363691858 файлов, а также второй экземпляр inetinfo.exe. System.dll из второго экземпляра inetinfo.exe расшифровал 363691858 как двоичный из первого экземпляра inetinfo.exe. Расшифрованный двоичный файл 363691858 был вставлен во второй экземпляр inetinfo.exe для создания туннеля с локальным именем и подключения к нему. Внедренный двоичный файл затем выполнил шелл-код в памяти, которая была подключена к IP-адресу 185.142.236 [.] 198, что привело к загрузке и выполнению полезной нагрузки».

В нем добавлено: «Злоумышленник смог преодолеть защиту агентства от вредоносного ПО, и inetinfo.exe избежал карантина».

CISA не уточнила, что это за вторичная полезная нагрузка - Threatpost обратился за дополнительной информацией.

Тем временем группа угроз также установила бэкдор в виде постоянного туннеля Secure Socket Shell (SSH) / обратного прокси-сервера SOCKS.

«Прокси-сервер позволял подключаться между удаленным сервером, управляемым злоумышленником, и одним из файловых серверов организации-жертвы», - сообщает CISA. «Обратный прокси-сервер SOCKS взаимодействовал через порт 8100. Этот порт обычно закрыт, но злоумышленник открыл его».

Затем была создана локальная учетная запись, которая использовалась для сбора и эксфильтрации данных. Из этой учетной записи киберпреступники просматривали каталоги на файловых серверах жертвы; скопировали файлы из домашних каталогов пользователей; подключил управляемый злоумышленником VPS с файловым сервером агентства (через обратный SMB SOCKS прокси); и извлекли все данные с помощью клиента служб терминалов Microsoft Windows.

Атака устранена - неизвестно, когда она произошла. CISA заявила, что, к счастью, ее система обнаружения вторжений смогла в конечном итоге пометить активность.

«CISA узнала - через EINSTEIN, систему обнаружения вторжений CISA, которая отслеживает федеральные гражданские сети - о потенциальном взломе сети федерального агентства», - говорится в предупреждении. «В сотрудничестве с затронутым агентством CISA провела операцию по реагированию на инциденты, подтвердив вредоносную деятельность». ***(Tara Seals. Feds Hit with Successful Cyberattack, Data Stolen // Threatpost (https://threatpost.com/feds-cyberattack-data-stolen/159541/). 24.09.2020).***

***

«Все больше людей, находящихся в сети во время карантина и смены на дому, оказались прибыльными для DDoS-атак.

В первой половине 2020 года наблюдался значительный рост числа распределенных атак типа «отказ в обслуживании» (DDoS) по сравнению с тем же периодом прошлого года - явление, которое, по-видимому, напрямую связано с глобальной пандемией коронавируса.

В операционном центре безопасности Neustar (SOC) за этот период количество DDoS-атак увеличилось на 151%, включая одну из самых крупных и длительных атак, которые когда-либо нейтрализовал Neustar - атака со скоростью 1,17 терабит в секунду (Тбит / с) и продолжалась. пять дней и 18 часов.

«Эти цифры отражают растущее число, объем и интенсивность сетевых кибератак по мере того, как организации перешли на удаленные операции, а зависимость сотрудников от Интернета возросла», - отметила компания в своем отчете о состоянии дел за первую половину, опубликованном в среду.

DDoS-атаки становятся все масштабнее, и, по словам Нойстара, их объемы «заметны»: количество атак размером 100 Гбит / с и выше выросло на 275 процентов. Ярким примером этого является атака со скоростью 2,3 Тбит / с, нацеленная на клиент Amazon Web Services в феврале - крупнейшая в истории масштабная DDoS-атака. Вышеупомянутая атака 1,17 Тбит / с была на 192 процента больше, чем самая крупная атака, которую компания предотвратила в первой половине 2019 года.

Тем не менее, увеличение общего количества атак ощущалось во всех категориях размеров, причем даже атаки размером 5 Гбит / с увеличились более чем на 200 процентов. В целом небольшие атаки размером 5 Гбит / с и ниже составили 70% всех атак, нейтрализованных Neustar в период с января по июнь.

«В то время как крупные объемные атаки привлекают внимание и заголовки, злоумышленники все чаще осознают ценность нанесения ударов на достаточно низком уровне, чтобы обойти пороговые значения трафика, которые могут вызвать смягчение последствий для снижения производительности или точного нацеливания на уязвимую инфраструктуру, такую как VPN», - сказал Майкл Качмарек, вице-президент Neustar президент по продуктам безопасности, в своем заявлении. «Эти сдвиги подвергают риску DDoS-атаки каждую организацию, имеющую доступ в Интернет».

Он добавил, что угроза особенно серьезна при удаленной работе сотрудников по всему миру. Стремительный рост всех показателей DDoS коррелирует с пандемией COVID-19 и компаниями, отправляющими своих сотрудников домой на работу.

Эта смена рабочей силы способствовала более высокому, чем когда-либо, интернет-трафику: Neustar сообщил, что использование Интернета выросло на 50-70 процентов, а потоковое видео только за первый квартал выросло более чем на 12 процентов.

«Это означает, что у злоумышленников всех типов, будь то серьезные киберпреступники или скучающие подростки, застрявшие дома, было больше экранного времени, чтобы мешать», - говорится в отчете.

Компания добавила, что росту атак способствуют и другие аспекты, например, тот факт, что в наши дни фирмы часто сильно полагаются на VPN для безопасного удаленного доступа: «VPN-серверы часто остаются уязвимыми, что

упрощает киберпреступникам задачу персонал в автономном режиме с целевой DDoS-атакой».

Кроме того, в то время как наиболее популярные сегменты веб-сайтов по-прежнему являются традиционной добычей для сайтов электронной коммерции и игр, DDoS-атаки теперь больше сосредоточены на медицинских организациях, которые содержат конфиденциальную информацию о пациентах и растущее количество небезопасных устройств IoT; Кроме того, онлайн-видеотрафик для таких сервисов, как Zoom, стремительно растет - и неудивительно, что количество атак в этой вертикали за последние шесть месяцев увеличилось на 461 процент, говорят исследователи.

Между тем злоумышленники также проводят более изощренные атаки, чем когда-либо прежде. Согласно отчету, почти половина (52 процента) угроз использует три или более вектора, при этом количество атак с одним вектором «практически не существует».

Neustar также отслеживал новые методы усиления, которые способствуют более интенсивным атакам. В течение периода анализа была зафиксирована атака со скоростью более 800 миллионов пакетов в секунду (Mpps) - по сравнению с предыдущим рекордом в 500 Mpps.

Эти методы включают увеличение количества пакетных и импульсных DDoS-атак, расширение злоупотреблений встроенными сетевыми протоколами, такими как ARMS, WS-DD, CoAP и Jenkins, для запуска атак с усилением DDoS, которые могут выполняться с ограниченными ресурсами и вызывать значительные сбои, NXNS атаки, нацеленные на DNS-серверы, атаки RangeAmp, нацеленные на сети доставки контента (CDN), и возрождение вредоносных программ, подобных Mirai, способных создавать крупные бот-сети за счет эксплуатации плохо защищенных устройств IoT.

Атаки совпадают с аналогичными выводами, сделанными исследователями в августе». ***(Tara Seals. DDoS Attacks Skyrocket as Pandemic Bites // Threatpost (https://threatpost.com/ddos-attacks-skyrocket-pandemic/159301/). 16.09.2020).***

***

«Злоумышленники проверяют учетные данные Office 365 жертв в режиме реального времени, когда они вводятся на целевой странице фишинга, с помощью API проверки подлинности.

Исследователи обнаружили фишинговую атаку с использованием нового метода: злоумышленники используют API-интерфейсы аутентификации для проверки учетных данных Office 365 жертв - в режиме реального времени - по мере того, как они вводят их на целевую страницу.

API-интерфейсы аутентификации используются приложениями и службами, работающими от имени пользователей, для доступа к их данным, сообщил Threatpost Прашант Арун, глава отдела науки о данных в Armorblox. Office 365 требует регистрации приложений для использования API-интерфейсов, но для регистрации требуется только адрес электронной почты, что позволяет злоумышленникам легко использовать их. Некоторые дополнительные настройки

приложения также требуют, чтобы пользователи указали веб-сайт для «получения» аутентификационной информации, добавил Арун.

В ходе фишинг-атаки, недавно обнаруженной исследователями, злоумышленник использовал API-интерфейсы аутентификации для перекрестной проверки учетных данных старшего руководителя в крупной корпоративной фирме с каталогом Azure Active Directory организации. Active Directory (AD) - это проприетарная служба каталогов Microsoft, которая позволяет администраторам управлять разрешениями и доступом к сетевым ресурсам. API проверки подлинности используют Azure AD для предоставления служб проверки подлинности.

В случае фишинг-атаки доступ к этой немедленной обратной связи «позволяет злоумышленнику разумно реагировать во время атаки», - заявили в четверг исследователи Armorblox. «Злоумышленник также сразу узнает о действующих скомпрометированных учетных данных и позволяет ему потенциально снискать расположение к скомпрометированной учетной записи перед любым исправлением».

Фишинговое письмо

Атака была впервые обнаружена нацеленной на топ-менеджера неназванной компании, которая, по словам исследователей, является американским брендом, вошедшим в число 50 самых инновационных компаний мира в 2019 году. Первоначальное электронное письмо, отправленное сотруднику, имело тему «Отчет о дебетах ACH» "," Имитирующий внутренний отчет, и был отправлен в пятницу вечером, когда жертвы, вероятно, ослабили бдительность, говорят исследователи.

По словам исследователей, целевая компания недавно сменила домены, поэтому общедоступный адрес электронной почты цели отличается от доменного имени, используемого при его входе в Active Directory. Злоумышленники знали об этом изменении, что заставило исследователей полагать, что кампания была очень целевой.

«Ограниченная активность на веб-сайте, на котором размещена фишинговая атака, и точное время отправки электронного письма до вечера пятницы также предполагает, что это тщательно спланированная атака», - говорят исследователи. «По нашим оценкам, с начала июня на этот веб-сайт было совершено 120 случайных посещений. Редкое число показывает, что фишинговые мошенничества, скорее всего, являются целевыми, а не спреями и молитвами».

В фишинговом письме жертвам предлагалось: «Найти прилагаемый отчет о переводе денег» от 7/11/2020 2:53:14. Спасибо за ваш бизнес!». И указывается на вложение, которое выглядит как текстовый файл.

«При открытии вложения из Office 365 в браузере отображается веб-сайт, идентичный странице входа в Office 365. Имя пользователя было введено заранее. Отмечается нестандартное сообщение «Поскольку вы получаете доступ к конфиденциальной информации, вам необходимо подтвердить свой пароль», - заявили исследователи.

Перекрестная проверка учетных данных

После того, как жертвы ввели свои учетные данные на фишинговую целевую страницу, журналы входа в Azure Active Directory отображают попытку немедленного входа, соответствующую запросам XHR, выполненным на веб-странице вложений.

«Нет особой уязвимости, которая делает это возможным, это уникальное внедрение API злоумышленниками», - подчеркнул Арун в электронном письме Threatpost.

Если аутентификация прошла успешно, пользователь перенаправляется на zoom.com. Однако в случае сбоя аутентификации пользователь перенаправляется на login.microsoftonline.com. По словам исследователей, это может быть способом скрыть фишинговую атаку как еще одну неудачную попытку входа на портал Office 365. Если введенный текст пароля пустой или слишком короткий, пользователь вынужден повторить попытку.

«Наши исследователи угроз подтвердили, что сайт работает в режиме реального времени, обновив скрипт с помощью тестового входа и фиктивного пароля, и увидели неудачную попытку входа в систему из Прово, штат Юта, на портале входа в Azure Active Directory», - заявили исследователи. «Как и ожидалось, IP-адрес (162.241.120.106), с которого была предпринята попытка входа, является той же конечной точкой, на которую фишинговый скрипт отправляет учетные данные».

В ходе дальнейшего расследования исследователи обнаружили, что веб-сервис, стоящий за фишинговой страницей учетных данных, размещен на teenagemoglen [.] Com, который зарегистрирован на Alibaba.com у сингапурского регистратора доменов с конца мая 2020 года.

«Веб-сайт размещен в UnifiedLayer, хостинговой компании из Индии, в центре обработки данных в Прово, штат Юта, США», - сказали они. «Похоже, что на веб-сайте размещены веб-страницы, скопированные с другого веб-сайта. Ни одна из ссылок, которые позволяют активно взаимодействовать с посетителем, не выглядит активной». ***(Lindsey O'Donnell. Office 365 Phishing Attack Leverages Real-Time Active Directory Validation // Threatpost (https://threatpost.com/office-365-phishing-attack-leverages-real-time-active-directory-validation/159188/). 11.09.2020).***

***

«Компанія Microsoft повідомила, що в 2019 році заблокувала понад 13 млрд шкідливих і підозрілих листів, з яких понад 1 млрд містили посилання на фішингові (підроблені) сторінки для отримання облікових даних. Про це йдеться в щорічній доповіді з кібербезпеки, опублікованому на сайті компанії.

Зазначається, що у першій половині 2020 року загальний обсяг атак збільшився приблизно на 35% в порівнянні з другою половиною 2019 року.

«Найбільше атак відбувалися з Росії», – йдеться в звіті.

У Microsoft повідомили, що 52% атак NSN виходять з Росії, далі ідуть Іран (25%), Китай (12%), КНДР (11%).

Найбільше атак припадає на США (69%), Великої Британію (19%), Канаду (5%), Південну Корею (4%), Саудівську Аравію (3%)». ***(Компанія Microsoft заявила, що більшість кібератак здійснюють хакери з Росії // Українські***

медійні системи (https://glavcom.ua/news/kompaniya-microsoft-zayavila-shcho-bilshist-kiberatak-zdiysnyuyut-hakeri-z-rosiji-708274.html). 30.09.2020).

***

«Інформаційне агентство Bloomberg повідомило, що комп'ютерні системи щонайменше 13 департаментів в американському штаті Вашингтон піддалися кібератаці, яка тривала тиждень і заподіяла шкоду.

Невідомі хакери заразили шкідливим вірусом сервери в'язниць, парків, зон відпочинку, рибних промислів і природних заповідників.

"Мотиви зловмисників поки не встановлені, і невідомо, чи вкрали вони цінну інформацію. Виборча система Вашингтона не постраждала", – відзначає Bloomberg. Місцева влада звернулася за допомогою до Федеральних департаменту внутрішньої безпеки, ФБР і Microsoft». ***(Лиза Солнцева. Влада штату Вашингтон стали цілью тижневої кібератаки // ІА "ЄУРАБОТА" (https://news.eurabota.ua/uk/usa/developments/vlada-shtatu-vashington-stali-cilju-tizhnevoi-kiberataki/). 29.09.2020).***

***

«Комп'ютерна система американської компанії Universal Health Services, що нараховує понад 400 медичних установ, стала об'єктом нападу хакерів, які потребують викупу…

…характеристики кібератаки "виглядають як вимога викупу". Невідомі в минулі вихідні використовували шкідливу програму, яка, вразивши комп'ютерну систему Universal Health Services, почала шифровувати файли. Зазвичай хакери вимагають заплатити викуп в обмін на пароль, що дозволяє розшифрувати ці файли.

За даними джерел телеканалу, часом для диверсії були навмисно обрані вихідні. У ці дні в медустановах присутньо мало технічного персоналу, здатного оперативно відреагувати і звести наслідки кібератаки до мінімуму. В даному випадку лікарям і медсестрам довелося перейти на паперову технологію, заповнюючи необхідні бланки від руки.

Universal Health Services є однією з найбільших в США приватних компаній, що надають послуги в галузі охорони здоров'я. Штаб-квартира підприємства розташована в штаті Пенсільванія, кількість співробітників за станом справ на минулий рік досягало 90 тис». ***(Хакери в США вивели з ладу мережу компаній медичних послуг // Інформаційне агентство «1NEWS» (https://1news.com.ua/svit/hakery-v-ssha-vyvely-z-ladu-merezhu-kompanij-medychnyh-poslug.html). 29.09.2020).***

***

«Найбільший телекомунікаційний оператор країни Magyar Telekom заявляє про кібератаку на деякі банківські й телекомунікаційні мережі.

…про це оператор заявив у суботу, 26 вересня.

Самі атаки сталися у четвер, 24 вересня, спричинивши збої у роботі систем.

Згідно з повідомленням оператора, DDoS-атаку здійснили із серверів, розташованих у Росії, Китаї та В'єтнамі.

"Це була одна з найбільших в історії країни кібератак - і за своїми масштабами, і складністю, - повідомляє компанія. - Російські, китайські та в'єтнамські хакери спробували здійснити DDoS-атаку проти фінансових установ Угорщини, а також вразити мережі Magyar Telekom".

Слід зауважити, що розташування серверів не означає, що й самі виконавці атаки знаходилися у цих країнах.

Об'єм трафіку даних, використаний під час неї, був у 10 разів вищим, ніж зазвичай, а сама атака відбувалася у декілька "хвиль".

Угорський OTP Bank також підтвердив, що зазнав атаки.

"У четвер була здійснена DDoS-атака на телекомунікаційні системи, що обслуговують одну з наших банківських послуг. Ми відбили атаку разом з Telekom, який також постраждав, і нетривалий збій у роботі сервісів після обіду було ліквідовано", - повідомили в OTP». ***(В Угорщині кажуть про кібератаку на декілька банків і телекомунікаційних мереж // Українська правда (https://www.pravda.com.ua/news/2020/09/26/7267826/). 26.09.2020).***

***

«Журналисты издания Bleeping Computer заметили, что создатели вымогателя REvil (он же Sodinokibi) внесли один миллион долларов в биткоинах на депозит на русскоязычном хакерском форуме. Таким образом хакеры хотят доказать потенциальным партнерам, что серьезно относятся к делу.

Дело в том, что REvil работает по схеме RaaS (Ransomware-as-a-Service, «Вымогатель-как-услуга»), то есть в данном случае разработчики малвари отвечают именно за разработку и поддержку, тогда как распространением и непосредственно взломом занимаются их клиенты и партнеры. Как правило, при таком «разделении труда» разработчики малвари получают долю 20-30%, тогда как распространителям остается 70-80% полученных выкупов.

Недавно создатели REvil объявили, что они ищут новых партнеров для распространения своих вымогательских программ. Хакеры писали, что заинтересованы в работе со знающими людьми и теми, кто имеет опыт в области пентеста.

Чтобы показать потенциальным партнерам серьезность своих намерений, разработчики REvil создали депозит на хакерском форуме в размере 99 биткоинов (примерно 1 миллион долларов по текущему курсу). Как нетрудно понять, данный ресурс позволяет участникам вносить криптовалюту в кошелек, привязанный к сайту. Пользователи не только могут видеть размеры депозитов друг друга, но и использовать эти биткоины для совершения сделок через форум.

Журналисты отмечают, что размер депозита REvil хорошо иллюстрирует, сколько денег приносят хакерам вымогательские атаки. Судя по всему, злоумышленников не слишком беспокоит, что в теории администрация форума может похитить у них такую сумму». ***(Мария Нефёдова. Разработчики REvil внесли миллион долларов на депозит на хакерском форуме // Хакер (https://xakep.ru/2020/09/29/revil-million/). 29.09.2020).***

***

«Крупнейший в мире производитель часов Swatch Group отключил свои IT-системы после выявления кибератаки. Как сообщили представители компании изданию BleepingComputer, они обнаружили кибератаку на выходных и отключили IT-системы с целью предотвратить распространение вредоносного ПО.

«Swatch Group немедленно оценила и проанализировала характер атаки, приняла соответствующие меры и внесла необходимые исправления. Ситуация вернется в норму как можно скорее», — сообщили представители компании.

Это далеко не первая кибератака, направленная против крупных кампаний в этом месяце. Например, ранее крупнейший итальянский производитель очков Luxottica и владелец бренда Ray-Ban подвергся кибератаке, которая привела к остановке производства продукции в Италии и Китае. Порталы Luxottica one.luxotrica.com и University.luxottica.com демонстрировали сообщения о техническом обслуживании сайтов.

На этой неделе одна из крупнейших в США частных компаний, Universal Health Services (UHS), предоставляющая услуги в области здравоохранения, была вынуждена отключить свои компьютерные системы вследствие кибератаки. Под управлением UHS находится более 400 медицинских учреждений в США и Великобритании, компания ежегодно предоставляет медицинские услуги порядка 3,5 млн пациентов». ***(Крупнейший производитель часов Swatch стал жертвой кибератаки // SecurityLab.ru (https://www.securitylab.ru/news/512587.php). 30.09.2020).***

***

Діяльність хакерів та хакерські угруповування

«Экспертный центр безопасности компании Positive Technologies (PT ESC) выявил очередную атаку группировки Winnti, а также изучил ее новый инструментарий и инфраструктуру. На сегодня обнаружены десятки зараженных систем по всему миру, включая Россию, США, Японию, Южную Корею, Германию, Монголию, Беларусь, Индию, Бразилию и пр. Некоторые скомпрометированные организации специалистам PT ESC удалось идентифицировать, все они получили соответствующие уведомления об имеющихся рисках по линии национальных CERT.

В рамках исследования угроз информационной безопасности (Threat Intelligence), специалисты PT ESC обнаружили бэкдор xDll, не известный ранее, а также ряд других образцов вредоносного ПО – как уже известного, так и нового. Детальный анализ вредоносного ПО, данные о сетевой инфраструктуре и даже информация о жертвах позволили соотнести выявленный бэкдор с активностью группировки Winnti (APT41, Barium и Axiom), происходящей из Китая и атакующей организации по всему миру по меньшей мере с 2012 г. Ключевые ее интересы – шпионаж и получение финансовой выгоды. За все время активности этой группировки ее жертвами становились компании авиационно-космической

промышленности, энергетики, фармацевтической, финансовой и телекоммуникационной отраслей и даже игровой индустрии.

Изученная экспертами PT ESC новая инфраструктура группы Winnti стремительно разрастается: выявлено более 150 IP-адресов контрольных серверов и не менее 147 доменов, связанных с этими адресами. Около половины серверов группировки находятся в Гонконге. IP-адреса распределены по 45 различным провайдерам, при этом более половины серверов сконцентрированы на IP-адресах шести провайдеров, пять из которых находятся в Азии – в Гонконге, Китае, Южной Корее.

При этом прямо во время исследования инфраструктуры специалисты Positive Technologies наблюдали, как злоумышленники многократно переводили домены с одного IP-адреса на другой. Все это свидетельствует об активной фазе атаки.

На сегодня под управлением группировки уже более 50 систем по всему миру, карта часовых поясов атакованных устройств совпадает с традиционной географией интересов группировки.

Среди пострадавших организаций оказалось пять разработчиков ПО для финансовых организаций из Германии и России. Анализ используемого злоумышленниками инструментария, техник и тактик позволяет утверждать, что в ряде случаев речь идет о первых этапах атаки типа supply chain. В частности, атакованные производители специфического ПО, являющиеся доверенным поставщиком ПО для целого ряда компаний, с большой долей вероятности будут использованы как плацдарм для развития атаки.

Как показывает практика, все большую популярность среди APT-группировок приобретают атаки на организации через менее защищенных партнеров, поставщиков, клиентов и пр. Фишинг такого типа входит сегодня в Топ-3 наиболее эффективных и часто используемых методов атаки. Нередко атакам подвергаются и ИТ-компании – разработчики ПО и системные интеграторы. Эти атаки – supply chain и trusted relationship – часто оказываются частью более сложных атак на промышленные, государственные организации или банки.

Во время исследования эксперты Positive Technologies также выявили пересечения новой инфраструктуры Winnti с инфраструктурой других групп, что может говорить о причастности Winnti к другим атакам, существующие данные об организаторах и участниках которых оказались не верны.

В частности обнаружен бэкдор ShadowPad, который используется группой Winnti. При изучении его инфраструктуры выявилены связанные домены, ранее использовавшиеся при атаках на организации в России, Беларуси, Южной Корее и Японии, которые, как тогда считалось, проводили группы TA459 и Tonto team. Также выявлены инфраструктурные пересечения с группировкой Nettraveller». ***(Группа Winnti заражает разработчиков софта, создавая плацдарм для сложных атак // Компьютерное Обозрение (https://ko.com.ua/gruppa_winnti_zarazhaet_razrabotchikov_softa_sozdavaya_placdarm_dlya_slozhnyh_atak_134431). 09.09.2020).***

***

«У четвер, 3 вересня, невідомі хакери зламали сайт МВС Білорусі й "оголосили" в розшук самопроголошеного президента країни Олександра Лукашенка.

Також у розшук "оголосили" главу МВС Білорусі Юрія Караєва.

Лукашенка та Караєв звинувачуються в "злочинах проти білоруського народу". Лукашенка також звинувачують в "узурпації влади"…». ***(Хакери зламали сайт МВС Білорусі й "оголосили" Лукашенка і Караєва в розшук // Рубрика (https://rubryka.com/2020/09/04/hakery-zlamaly-sajt-mvs-bilorusi-j-ogolosyly-lukashenka-i-karayeva-v-rozshuk/). 04.09.2020).***

***

«Білоруські хакери оголосили про тотальну атаку на режим президента Білорусі Олександра Лукашенка…

Про це йдеться в телеграм-каналі “Кібер Партизани”.

Хакери повідомляють про “тотальну атаку” на режим Лукашенка з 24 по 30 вересня.

При цьому вони додають, що спеціально не публікують попередження, щоб не зірвати свій план дій.

Зазначається, що в жовтні почнеться набір нових кібер-партизанів». ***(“Тотальну атаку” на режим Лукашенка оголосили білоруські хакери // Інформаційне агентство «1NEWS» (https://1news.com.ua/svit/totalnu-ataku-na-rezhym-lukashenka-ogolosyly-biloruski-hakery.html). 24.09.2020).***

***

«На прошедших выходных группа хакеров опубликовала в открытом доступе имена и другие персональные данные более 1 тыс. высокопоставленных служащих МВД Республики Беларусь.

Имена, даты рождения и сведения о занимаемой должности сотрудников МВД распространяются через сервис «Таблицы Google». Большая часть данных принадлежит высокопоставленным лицам в должности лейтенанта, майора и капитана.

Кроме того, хакеры предоставили похищенные данные белорусскому изданию Nexta, опубликовавшему неотредактированную версию таблиц на своем Telegram-канале. Издание обратилось к своим читателям с просьбой не только помочь в проверке подлинности данных, но и предоставить дополнительные сведения о милиционерах (адреса, номера телефонов, номера автомобилей, информацию о правонарушениях и пр.), если таковые у них имеются.

На момент написания новости официальный сайт министерства был недоступен». ***(В Сети опубликованы персональные данные белорусских милиционеров // SecurityLab.ru (https://www.securitylab.ru/news/512289.php). 21.09.2020).***

***

«…Хакери однієї з іноземних держав атакували та викрали дані з грузинського Дослідницького центру громадської охорони здоров'я імені Річарда Лугара.

Кібератака була здійснена 1 вересня на комп'ютерні системи центрального офісу та структурних підрозділів МОЗ Грузії.

Хакери викрали з бази лабораторії Лугара медичну документацію і «важливу інформацію» про боротьбу з пандемією коронавірусу, стверджують в міністерстві. Частина цих даних виявилася у відкритому доступі.

У МВС Грузії зазначають, що при цьому разом зі справжніми незаконно здобутими документами на «одному із зарубіжних веб-сайтів» розміщені фальшиві дані. У відомстві вважають, що таким чином кіберзлочинці хочуть залякати громадськість.

«Згідно з отриманими на даному етапі доказам, кібератака була здійснена спецслужбою однієї з іноземних держав», – зазначено в заяві.

Найближчим часом МВС Грузії планує звернутися до відповідних служб країн-партнерів з проханням про надання допомоги в розслідуванні кіберзлочину.

Одночасно відомство обіцяє періодично інформувати громадськість про хід слідства…» ***(Хакери викрали з грузинської лабораторії дані про боротьбу з Covid-19 // Українські медійні системи (https://glavcom.ua/news/hakeri-vikrali-z-gruzinskoji-laboratoriji-dani-pro-borotbu-z-covid-19-703165.html). 04.09.2020).***

***

«С сентября 2019 года хакерская группа Strontium, которую связывают с ГРУ России, совершила кибератаки на более чем 200 организаций, прямо или косвенно связанных с предстоящими выборами президента США. Об этом говорится в заявлении вице-президента Microsoft по безопасности Тома Берта.

По его информации, в течение последних месяцев российские хакеры пытались атаковать сотрудников компании SKDKnickerbocker из Вашингтона, которая работает с кандидатом в президенты США от Демократической партии Джо Байденом и другими влиятельными демократами. Получить доступ к компьютерным сетям компании злоумышленникам не удалось.

В свою очередь пресс-секретарь российского президента Дмитрий Песков назвал эти обвинения «чепухой». Представители России последовательно отрицают причастность к вмешательству в выборы в других странах.

Джон Халтквист, топ-менеджер компании FireEye, специализирующейся на кибербезопасности, заявил, что активность российских хакеров представляет наибольшую опасность, так как они склонны к «разрушительным действиям». ***(Российские хакеры пытались взломать сети фирмы, связанной с Байденом // АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/407387-rossijskie_hakery_pytalisj_vzlomatj_seti_firmy_svjazannoj_s_bajdenom). 11.09.2020).***

***

«В недавней атаке киберпреступная группа TeamTNT использовала законный инструмент, чтобы избежать развертывания вредоносного кода в

скомпрометированной облачной инфраструктуре и по-прежнему хорошо ее контролировать.

Они использовали инструмент с открытым исходным кодом, специально созданный для мониторинга и управления облачными средами с установками Docker и Kubernetes, что уменьшило их влияние на взломанный сервер.

Неправильное использование инструмента торговли

Анализируя атаку, исследователи из Intezer обнаружили, что TeamTNT установила инструмент с открытым исходным кодом Weave Scope, чтобы получить полный контроль над облачной инфраструктурой жертвы.

По их словам, это может быть первый случай злоупотребления законным сторонним инструментом для выполнения роли бэкдора в облачной среде, что также указывает на эволюцию этой конкретной группы.

Weave Scope легко интегрируется с Docker, Kubernetes, распределенной облачной операционной системой (DC / OS) и AWS Elastic Compute Cloud (ECS). Он предоставляет полную карту процессов, контейнеров и хостов на сервере, а также контроль над установленными приложениями.

«Злоумышленники устанавливают этот инструмент, чтобы отобразить облачную среду своей жертвы и выполнить системные команды без развертывания вредоносного кода на сервере», - отмечает Intezer в сегодняшнем отчете.

Описывая поток атаки в результате инцидента, исследователи говорят, что путь TeamTNT заключался в открытом Docker API. Это позволило им создать чистый контейнер Ubuntu, настроенный для монтирования на сервере-жертве, таким образом получив доступ к файлам на хосте.

Затем они настраивают локального пользователя с именем «hilde» с повышенными привилегиями и используют его для подключения к серверу через SSH. Установка Weave Scope - это следующий шаг в атаке, для которой требуется всего три команды для загрузки, установки разрешений в приложении Scope и запуска.

С помощью утилиты на сервере TeamTNT может подключаться к панели управления Weave Scope через HTTP через порт 4040 (по умолчанию для конечной точки приложения Scope) и брать на себя управление.

Исследователи говорят, что этот сценарий, хотя и редкий, можно было бы предотвратить, если бы порты Docker API были закрыты или существовали политики ограниченного доступа.

Другая неправильная конфигурация - это разрешение подключения к панели инструментов Weave Scope извне сети. В документации к инструменту четко сказано, что порт 4040 не должен быть доступен через Интернет…». ***(Ionut Ilascu. Hackers use legit tool to take over Docker, Kubernetes platforms // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hackers-use-legit-tool-to-take-over-docker-kubernetes-platforms/). 08.09.2020).***

***

«Иранские «правительственные» хакеры из группировки Pioneer Kitten (она же Fox Kitten и Parisite) торгуют доступом к сетям скомпрометированных компаний на хакерских форумах, сообщают специалисты Crowdstrike.

Напомню, что в 2019-2020 годах эта группировка провела серию атак с использованием уязвимостей в VPN и сетевом оборудовании. К примеру, хакеры эксплуатировали:

корпоративные VPN Pulse Secure (CVE-2019-11510);

VPN-сервера Fortinet под управлением FortiOS (CVE-2018-13379);

VPN-серверы Palo Alto Networks «Global Protect» (CVE-2019-1579);

ADC-серверы Citrix и сетевые шлюзы Citrix (CVE-2019-19781);

балансировщики нагрузки F5 Networks BIG-IP (CVE-2020-5902).

По информации компании Dragos, группировка взламывала сетевые устройства, используя перечисленные уязвимости, оставляла в сетях организаций бэкдоры, а затем предоставляла доступ к ним другим иранским хакерским группам, включая APT33 (Elfin, Shamoon), APT34 (Oilrig) и APT39 (Chafer).

Теперь же эксперты Crowdstrike сообщают, что Pioneer Kitten не только делится доступом с « коллегами», но и продает доступ к некоторым взломанным сетям на хакерских форумах, по крайней мере, с июля 2020 года. Исследователи полагают, что таким образом группировка пытается диверсифицировать свои доходы и монетизировать доступ к сетям, которые не имеют никакой ценности для иранских спецслужб». ***(Мария Нефёдова. Иранские хакеры продают доступ к сетям взломанных компаний // Xakep (https://xakep.ru/2020/09/01/access-for-sale/). 01.09.2020).***

***

«Связанная с Китаем группа угроз RedDelta продолжала проводить кибератаки на католические учреждения с мая 2020 года до последней недели.

Спонсируемая государством группа угроз, связанная с Китаем, участвовала в пятимесячной кибератаке против Ватикана и других организаций, связанных с католической церковью. Атаки осуществлялись в форме целевых фишинговых писем, в которых использовался инструмент удаленного доступа PlugX (RAT) в качестве полезной нагрузки.

Исследователи из Recorded Future наблюдали, как группа RedDelta атакует почтовые серверы католических организаций с начала мая 2020 года. Это происходит в преддверии ожидаемого в сентябре 2020 года продления знаменательного временного соглашения между Китаем и Ватиканом 2018 года, которое называется сделкой Китая и Святейшего Престола. В сети интрузии не произошло вплоть до недели, прежде чем Министерство иностранных дел Китая объявило о том, что сделка была «успешно реализован» на прошлой неделе, 10 сентября, говоря возобновление сделки как ожидается, будет объявлено в ближайшие недели - в этот момент По словам исследователей, наблюдаемая активность угрозы прекратилась.

Исследователи полагают, что это нападение на Ватикан и другие организации, связанные с католической церковью, вероятно, дало бы RedDelta представление о переговорной позиции Святейшего Престола перед продлением сделки в сентябре 2020 года.

«RedDelta в основном оставалась невозмутимой из-за обширных публичных сообщений о том, что она нацелена на Ватикан и другие католические

организации», - утверждают исследователи Insikt Group из Recorded Future в отчете, опубликованном во вторник. «Несмотря на принятие основных оперативных мер безопасности путем изменения статуса разрешения доменов командования и контроля (C2) сразу после этого отчета, тактика, методы и процедуры группы (ДТС) остались неизменными».

RedDelta также расширила свою виктимологию своих кампаний, о чем свидетельствуют новые целевые фишинговые атаки с использованием ложных документов, посвященных католицизму, отношениям Тибета и Ладакха и Совету Безопасности Генеральной Ассамблеи Организации Объединенных Наций против других католических институтов; а также дополнительные сетевые вторжения, нацеленные на правительственные системы Мьянмы и два университета Гонконга.

Кибератаки на Ватикан

Начиная с начала мая 2020 года исследователи наблюдали, как RedDelta предпринимала попытки различных сетевых вторжений, нацеленных на Ватикан, а также на другие организации, такие как Гонконгская исследовательская миссия в Китае и Папский институт иностранных миссий (PIME), Италия.

Ранее исследователи в июльском отчете пролили свет на успешную атаку группы угроз на Ватикан, которая распространила PlugX RAT. PlugX ранее использовался в атаках, направленных на правительственные учреждения, и позволяет удаленным пользователям осуществлять кражу данных или брать под контроль уязвимые системы без разрешения или авторизации. Он может копировать, перемещать, переименовывать, выполнять и удалять файлы; регистрировать нажатия клавиш; отпечаток пальца зараженной системы; и более.

Исследователи полагают, что кибератака изначально была инициирована с помощью целевых фишинговых писем с приманкой. С мая по июль они использовали контроллер RAT и методы анализа сетевого трафика для определения нескольких серверов PlugX C2, которые обмениваются данными с хостами Ватикана. Исследователи также выявили инфраструктуру Poison Ivy и Cobalt Strike Beacon C2, которая в это время обменивалась данными с хостами Ватикана.

После того, как Recoded Future опубликовала подробности этой кампании в июльском отчете, они отметили, что группа RedDelta предприняла ряд уклончивых шагов, связанных с инфраструктурой, чтобы избежать обнаружения, в частности, изменив разрешение IP в нескольких своих доменах C2.

«При анализе связи между целевыми организациями и инфраструктурой RedDelta C2 с использованием анализа записанного будущего сетевого трафика мы обнаружили, что сетевое взаимодействие между католическими церковными организациями прекратилось сразу же после публикации отчета», - заявили они. «Однако это длилось недолго, и в течение 10 дней группа вернулась к своей атаке на почтовый сервер католической епархии Гонконга, а через 14 дней - на почтовый сервер Ватикана. Это свидетельствует о настойчивости RedDelta в поддержании доступа к этим средам для сбора разведывательной информации в дополнение к вышеупомянутой группе высокой толерантности к риску».

С тех пор неясно, смогла ли группа успешно восстановить доступ к сети Ватикана, однако попытки сделать это, а также появление новой приманки на тему католической церкви RedDelta подчеркивают всеохватывающее внимание Китая.

По их словам, Коммунистическая партия (КПК) стремится усилить надзор за католической общиной в Китае.

Расширение виктимологии

Исследователи заявили, что RedDelta также нацелена на католические организации, а также на новые сетевые вторжения, затрагивающие правоохранительные и правительственные органы в Индии, правительственную организацию в Индонезии и другие неопознанные цели в Мьянме, Гонконге и Австралии.

Увеличение числа жертв было замечено в том, что группа угроз изменила свои приманки, используемые в кампаниях. Ранее группа угроз сосредоточилась на документах о приманках, ориентированных на католиков, в том числе на одном, якобы официальном письме Ватикана, адресованном нынешнему главе Гонконгской исследовательской миссии в Китай, и на подделке бюллетеня новостей Союза католических новостей Азии, касающегося грядущее введение в действие нового закона Гонконга о национальной безопасности.

Совсем недавно группа была замечена с помощью дополнительных приманок, ссылающихся на католиков в Китае, отношений Тибета и Ладакха и Совета Безопасности Генеральной Ассамблеи ООН, чтобы попытаться загрузить PlugX на целевые машины. Например, один обнаруженный образец приманки, документ-приманка под названием «История отношений Тибет-Ладакх и их современные последствия», использует законный исполняемый файл Microsoft Word для боковой загрузки загрузчика DLL первого уровня с двумя файлами, изначально хранящимися в zip-архиве. файл. После первой фазы боковой загрузки DLL зашифрованная полезная нагрузка PlugX DAT удаляется.

По словам исследователей, ТТП RedDelta «продолжают работать в соответствии со стратегическими приоритетами Китая». Например, продолжающееся нападение группы на Ватикан, использование ею целевых ложных документов, посвященных текущим геополитическим вопросам, имеющим отношение к Китайской Народной Республике (КНР), и ее конечные цели кибершпионажа отражают группы угроз, связанных с Китаем, считают исследователи.

«Повторное использование группой публично известной инфраструктуры и TTP, вероятно, свидетельствует о том, что группа добивается успеха в работе, и подчеркивает прагматический подход к операционной безопасности, при этом RedDelta желает продолжать использовать публично известную инфраструктуру, пока сохраняется доступ», - заявили исследователи». ***(Lindsey O'Donnell. Hackers Continue Cyberattacks Against Vatican, Catholic Orgs // Threatpost (https://threatpost.com/hackers-continue-cyberattacks-against-vatican-catholic-orgs/159306/). 16.09.2020).***

***

«Два хакера якобы взломали более 50 веб-сайтов, размещенных в США, и испортили их проиранскими сообщениями.

Министерство юстиции (DoJ) предъявило обвинение двум хакерам, в том числе одному подростку, якобы в вандализме более чем на 50 веб-сайтах, размещенных в США, с проиранскими сообщениями.

Обвинительное заключение, распечатанное во вторник, обвиняет Бехзада Мохаммадзаде, гражданина Исламской Республики Иран, которому предположительно 19 лет, и Марвана Абусрура, гражданина Палестинской администрации без гражданства, которому предположительно 25 лет. Обоим были предъявлены обвинения по одному пункту обвинения в сговоре с целью умышленного повреждения защищенного компьютера и по одному пункту обвинения в умышленном повреждении защищенного компьютера.

Считается, что обвиняемые проживают в Иране и Палестине и разыскиваются властями США.

«Этих хакеров обвиняют в организации наглой кибер-атаки, в результате которой были испорчены десятки веб-сайтов по всей стране, чтобы выразить протест и отомстить Соединенным Штатам за убийство лидера иностранной террористической организации», - сказал Джозеф Бонаволонта, ответственный специальный агент. из Бостонского отделения ФБР в заявлении во вторник. «Теперь они разыскиваются ФБР и больше не могут свободно выезжать за пределы Ирана или Палестины без риска ареста».

Уничтожение веб-сайта произошло после того, как конфликт между США и Ираном достиг своего пика в начале 2020 года, когда 3 января американские беспилотники убили Касема Сулеймани, иранского генерала из Корпуса стражей исламской революции, которого очень уважали в Иране. Сразу после убийства Сулеймани иранские лидеры пообещали отомстить.

По пятам этого инцидента Мохаммадзаде и Абусрур якобы работали вместе над повреждением 51 веб-сайта, размещенного в США. Некоторые из них были размещены на компьютерах, принадлежащих компании, штаб-квартира которой находится в Массачусетсе. Эти двое якобы заменили содержание этих сайтов фотографиями Сулеймани на фоне иранского флага вместе с сообщением на английском языке «Долой Америку». Два хакера якобы взяли кредит онлайн за дефейсы своих веб-сайтов.

Веб-сайт по крайней мере одного правительственного агентства США - веб-сайт Федеральной депозитарной библиотеки (FDLP) - также был искажен в это время, хакеры, стоящие за атакой, ссылались на смерть Сулеймани на целевой странице FDLP и включали фотографию окровавленного президента Дональда. Трампу бьют по лицу и проиранские послания. Однако неясно, был ли этот веб-сайт одним из 51, предположительно атакованных Мохаммадзаде и Абусруром.

Мохаммадзаде и Абусрур якобы уничтожали веб-сайты задолго до инцидента 2 января. Согласно обвинительному заключению, Мохаммадзаде публично заявил, что начиная с 2018 года лично испортил более 1100 веб-сайтов по всему миру с помощью проиранских и хакерских сообщений.

Между тем Абусрур является спамером, который сам себя называет (который рассылает незапрашиваемые электронные письма с целью получения прибыли), а также незаконным торговцем украденными кредитными картами, который публично заявил, что испортил по меньшей мере 337 веб-сайтов по всему миру,

которые он якобы начал не позднее, чем 6 июня 2016 г. и продолжаться как минимум до июля этого года.

Эти двое якобы начали работать вместе примерно 26 декабря, когда Абусрур начал предоставлять Махаммадзаде доступ к взломанным веб-сайтам. Хотя Министерство юстиции не указало, как эти двое якобы получили доступ к веб-сайтам, популярные методы взлома могут включать уязвимости в сторонних плагинах и украденные учетные данные для входа.

Согласно Министерству юстиции, обвинение в сговоре с целью умышленного повреждения защищенного компьютера предусматривает наказание в виде лишения свободы сроком до пяти лет, трех лет контролируемого освобождения и штрафа в размере 250 000 долларов, что в два раза превышает прибыль или убыток (в зависимости от того, что больше).. Между тем, обвинение в умышленном повреждении защищенного компьютера предусматривает наказание в виде тюремного заключения на срок до 10 лет, три года освобождения под надзором и штраф в размере 250 000 долларов США, что в два раза превышает прибыль или убыток (в зависимости от того, что больше).

«Сегодняшнее обвинительное заключение должно послать мощный сигнал о том, что мы без колебаний будем преследовать любого, кто совершает злонамеренные кибер-вторжения против ни в чем не повинных американцев, чтобы вызвать хаос, страх и экономический ущерб», - говорится в заявлении Бонаволонты». ***(Lindsey O'Donnell. DoJ Indicts Two Hackers for Defacing Websites with Pro-Iran Messages // Threatpost (https://threatpost.com/doj-indicts-hackers-pro-iran/159293/). 16.09.2020).***

***

«Хакери з Азербайджану здійснили кібератаку на провідні ЗМІ Вірменії та інші новинні сайти.

Таку інформацію повідомили у пресцентрі Служби нацбезпеки Вірменії…

«Служба національної безпеки Республіки Вірменія повідомляє, що 1in.am, armenpress.am, news.am, mamul.am та ряд інших сайтів новин знаходиться в домені сервера іноземної компанії «Cloudflare» на договірній основі; азербайджанські хакери змінили налаштування цих сайтів, які були виправлені за короткий час», — йдеться у повідомленні.

У СНБ Вірменії додали, що професійний персонал, який підтримує сайти новин, «постійно отримує відповідну підтримку з міркувань безпеки». ***(Азербайджанські хакери здійснили кібератаку на провідні ЗМІ Вірменії // Чорноморські новини (https://www.blackseanews.net/read/168707). 28.09.2020).***

***

Вірусне та інше шкідливе програмне забезпечення

«Компания Eset обнаружила вредонос, который нацелен на софтсвичи my VoIP-платформы на ОС Linux. Данная платформа довольно специфична и используется двумя коммутаторами: Linknat VOS2009 и VOS3000.

Софтсвич (от англ. softwitch, software switch) – основной элемент VoIP-сети, который позволяет контролировать вызовы и биллинг, а также управлять звонками. При помощи CDRThief злоумышленники похищают приватную информацию, например, метаданные звонков, среди которых номера телефонов и IP-адреса пользователей, продолжительность звонка, его стоимость и др. Для получения перечисленных сведений вредонос отправляет запрос к внутренним базам данных MySQL, используемым софтсвичем.

Эксперты отмечают, что злоумышленники хорошо изучили внутреннюю архитектуру атакуемой платформы. Чтобы получить доступ к базе MySQL, вредонос считывает учетные данные из Linknat – конфигурационных файлов VOS2009 и VOS3000. При этом пароли конфигурационных файлов хранятся в зашифрованном виде, но CDRThief способен их расшифровать.

Вредоносная программа может быть развернута в любом месте на диске с любым именем файла. При этом она способна встраиваться в обычную загрузочную цепочку платформы и маскироваться под компонент софтсвича Linknat.

В настоящее время сложно определить конечную цель злоумышленников, однако есть предположение, что она состоит в кибершпионаже и мошенничестве». ***(Вредонос CDRThief перехватывает данные софтсвичей VoIP-платформы // Компьютерное Обозрение (https://ko.com.ua/vredonos_cdrthief_perehvatyvaet_dannye_softsvichej_voip-platformy_134468). 11.09.2020).***

***

«Компания Eset обнаружила новый троян KryptoCibule, который нацелен на кражу и добычу криптовалюты. Вредонос обладает широким набором функций: криптомайнинг с использованием зараженной машины, перехват данных из буфера обмена и вывод файлов из целевой системы (эксфильтрация). Например, с помощью KryptoCibule можно подменить данные криптокошелька в буфере обмена, что приведет к отправке средств на счет злоумышленника.

KryptoCibule нацелен преимущественно на жителей Чехии и Словакии, поэтому его название состоит из «Krypto» и «Cibule», что в переводе означает «лук». Такое название связано с тем, что операторы malware используют «луковые» службы для осуществления вредоносных действий.

KryptoCibule попадает на устройство жертвы в ZIP-архиве при загрузке торрента с пиратским контентом.

При запуске инсталлятора на компьютере пользователя разворачивается вредоносное ПО. При этом KryptoCibule использует различные способы защиты от обнаружения». ***(Троян KryptoCibule атакует пользователей торрент-трекеров // Компьютерное Обозрение (https://ko.com.ua/troyan_kryptocibule_atakuet_polzovatelej_torrent-trekerov_134365). 04.09.2020).***

***

«Компанія Apple добре відома своїми жорсткими правилами. І, зазвичай, це допомагає їй уникнути прослизанню шкідливого ПЗ у свій магазин застосунків. Торік компанія ввела нову систему нотарізації програмного забезпечення. Згідно з нею, будь-який додаток або оновлення мають бути підписані розробником і завірені самою Apple. Програми, яким не вдалося пройти перевірку блокуються на macOS, навіть якщо вони поширюються не через Mac App Store.

Але від помилок ніхто не застрахований. Фахівці з кібербезпеки (Patrick Wardle та Peter Dantini) встановили, що компанія випадково дала дозвіл шкідливій програмі Shlayer працювати на macOS. ПЗ маскувалося під оновлення для Adobe Flash Player і пройшло необхідну верифікацію. Фахівці вперше зіткнулися з подібною ситуацією.

Shlayer – це відоме шкідливе ПЗ, яке було найпоширенішою загрозою для macOS у 2019 році. Воно може перехоплювати зашифрований Інтернет-трафік і заміняти результати пошуку шахрайською рекламою. Apple зреагувала досить швидко. Компанія відкликала свій дозвіл та відключила обліковий запис розробника цього плагіна. Згодом розробник шкідливого ПЗ спробував знову проникнути у App Store, але спроба виявилася безуспішною». ***(Apple випадково пропустила шкідливу програму в App Store // Pingvin Pro (https://pingvin.pro/gadgets/news-gadgets/apple-vypadkovo-propustyla-shkidlyvu-programu-v-app-store.html). 02.09.2020).***

***

«Исследователи вредоносных программ обнаружили новую угрозу, которую они назвали CDRThief, нацеленную на конкретную систему передачи голоса по IP для кражи записей данных о звонках (CDR) с оборудования телефонной станции.

Анализ вредоносного ПО показал, что он был специально создан для конкретной платформы Linux VoIP, а именно для программных коммутаторов Linknat VOS2009 / 3000.

Программный коммутатор - это программное решение, действующее как сервер VoIP, который управляет трафиком (аудио / видео / текст) в телекоммуникационной сети. Это центральный элемент, обеспечивающий соединение между внутренними и внешними линиями.

Цель CDRThief - взломать программные коммутаторы VOS2009 / 3000 и украсть метаданные вызовов из внутренних баз данных MySQL, такие как IP-адреса вызывающих абонентов, номера телефонов, время начала и продолжительность вызова, его маршрут и тип.

Анализируя вредоносную программу, исследователи ESET обнаружили, что она пыталась скрыть вредоносные функции с помощью шифра Corrected Block TEA (XXTEA), а затем запускать кодировку Base64 для подозрительных ссылок.

Хотя доступ к базе данных MySQL защищен паролем, ключ зашифрован в файле конфигурации, CDRThief может читать и расшифровывать его, что указывает на то, что тот, кто его разработал, очень хорошо знает атакованную платформу.

ESET считает, что автору пришлось перепроектировать двоичные файлы платформы, чтобы получить в коде Linknat сведения об алгоритме шифрования (AES) и ключе, который расшифровывает пароль доступа к базе данных.

По функциям вредоносного ПО исследователи определили, что интерес CDRThief представляют таблицы, содержащие журналы системных событий, информацию о шлюзах VoIP и метаданные вызовов.

Вредоносная программа доставляет информацию на командный сервер (C2), используя JSON через HTTP, после сжатия и шифрования с помощью жестко запрограммированного открытого ключа RSA-1024…

Анализ показал, что CDRThief может запускаться из любого места на диске, используя любое имя файла. После развертывания он пытается запустить допустимый двоичный файл с платформы Linknat VOS2009 / 3000…

Неясно, как достигается постоянство, но исследователи говорят, что приведенная выше команда предполагает, что вредоносная программа может быть вставлена в цепочку загрузки платформы, возможно, маскируясь под компонент программного коммутатора Linknat.

Основываясь на текущих наблюдениях из анализа, CDRThief может использоваться для операций кибершпионажа или мошенничества с использованием VoIP». ***(Ionut Ilascu. New CDRThief malware steals VoIP metadata from Linux softswitches // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-cdrthief-malware-steals-voip-metadata-from-linux-softswitches/). 10.09.2020).***

***

«Официальное иммиграционное агентство Аргентины Dirección Nacional de Migraciones подверглось атаке с помощью программы-вымогателя Netwalker, которая временно остановила пересечение границы в страну и из страны.

Хотя атаки программ-вымогателей против городов и местных агентств стали обычным явлением, это может быть первая известная атака против федерального агентства, которая прервала деятельность страны.

Согласно жалобе на уголовное преступление, опубликованной аргентинским агентством по борьбе с киберпреступностью Unidad Fiscal Especializada en Ciberdelincuencia, правительство впервые узнало об атаке программы-вымогателя после получения многочисленных звонков в службу технической поддержки с контрольно-пропускных пунктов примерно в 7 утра 27 августа.

«Примерно в 7 часов утра дня, указанного в предыдущем абзаце, в Управление технологий и коммуникаций Главного управления информационных систем и технологий этой Организации поступило множество звонков с различных контрольно-пропускных пунктов с просьбой о технической поддержке».

«Они поняли, что это не обычная ситуация, поэтому было оценено состояние инфраструктуры Центрального центра обработки данных и распределенных серверов, отмечая активность вируса, который затронул системные файлы на базе MS Windows (ADAD SYSVOL и SYSTEM CENTER DPM в основном) и файлы

Microsoft Office (Word, Excel и т.д.), существующие в рабочих местах и общих папках пользователей», - говорится в переводе жалобы.

Чтобы программа-вымогатель не заразила другие устройства, компьютерные сети, используемые иммиграционными службами и контрольными пунктами, были отключены.

По сообщению аргентинского новостного сайта Infobae, это привело к временной приостановке пересечения границы на четыре часа, пока серверы были переведены в онлайн.

«Комплексная система миграционного контроля (SICaM), которая действует на международных пунктах пересечения границы, особенно пострадала, что привело к задержкам въезда и выезда на национальную территорию», - заявили в Национальном управлении миграции (DNM).

Источники в правительстве сообщили Infobae, что «они не будут вести переговоры с хакерами и не слишком озабочены получением этих данных».

Netwalker требует выкуп в размере 4 миллионов долларов

Когда Netwalker выполняет атаку программы-вымогателя, записки о выкупе остаются на зашифрованных устройствах.

Эти заметки о выкупе содержат ссылки на темный веб-сайт оплаты, который содержит информацию о том, как приобрести дешифратор, сумму выкупа и информацию о любых незашифрованных файлах, которые были украдены во время атаки.

На странице оплаты Netwalker Tor, доступной для BleepingComputer, мы узнали, что злоумышленники изначально требовали выкуп в размере 2 миллионов долларов.

По прошествии семи дней сумма выкупа увеличилась до 4 миллионов долларов, или примерно 355 биткойнов, как показано ниже на изображении страницы выкупа Dirección Nacional de Migraciones…» ***(Lawrence Abrams. Netwalker ransomware hits Argentinian government, demands $4 million // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/netwalker-ransomware-hits-argentinian-government-demands-4-million/). 06.09.2020).***

***

«Французское национальное агентство кибербезопасности сегодня опубликовало предупреждение о всплеске атак Emotet, нацеленных на частный сектор и государственные административные учреждения по всей стране.

Французское государственное управление состоит из трех подсекторов: центрального публичного управления (APUC), местного самоуправления (LUFA) и управления социального обеспечения (ASSO).

Emotet, изначально являвшийся обычным банковским троянцем, впервые обнаруженный в 2014 году, теперь представляет собой ботнет вредоносного ПО, используемый группой угроз, известной как TA542 и Mummy Spider.

Вредоносное ПО используется злоумышленниками для удаления других семейств вредоносных программ, включая Trickbot (известный вектор,

используемый для развертывания полезных нагрузок программ-вымогателей Ryuk и Conti) и троянов QakBot в зараженных системах.

Приступы резко усилились на несколько дней

«В течение нескольких дней, Анси наблюдал адресность французских компаний и администраций Emotet вредоносного» Ансите (Agence Nationale - де - ла Sécurité дез Systèmes d'Information) бюллетень оповещения читает.

«На это следует обратить особое внимание, потому что Emotet теперь используется для развертывания другого вредоносного кода, который может оказать сильное влияние на активность жертв».

Как заметил ANSSI, ботнет нацелен на «все типы бизнес-секторов по всему миру», и в последние несколько дней количество атак на французские организации резко возросло.

ANNSI также предоставляет список рекомендаций, которым организации должны следовать, чтобы предотвратить заражение Emotet и правильно реагировать после взлома их систем:

• Предупредите пользователей, чтобы они не включали макросы во вложениях и были особенно внимательны к получаемым электронным письмам, а также сократите выполнение макросов.

• Ограничьте доступ в Интернет для всех агентов контролируемым белым списком.

• Отключите скомпрометированные машины от сети без удаления данных.

• Вообще говоря, удаление / очистка антивирусом не является достаточной гарантией. Только переустановка аппарата гарантирует стирание имплантата.

• Отправьте доступные вам образцы (.doc и.eml) для анализа в ANSSI, чтобы определить IoC, которые могут быть переданы. Этот момент важен, поскольку инфраструктура злоумышленника часто развивается, поэтому необходим доступ к последним образцам.

Возродился после пяти месяцев молчания

Это предупреждение появилось после того, как вредоносный ботнет Emotet вернулся к жизни с помощью масштабной кампании вредоносного спама, замаскированного под отчеты об оплате, счетах, возможностях трудоустройства и информацию о доставке, с доставкой вредоносных документов Word и вложений электронных таблиц с 17 июля через все кластеры серверов.

Как сообщил тогда BleepingComputer исследователь Binary Defense Джеймс Куинн, Emotet последний раз видели 7 февраля 2020 года, когда вредоносное ПО не работало в течение пяти месяцев и не рассылало спам до июля.

«С момента возрождения 17 июля, Emotet продолжал свою деятельность, ежедневно рассылая более 500 тыс. Писем (кроме выходных), начиная примерно с 2:00 утра по тихоокеанскому времени (UTC -7)», - заявила в то время Microsoft.

С тех пор, как он вернулся к жизни, Emotet начал устанавливать троян TrickBot на зараженные компьютеры Windows, позже переключившись на полную замену полезных нагрузок TrickBot и широко распространяя вредоносное ПО QakBot.

На данный момент в отчетах говорится, что QakBot будет поставлять вымогатель ProLock в качестве окончательной полезной нагрузки для некоторых систем, изначально взломанных Emotet.

Теперь тоже кража вложений

Emotet теперь также использует украденные вложения для повышения подлинности своих вредоносных писем, впервые Куинн сказал BleepingComputer.

Эта новая тактика дополняет использование перехваченных цепочек писем, в которые внедряются вредоносные URL-адреса или вложения в новые электронные письма, прикрепленные к существующим разговорам (как было обнаружено Minerva Labs в марте 2019 года).

С тех пор, как он вернулся в Интернет, Emotet занял первое место в списке из 10 основных штаммов вредоносных программ, проанализированных на платформе интерактивного анализа вредоносных программ Any.Run.

Этот топ ставит его на голову выше следующего вредоносного ПО (троян для удаленного доступа Agent Tesla), у которого более чем в разы больше образцов, отправленных для анализа». ***(Sergiu Gatlan. France warns of Emotet attacking companies, administration // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/france-warns-of-emotet-attacking-companies-administration/). 07.09.2020).***

***

«Вредоносная программа появилась в рамках целевой кампании и новой процедуры заражения.

Программа-вымогатель Zeppelin снова стала актуальной после перерыва в несколько месяцев.

В августе исследователи Juniper Threatlab заметили волну атак с использованием нового троянского загрузчика. Они, как и первоначальная волна Zeppelin, наблюдавшаяся в конце 2019 года, начинаются с фишинговых писем с вложениями Microsoft Word (называемыми «счетами»), которые содержат вредоносные макросы. Как только пользователь включает макросы, начинается процесс заражения.

В последней кампании фрагменты сценариев Visual Basic скрыты среди мусорного текста за различными изображениями. Вредоносные макросы анализируют и извлекают эти сценарии и записывают их в файл по адресу c: \ wordpress \ about1.vbs.

Затем второй макрос ищет строку «winmgmts: Win32_Process» внутри текста документа и использует ее для выполнения about1.vbs с диска. About1.vbs - это вышеупомянутый загрузчик троянов, который в конечном итоге загружает вымогатель Zeppelin на компьютер жертвы.

Согласно недавно опубликованному анализу, двоичный файл находится в спящем режиме 26 секунд, «пытаясь превзойти динамический анализ в автоматизированной песочнице, а затем запускает исполняемый файл программы-вымогателя». «Как и в предыдущих версиях, исполняемый файл Zeppelin проверяет языковые настройки компьютера и геолокацию IP-адреса потенциальной жертвы,

чтобы избежать заражения компьютеров в России, Беларуси, Казахстане и Украине».

Что касается атрибуции, согласно предыдущему исследованию Виталия Кремеза, Zeppelin представляет собой простой фрагмент кода, который распространяется через аффилированный бизнес: вредоносное ПО создается с помощью мастера графического интерфейса и предлагается дистрибьюторам в обмен на долю дохода.

Исследователи Juniper отметили, что последняя кампания затронула около 64 известных жертв и целей, что указывает на определенный уровень нацеливания. Это могло начаться 4 июня, когда был зарегистрирован командно-административный (C2) сервер, который использует вредоносная программа; а данные пассивного DNS показывают, что он работал как минимум до 28 августа; Согласно данным пассивного DNS, 28 августа - последнее разрешение имен для домена C2.

«[Это] может указывать на то, что вредоносное ПО не заражало новые сети за последние несколько дней», - говорится в сообщении.

Zeppelin - это вариант семейства программ-вымогателей как услуги (RaaS) на базе Delphi, первоначально известного как Vega или VegaLocker, которое, по данным BlackBerry Cylance, появилось в начале 2019 года в рекламных объявлениях российского Яндекс.Директа. В отличие от своего предшественника, Zeppelin гораздо более нацелен, и сначала он был нацелен на целевые технологические и медицинские компании в Европе и США». ***(Tara Seals. Zeppelin Ransomware Returns with New Trojan on Board // Threatpost (https://threatpost.com/zeppelin-ransomware-returns-trojan/159092/). 09.09.2020).***

***

«Шесть вредоносных приложений были удалены из Google Play, но по-прежнему могут угрожать 200 000 установкам.

Google удалил шесть приложений из своей торговой площадки Google Play, которые заражали пользователей вредоносным ПО Joker (также известным как Bread).

Вместе эти приложения, которые рекламируют различные функции, от обмена текстовыми сообщениями до обоев с эмодзи, составляют почти 200 000 установок, сообщили исследователи из Pradeo в своем сообщении на этой неделе. По состоянию на среду, Google подтвердил Threatpost, что все зараженные приложения были удалены из Google Play, но исследователи заявили, что они все еще установлены на устройствах их пользователей, и призвали пользователей немедленно удалить приложения.

«Большинство приложений, встраивающих вредоносное ПО Joker, запрограммированы на загрузку и выполнение внешнего кода после публикации в магазине», - сообщила Threatpost Роксана Суау из Pradeo. «Во-первых, эти приложения пронизаны запросами на разрешение и отправлены в Google Play их разработчиками. Они утверждаются, публикуются и устанавливаются пользователями. После запуска на устройствах пользователей они автоматически

загружают вредоносный код. Затем они используют свои многочисленные разрешения для выполнения вредоносного кода».

Среди вредоносных программ обнаружены следующие приложения: Convenient Scanner 2 (100 000 установок), Отдельный сканер документов (50 000 установок), Safety AppLock (10 000 установок), Push-сообщения, текстовые сообщения и SMS (10 000 установок), Emoji Wallpaper (10 000 установок). установок) и Fingertip GameBox (1000 установок). Более подробную информацию об этих приложениях можно найти здесь.

Cyay сообщил Threatpost, что приложения были специально разработаны людьми, которые запрограммировали их на злонамеренные действия. Cyay сказал, что просмотр рейтингов приложений выявил несколько красных флажков, включая обзоры, в которых говорится, что приложения являются поддельными (см. Рисунок ниже).

Joker - это семейство вредоносных программ для мошенничества с выставлением счетов (которые исследователи классифицируют как «вредоносное ПО»), появившееся в 2017 году, но начало расти в 2019 году.

По словам исследователей, оно рекламирует себя как законное приложение, но после установки имитирует щелчки и перехватывает SMS-сообщения, чтобы подписать жертв на нежелательные платные услуги премиум-класса (без их ведома).

Вредоносные приложения, распространяющие Joker, продолжают обходить защиту Google Play с 2019 года, поскольку автор вредоносной программы продолжал вносить небольшие изменения в ее код.

«Используя как можно меньше кода и тщательно скрывая его, Joker создает очень незаметный след, который может быть сложно обнаружить», - сказал Cyay.

В 2020 году вредоносная программа Joker продолжила процветать в Google Play. В июле Google удалил из магазина 11 вредоносных приложений для Android, которые распространяли вредоносное ПО, а в январе исследователи обнаружили, что на тот момент Google удалил 17 000 приложений для Android, которые служили проводниками для вредоносного ПО Joker.

Хэнк Шлесс, старший менеджер по решениям безопасности в Lookout, сказал, что исследователи продолжают видеть, как Джокер появляется в приложениях для Android - и теперь, когда сотрудники удаляются из-за текущей, продолжающейся пандемии, угроза распространения Джокера через приложения для повышения производительности возрастает.

«Из-за того, как часто Joker и другие скрытые вредоносные программы появляются в большом количестве приложений, мобильные пользователи должны использовать мобильную безопасность, чтобы обезопасить себя и свою организацию», - сказал он по электронной почте. «Особенно во время глобальной удаленной работы мобильные устройства и планшеты используются как в рабочих, так и в личных целях. Если вы загружаете приложение, зараженное Joker или другим вредоносным ПО, вы предоставляете злоумышленнику доступ к своим личным данным, а также ко всем данным компании, к которым вы получаете доступ с этого устройства».

По словам Джонатана Кнудсена, старшего стратега по безопасности Synopsys, повторное появление вредоносного ПО Joker в магазине Google Play также подчеркивает фундаментальную проблему того, как пользователи могут узнать, достаточно ли защищено программное обеспечение.

«В магазине приложений непрактично понимать процессы разработки каждого приложения, поэтому магазин должен полагаться на тестирование безопасности для оценки отправленных приложений», - сказал он. «Однако для многих организаций процесс закупок предлагает неиспользованные возможности для оценки того, как поставщики создают программное обеспечение, для проведения тщательного тестирования и принятия обоснованных решений с учетом рисков». ***(Lindsey O'Donnell. Joker Spyware Plagues More Google Play Apps // Threatpost (https://threatpost.com/joker-spyware-google-play-apps-2/158895/). 02.09.2020).***

***

«Исследователи NVISO Labs обратили внимание, что группировка Epic Manchego использует для атак необычные файлы Excel, созданные специально для обхода защитных механизмов. Дело в том, что эти файлы создаются не через Microsoft Office, а с использованием.NET библиотеки EPPlus.

Как правило, данную библиотеку используют разработчики приложений, например, для добавления таких функций, как «Экспорт в Excel» или «Сохранить как электронную таблицу». Библиотека может использоваться для создания файлов в широком спектре форматов и поддерживает Excel 2019.

Эксперты пишут, что хакеры, похоже, применяют EPPlus для создания электронных таблиц в формате Office Open XML (OOXML). В файлах, созданных Epic Manchego, не хватает части VBA-кода, характерного для документов Excel, скомпилированных в проприетарном Microsoft Office.

Оказалось, что некоторые антивирусные продукты и email-сканеры рассматривают именно эту часть VBA-кода, как один из возможных признаков подозрительного файла Excel, ведь, как правило, именно там хранится вредоносный код. Поэтому специальные файлы Epic Manchego гораздо реже обнаруживаются защитными решениями (по сравнению с другими вредоносными файлами Excel).

Разумеется, это не значит, что файлы Epic Manchego абсолютно безобидны. Хотя файлы работали корректно, как и любой другой документ Excel, эксперты объясняют, что злоумышленники хранят в них малварь, используя кастомный формат кода VBA, который к тому же защищен паролем, чтобы системы безопасности и ИБ-специалисты не могли провести анализ содержимого.

Аналитики отмечают, что использование EPPlus не только помогло, но и навредило Epic Manchego. Дело в том, что эксперты смогли обнаружить многочисленные прошлые операции группировки, попросту поискав необычные файлы Excel. В итоге было обнаружено более 200 файлов, связанных с Epic Manchego, первый из которых датируется 22 июня текущего года.

Как не трудно догадаться, такие вредоносные документы содержат вредоносный макрос-скрипт. Так, если жертва откроет файл Excel и разрешит

выполнение скрипта, макросы загрузят и установят на ее машину вредоносное ПО. Пейлоадами в данном случае выступают классические трояны-инфостилеры, такие как Azorult, AgentTesla, Formbook, Matiex и njRat, которые воруют пароли из браузеров, почты и FTP-клиентов и отправляют их на серверы Epic Machengo.

Стоит отметить, что в целом эксперты NVISO Labs не были удивлены тем, что хак-группа использует EPPlus для атак. Они пишут:

«Мы давно знакомы с этой.NET библиотекой, так как уже несколько лет используем ее для создания вредоносных документов для нашей красной команды и пентестеров». ***(Мария Нефёдова. Хакеры используют.NET библиотеку для создания вредоносных файлов Excel // Xakep (https://xakep.ru/2020/09/07/epic-manchego/). 07.09.2020).***

***

«Издание Bleeping Computer сообщает, что на этой неделе компания K-Electric, поставщик электроэнергии в пакистанском городе Карачи, подверглась атаке вымогателя Netwalker, что привело к нарушению работы биллинга и ряда других онлайн-сервисов.

K-Electric является одним из крупнейших поставщиков электроэнергии в Пакистане, обслуживающим 2,5 миллиона клиентов и насчитывающим более 10 000 сотрудников.

7 сентября 2020 года клиенты компании обнаружили, что не могут получить доступ к онлайн-сервисам для своих учетных записей. Пытаясь решить эту проблему, специалисты K-Electric перенаправили пользователей на промежуточный сайт, однако в настоящее время и в его работе наблюдаются трудности.

ИБ-исследователь, известный под псевдонимом Ransom Leaks, который рассказал изданию об инциденте, сообщает, что, по данным местной пакистанской ИБ-компании, эта атака затронула внутренние службы K-Electric, но не повлияла на поставку электроэнергии.

BeepingComputer также цитирует и собственные анонимные источники в ИБ-сообществе, которые заявляют, что K-Electric стала жертвой вымогателя Netwalker. Так, журналисты приводят скриншоты платежного Tor-сайта злоумышленников, где операторы шифровальщика требуют от представителей K-Electric 3 850 000 долларов выкупа в криптовалюте. Если выкуп не будет выплачен в течение следующей недели, злоумышленники обещают увеличить сумму до 7 700 000 долларов.

Кроме того, на этом сайте хакеров также имеется ссылка на страницу Stolen data («Украденные данные»), где операторы Netwalker заявляют, что похитили у K-Electric некие файлы перед выполнением атаки. Пока неизвестно, какую именно информацию и в каком объеме могли похитить злоумышленники, но хакеры грозятся обнародовать файлы через 20 дней, если компания не заплатит.

Вымогатель NetWalker был впервые обнаружен в августе 2019 года. Изначально он получил название Mailto, но потом исследователи переименовали его в NetWalker.

Малварь работает по модели RaaS (ransomware-as-a-service, «вымогатель как услуга»): злоумышленники регистрируются на специальном портале и проходят проверку, после чего получают возможность создавать собственные версии шифровальщика.

Американские правоохранители и ИБ-эксперты отмечают, что в последние месяцы активность группировки значительно возросла. В настоящее время самой известной жертвой NetWalker является Мичиганский государственный университет, зараженный шифровальщиком в конце мая текущего года.

По информации экспертов компании McAfee, по «прибыльности» NetWalker вполне может сравниться с Ryuk или REvil, так как с марта 2020 года шифровальщик принес своим операторам около 25 000 000 долларов США». ***(Мария Нефёдова. Шифровальщик Netwalker атаковал одного из крупнейших поставщиков электроэнергии в Пакистане // Хакер (https://xakep.ru/2020/09/10/k-electric-netwalker/). 10.09.2020).***

***

«Исследователи безопасности Zscaler обнаружили новую шпионскую кампанию против пользователей Android, в рамках которой злоумышленники распространяют «Pro-версию» TikTok на волне опасений по поводу возможной блокировки приложения в США. Вредоносное ПО способно захватывать контроль над базовыми функциями устройства – делать фотографии, читать и отправлять SMS-сообщения, осуществлять телефонные звонки и запускать приложения. Кроме того, с помощью фишинга вредонос может похищать учетные данные пользователей Facebook.

Вредоносное приложение TikTok Pro распространяется киберпреступниками через SMS-сообщения и сообщения в WhatsApp, в которых пользователям предлагается скачать «последнюю версию TikTok» с определенного web-адреса. В первую волну распространения вредонос запрашивал только учетные данные и разрешение на использование функций Android-устройства, в том числе камеры и микрофона. В результате пользователи подвергались «бомбардировке» рекламой.

Во вторую волну киберпреступники стали распространять новую версию приложения, в котором скрыто уже «полнофункциональное шпионское ПО с премиум-функциями, позволяющее с легкостью следить за пользователями».

После установки и открытия TikTok Pro на устройстве отображается поддельное уведомление, которое затем исчезает вместе с иконкой приложения. Уведомление играет роль отвлекающего маневра, пока вредонос прячется на устройстве, и заставляет пользователя думать, будто приложение просто неисправно.

Помимо захвата контроля над функциями смартфона, такими как съемка фотографий, отправка SMS-сообщений, выполнение команд, создание снимков экрана, осуществления телефонных звонков и запуск других приложений на устройстве, шпионское ПО также способно похищать учетные данные для авторизации в Facebook – уникальная функция, нехарактерная для этих шпионских приложений». ***(На волне опасений блокировки TikTok распространяется***

шпионское ПО TikTok Pro // SecurityLab.ru (https://www.securitylab.ru/news/511972.php). 10.09.2020).

***

«Команія з кібербезпеки Check Point заявила, що виявила іранську хакерську групу, яка розробила спеціальне шкідливе ПЗ для Android. Воно дозволяє їм обходити двофакторну автентифікацію – перехоплювати і викрадати коди (2FA), що відправляються через SMS. Шкідлива програма входила в арсенал інструментів, розроблених хакерською групою Rampant Kitten.

Check Point заявляє, що група діє не менше шести років і бере участь в постійній операції зі спостереження за іранськими меншинами, антиурядовими організаціями і рухами опору. У цих кампаніях використовувався широкий спектр сімейств шкідливих програм, включаючи чотири варіанти інфостилерівв для Windows і бекдор Android, замаскований всередині шкідливих додатків. Штами шкідливих програм для Windows, в основному, використовувалися для крадіжки особистих документів жертви і отримання доступу до облікового запису Telegram, а також файлів з месенджера. Хакери також викрадали файли з диспетчера паролів KeePass.

Як використовували двофакторну автентифікацію для Android

Хоча хакери Rampant Kitten надавали перевагу троянам для Windows, вони також розробили аналогічні інструменти для Android. В опублікованому звіті, дослідники Check Point заявили, що вони також виявили серйозний бекдор для Android, розроблений цією групою. Це дозволяло їм викрасти список контактів жертви і SMS-повідомлення, непомітно записати жертву через мікрофон і показувати фішингові сторінки. Але також бекдор містив процедури, спеціально призначені для крадіжки кодів 2FA.

Check Point заявила, що розроблена шкідлива програма перехоплюватиме і пересилатиме зловмисникам будь-яке SMS-повідомлення, що містить літеру «G-». Вона використовується для префікса кодів 2FA, що відправляються користувачам через SMS, при спробі ввійти у свій обліковий запис Google.

Передбачається, що хакери Rampant Kitten використовуватимуть троян для Android, щоб відображати фішингову сторінку Google і захопити облікові дані користувача. В подальшому – отримати доступ до облікового запису жертви.

Check Point також виявила докази того, що шкідлива програма автоматично пересилає всі вхідні SMS-повідомлення з Telegram й інших додатків соціальних мереж. Ці типи повідомлень також містять коди 2FA, і дуже ймовірно, що група використовувала цю функцію для обходу 2FA не лише для профілів Google.

Наразі, це шкідливе ПЗ виявили всередині програми для Android, що маскується під послугу, яка допомагає носіям перської мови в Швеції отримати водійські права. Однак, воно може ховатися всередині й інших додатків». ***(Грицина Вікторія. Новий вірус дозволяє хакерам обходити двофакторну автентифікацію на Android // Pingvin Pro (https://pingvin.pro/gadgets/news-gadgets/novyj-virus-dozvolyaye-hakeram-obhodyty-dvofaktornu-avtentyfikacziyu-na-android.html). 19.09.2020).***

***

«Американское правительственное агенство инфраструктурной и кибернетической безопасности (CISA) оповестило федеральные учреждения и частный сектор о значительном росте использования за последние три месяца ПО LokiBot — одного из самых опасных и широкораспространённых штаммов вредоносного ПО, который относят к категории троянов, похищающих информацию.

Пик активности LokiBot, зарегистрированный разработанной в CISA платформой обнаружения вторжений, EINSTEIN, был независимо подтверждён группой аналитики угроз Malwarebytes.

Также известный под названиями Loki или Loki PWS, LokiBot ищет на заражённом компьютере локальные приложения и извлекает идентификационные данные из их внутренних баз данных. По умолчанию, LokiBot нацелен на браузеры, почтовые клиенты, приложения FTP и криптокошельки.

LokiBot дебютировал на форумах теневого Интернета в середине 2010-х и с тех пор постоянно совершенствуется. Авторы дополнили его компонентом для записи в реальном времени нажатий на кнопки, что позволяет похищать пароли от учётных записей, отсутствующие во внутренней БД браузера. Новая утилита снимков экрана служит для кражи тех документов, что открываются на заражённом компьютере.

Кроме того, LokiBot предоставляет хакерам «чёрный ход» для запуска произвольного кода на взломанном хосте и для потенциальной эскалации атак.

Распространением его сегодня занимаются многие группы, использующие различные техники: от почтового спама до взломанных установщиков и торрент-файлов с вредоносной начинкой.

В прошлогоднем рейтинге от SpamHaus LokiBot занимал первое место среди вредоносных программ с самыми активными центрами управления (C&C), в этом году он спустился на второе место.

Опубликованное вчера предупреждение CISA включает рекомендации по обнаружению и смягчению последствий для борьбы с атаками и заражениями LokiBot. Дополнительные сведения о LokiBot можно найти на посвящённой этому штамму странице ресурса Malpedia». ***(Активность опасного трояна резко возросла с июля этого года // Компьютерное Обозрение (https://ko.com.ua/aktivnost_opasnogo_troyana_rezko_vozrosla_s_iyulya_jetogo_goda_134612). 23.09.2020).***

***

«В августе анализ данных статистики Dr.Web показал значительное снижение общего числа обнаруженных угроз на 67.16% по сравнению с июлем. Количество уникальных угроз сократилось на 9.85%. Большинство угроз по-прежнему приходится на долю рекламных программ, а также загрузчиков и установщиков вредоносов. В почтовом трафике продолжает доминировать ПО, использующее уязвимости документов Microsoft Office. Кроме того, пользователям угрожают различные модификации вредоносных HTML-документов,

распространяемых в виде вложений и перенаправляющих пользователей на фишинговые сайты.

По сравнению с июлем в прошедшем месяце количество обращений пользователей за расшифровкой файлов снизилось на 2.5%. Самым распространенным шифровальщиком остается Trojan.Encoder.26996, на долю которого по-прежнему приходится более четверти всех инцидентов.

Основные угрозы августа 2020 г., по данным сервиса статистики «Доктор Веб»:

Trojan.LoadMoney.4020 – семейство программ-установщиков, вместе с требуемыми приложениями инсталлирующих на компьютеры жертв всевозможные дополнительные компоненты. Некоторые модификации трояна могут собирать и передавать злоумышленникам различную информацию об атакованном компьютере;

Adware.Downware.19741 – рекламное ПО, часто выступающее в роли промежуточного установщика пиратских программ;

Adware.Softobase.15 – программа-установщик, распространяющая устаревшее ПО. Меняет настройки браузера;

Adware.Elemental.17 – семейство рекламных программ, попадающих на устройства путем подмены ссылок на файлообменных сервисах. Вместо ожидаемых файлов жертвы получают эти приложения, которые показывают рекламу, а также инсталлируют ненужное ПО;

Adware.Ubar.18 – торрент-клиент, устанавливающий нежелательное ПО на устройство.

Рейтинг вредоносных программ в почтовом трафике:

W97M.DownLoader.2938 – семейство троянов-загрузчиков, использующих в работе уязвимости документов Microsoft Office. Предназначены для загрузки на атакуемый компьютер других вредоносных программ;

Exploit.CVE-2012-0158 – измененный документ Microsoft Office Word, для выполнения вредоносного кода использующий уязвимость CVE-2012-0158;

HTML.Redirector.35, HTML.Redirector.32 – вредоносные HTML-документы, как правило, маскирующиеся под безобидные вложения к электронным письмам. При открытии перенаправляют пользователей на фишинговые сайты или загружают полезную нагрузку на заражаемые устройства;

Tool.KMS.7 – хакерские утилиты, которые используются для активации продуктов Microsoft с поддельной лицензией.

По сравнению с июлем в августе в антивирусную лабораторию «Доктор Веб» поступило на 2.5% меньше запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков. При этом чаще всего встречались: Trojan.Encoder.26996 – 26.33%; Trojan.Encoder.567 – 7.40%; Trojan.Encoder.29750 – 5.03%; Trojan.Encoder.30356 – 2.96%; Trojan.Encoder.11464 – 2.07%.

В базу нерекомендуемых и вредоносных сайтов в августе был добавлен 174501 интернет-адрес – на 12.08% меньше, чем в июле.

В августе вирусные аналитики обнаружили в каталоге Google Play очередные угрозы. Среди них были многочисленные троянские приложения семейства

Android.FakeApp, которые распространялись под видом справочников с информацией о способах получения возврата НДС и социальных выплат. На самом деле они загружали мошеннические веб-сайты, с помощью которых злоумышленники похищали у жертв персональные данные и деньги. Кроме того, был найден новый представитель опасного семейства троянов Android.Joker. Он загружал и выполнял произвольный код, а также подписывал владельцев Android-устройств на дорогостоящие услуги». ***(Общее число обнаруженных угроз в августе снизилось на 67% // Компьютерное Обозрение (https://ko.com.ua/obshhee_chislo_obnaruzhennyh_ugroz_v_avguste_snizilos_na_67_134562). 18.09.2020).***

***

«Компания Eset обнаружила всплеск вредоносной активности, нацеленной на пользователей пиратского контента. Преступники распространяют вредоносы через торрент-файлы с фильмом «Мулан» студии Disney, который стал самым скачиваемым по данным TorrentFreak. Рост числа выявленных угроз совпадает с датой выхода фильма.

Только среди результатов обычного поискового запроса «Mulan.2020» встречаются около 18 тыс. файлов фильма с признаками вредоносного поведения. Скорее всего, в реальности их намного больше под другими названиями.

Среди обнаруженных угроз встречается вредоносный houdrat-код, который используется в основном для криптомайнинга. Криптомайнинг может долго оставаться незаметным и способен вывести из строя устройство.

Кроме того, распространены LNK-файлы – расширения, позволяющие перенаправить пользователя на другие ресурсы: рекламные сайты или ссылки, по которым запускается другой вредоносный код.

Пользователи во всех странах мира регулярно становятся жертвами преступных кампаний из-за пиратского контента, ведь это один из наиболее простых и эффективных способов распространения вредоносов. К примеру, в своем исследовании год назад Eset выяснила, что лишь 9% пользователей выбирают легальный контент. При этом даже на торрент-сайтах есть предупреждение об угрозе распространения вредоносов через файлы игр, фильмов и сериалов». ***(Вредоносы маскируются на пиратских сайтах под популярную новинку Disney // Компьютерное Обозрение (https://ko.com.ua/vredonosy_maskiruyutsya_na_piratskih_sajtah_pod_populyarnuyu_novinku_disney_134557). 18.09.2020).***

***

«Команда исследователей Check Point Research опубликовала отчет Global Threat Index с самыми активными угрозами в августе 2020 года. Исследователи сообщают, что троян Qbot (также известный как Qakbot и Pinkslipbot) впервые вошел в первую десятку самых распространенных вредоносных программ в августе — он занял 10-е место. На первом месте по-прежнему остается троян Emotet, он затрагивает 14% организаций во всем мире.

Впервые троян Qbot появился в 2008 году, и с тех пор он постоянно дорабатывался и улучшался. Сейчас он использует продвинутые методы для кражи учетных данных и установки программ-вымогателей, что, по мнению исследователей, делает его вредоносным компьютерным эквивалентом швейцарского армейского ножа. Сейчас у Qbot появился новый модуль сбора сообщений электронной почты: он извлекает трафик из Outlook жертвы и загружает его на внешний удаленный сервер.

Так Qbot может перехватывать электронные сообщения своих жертв, а затем рассылать спам, используя эти письма. Это увеличивает шансы на то, что другие пользователи тоже заразятся. Также Qbot может в любое время подключаться к устройству жертвы и осуществлять банковские транзакции без ее ведома.

Исследователи Check Point обнаружили несколько кампаний с обновленной версией Qbot в период с марта по август 2020 года, в том числе кампанию, где Qbot распространялся с помощью трояна Emotet. В июле 2020 года эта кампания затронула 5% организаций во всем мире.

«Злоумышленники всегда ищут способы усовершенствовать вредоносное ПО. Сейчас они явно вкладывают значительные средства в разработку Qbot — его можно будет использовать для массовых краж данных организаций и рядовых пользователей, — рассказывает Василий Дягилев, глава представительства Check Point Software Technologies в России и СНГ. — Мы уже видели активные кампании вредоносного спама, которые распространяли Qbot. Мы также отмечали, что иногда Qbot распространяется с помощью другого трояна, Emotet. Компаниям необходимо задуматься о введении защитных решений, которые предотвратят попадание такого контента к пользователям. Важно напоминать сотрудникам, что нужно быть очень аккуратными при открытии писем, даже если на первый взгляд кажется, что они пришли из надежного источника».

В этом месяце Emotet остается самым распространенным вредоносным ПО в мире –- он затронул 14% организаций. За ним следуют Agent Tesla и Formbook, каждый из которых затрагивает по 3% компаний.

1. 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.

2. 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, MozillaFirefox и Microsoft Outlook).

3. FormBook был впервые обнаружен в 2016 году: это инфостилер, предназначенный для ОС Windows. На подпольных хакерских форумах он позиционируется как MaaS из-за его развитых методов уклонения и относительно низкой цены. FormBook собирает учетные данные из различных веб-браузеров, делает снимки экрана, отслеживает и регистрирует нажатия клавиш, а также может

загружать и выполнять файлы в соответствии с приказами своего командного сервера.

Самые распространенные уязвимости в августе 2020:

В этом месяце самой популярной уязвимостью стала «Раскрытие информации в хранилище Git на веб-сервере» — она затронула 47% организаций во всем мире. На втором и третьем месте — «Удаленное выполнение кода MVPower DVR» (затронуло 43% организаций по всему миру) и «Обход аутентификации роутера Dasan GPO» — 37%.

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

2. 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.

3. Обход аутентификации роутера Dasan GPON (CVE-2018-10561) - уязвимость обхода аутентификации, существующая в роутерах Dasan GPON. Успешное использование этой уязвимости позволит удаленным злоумышленникам получить конфиденциальную информацию и получить несанкционированный доступ к уязвимой системе.

Самые активные мобильные угрозы в августе 2020

1. 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.

2. Necro — троян-дроппер для Android, который загружает вредоносное ПО, запускает навязчивую рекламу и оформляет платные подписки, взымая деньги с пользователей.

3. 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». ***(Обновленный троян Qbot впервые вошел в топ вредоносных программ // Компьютерное Обозрение (https://ko.com.ua/obnovlennyj_troyan_qbot_vpervye_voshel_v_top_vredonosnyh_programm_134503). 15.09.2020).***

***

«Эксперты IBM обнаружили ботнет Mozi, основанный на коде Mirai и Gafgyt. Исследователи утверждают, что в период с октября 2019 года по июнь 2020 года именно этот ботнет генерировал 90% всего IoT-трафика. При этом количество IoT-атак, зафиксированных за этот период времени, было на 400% выше, чем общее количество IoT-атак за последние два года.

Исследователи отмечают, что значительный рост IoT-атак также может быть связан с большим количеством устройств интернета вещей, которых уже

насчитывается примерно 31 миллиард по всему миру. К тому же Mozi не пытался убрать с этого «рынка» другие конкурирующие ботнеты, он попросту был настолько активен, что затмил их.

Аналитики компании наблюдают за Mozi уже четыре года и описывают его как P2P-ботнет, основанный на протоколе Distributed Hash Table (DHT), распространяющийся посредством эксплоитов и слабых паролей (через Telnet). Успех Mozi специалисты объясняются тем, что он эксплуатирует инъекции команд и неправильные конфигурации IoT девайсов. Так, почти все изученные атаки начинались именно с инъекций команд и wget, а затем малварь изменяла права, чтобы облегчить взаимодействие хакеров с пораженной системой.

Атаки злоумышленников в основном были нацелены на архитектуру MIPS: на уязвимые устройства загружался и затем запускался файл mozi.a.

Для заражения устройств Mozi эксплуатирует множество разных уязвимостей: CVE-2017-17215 (Huawei HG532), CVE-2018-10561 и CVE-2018-10562 (маршрутизаторы GPON), CVE-2014-8361 (Realtek SDK), CVE-2008-4873 (Sepal SPBOARD), CVE-2016-6277 (Netgear R7000/R6400), CVE-2015-2051 (устройства D-Link), инъекции команд в беспроводные маршрутизаторы Eir D1000, RCE без аутентификации в setup.cgi Netgear, выполнение команд в MVPower DVR, выполнение команд в DLink UPnP SOAP, а также RCE-баг, затрагивающий ряд поставщиков CCTV-DVR. Также, как было сказано выше, для взлома используется перебор учетных данных через Telnet по заранее подготовленному списку.

В итоге Mozi может использовать зараженные устройства для запуска DDoS-атак (HTTP, TCP, UDP), атак на выполнение команд, может загружать и выполнять дополнительные пейлоады, а также может собирать информацию о своих ботах.

Исследователи пишут, что им все чаще приходится сталкиваться с атаками злоумышленников на корпоративные IoT-устройства и напоминают о необходимости изменения настроек устройств по умолчанию». ***(Мария Нефёдова. IBM: ботнет Mozi генерировал 90% всего IoT-трафика // Xakep (https://xakep.ru/2020/09/21/mozi-2/). 21.09.2020).***

***

«По данным центра Европола по борьбе с киберпреступностью (EC3), в настоящее время вымогательское ПО является одной из главных киберугроз в мире. Операторы программ-вымогателей постоянно находят новые векторы для своих атак и сейчас ведут себя намного агрессивнее, чем раньше. Например, злоумышленники не просто шифруют файлы своих жертв, но также похищают и публикуют их конфиденциальную информацию. В связи с этим Европол запустил новый проект под названием No More Ransom, призванный помочь жертвам вымогательского ПО восстановить свои данные без уплаты выкупа.

В рамках проекта был запущен сайт, позволяющий не только определить, какую программу-вымогатель использовали злоумышленники, но и предоставляющий свыше сотни бесплатных утилит-декрипторов, полученных Европолом от более чем 150 партнеров из правоохранительных органов, научных организаций и ИБ-компаний по всему миру. Арсенал утилит постоянно

пополняется по мере появления новых семейств вымогателей и декрипторов для них.

Для того чтобы получить декриптор, жертва вымогательского ПО сначала должна заполнить специальную форму на сайте, которая позволит определить, какой программой пользовались киберпреступники. Если декриптор для данного ПО доступен на сайте, пользователю сразу же будет предоставлена ссылка для его загрузки.

«Общая рекомендация – не платить выкуп. Отправляя деньги киберпреступникам, вы подтверждаете, что троянцы-вымогатели делают свое дело, и нет гарантии, что в ответ вы получите необходимый вам ключ для расшифровки данных», – советует Европол». ***(Европол предоставил более ста бесплатных утилит для расшифровки файлов // SecurityLab.ru (https://www.securitylab.ru/news/512318.php). 22.09.2020).***

***

«Компания по цифровой безопасности провела исследование и обнаружила семь мошеннических приложений в Google Play и Apple App Store, которые принесли своим разработчикам более полумиллиона долларов.

Avast обнаружил вредоносные программы после того, как 12-летняя девочка увидела подозрительное приложение, продвигаемое в профиле TikTok в рамках своего проекта Be Safe Online в Чешской Республике, где базируется компания.

Рекламные приложения были загружены более 2,4 миллиона раз, а их разработчики заработали более 500 000 долларов США, сообщает Avast в своем блоге.

По словам Avast, многие приложения продвигаются в TikTok как минимум в трех профилях, у одного из которых более 300 000 подписчиков. Также было обнаружено, что аналогичный профиль в Instagram с более чем 5000 подписчиков продвигает одно из мошеннических приложений.

Avast объяснил, что программы представляют собой развлекательные приложения, которые либо активно отображают рекламу, либо берут от 2 до 10 долларов за покупку программного обеспечения.

Он добавил, что некоторые из приложений являются троянами HiddenAds, которые маскируются под безопасные приложения, но показывают рекламу вне приложения.

«Обнаруженные нами приложения являются мошенническими и нарушают политику приложений Google и Apple, либо делая вводящие в заблуждение заявления о функциях приложения, либо размещая рекламу за пределами приложения и скрывая оригинальный значок приложения вскоре после его установки», - заявил Якуб Вавра, аналитик по угрозам в Avast.

«Особое беспокойство вызывает то, что приложения продвигаются на платформах социальных сетей, популярных среди детей младшего возраста, которые могут не распознавать некоторые опасности, окружающие приложения, и поэтому могут активно использовать их», - добавил он.

Трудно обнаружить

Трояны HiddenAds могут быть особенно опасны, поскольку они будут продолжать показывать рекламу даже после удаления приложения, в котором они были установлены.

«Благодаря тому, что рекламное ПО устанавливается отдельно через исходное приложение, оно классифицируется как троян, а не просто как рекламное ПО», - пояснил Джонатан Таннер, старший исследователь безопасности в Barracuda Networks.

«Оригинальное приложение обманом заставляет пользователя заразить свое устройство реальным рекламным ПО, а не просто действовать как реклама», - сказал он TechNewsWorld.

Поскольку приложение загружает рекламное ПО и не обслуживает саму рекламу, ненандежное приложение должно быть легче обнаружить, но оно снижает свой профиль, ограничивая себя только функциями, используемыми законными программами, и ничего более.

«Обычно это хороший способ обнаружения вредоносных программ», - сказал Таннер. «Вредоносное ПО часто требует большего контроля над смартфоном, чем доступно разработчикам, часто требует рутирования телефона, что легче обнаружить».

Рекламное ПО, как правило, бывает трудно обнаружить, потому что реклама является обычным явлением внутри приложений. «Рекламное ПО заходит слишком далеко в этой пркатике, либо слишком агрессивно, истощая вычислительные ресурсы и пропускную способность, либо используя менее уважаемые рекламные сети, которые могут распространять вредоносное ПО», - пояснил Таннер.

«Обнаружение инвазивной рекламы по сравнению с простым баннером потребует детального изучения приложения или обратного проектирования его кода, что может быть сложно и требует много времени для выполнения в масштабе», - сказал он.

«Обнаружение вредоносных рекламных сетей требует отслеживания того, какие рекламные из них являются законными, а какие нет, что, опять же, является нетривиальной задачей», - продолжил он. «Как и в случае с самими приложениями, рекламные сети могут внезапно перейти от безопасных к вредоносным, если не тот рекламодатель зарегистрируется и имеет слишком много свободы в отношении разрешенного контента».

Влияние известных личностей

Магазину приложений может быть сложно отмечать программы, которые взимают деньги, но предлагают небольшую или тривиальную функциональность, если они соответствуют своим требованиям, какими бы ничтожными они ни были.

«Например, всплеск количества приложений-фонариков в первые дни существования App Store был в основном законным, хотя и сомнительным соотношением цены и качества», - сказал Крис Клементс, вице-президент по архитектуре решений Cerberus Sentinel, компании, занимающейся консалтингом в области кибербезопасности и тестирования на проникновение.

«С тех пор магазины Apple и Google пытались расправиться с приложениями, которые выполняют незначительные функции, - сказал он в интервью, - однако

определение того, что представляет собой незначительность функций, может быть непонятным для обозревателей».

Неопытные пользователи также могут облегчить работу с теневыми приложениями. «Мобильные устройства – это «черный ящик» для большинства пользователей, и они плохо разбираются в том, что происходит на более глубоком уровне устройства», - сказал Сарью Найяр, генеральный директор Gurucul, компании по анализу угроз из Эль-Сегундо, Калифорния.

«Существует ряд приемов, которые разработчики мобильных приложений могут использовать, чтобы скрыть функционал от случайного пользователя», - добавил эксперт.

Пользователи таких сетей, как TikTok, также могут быть слишком подвержены влиянию известных личностей в социальных сетях. «Многие влиятельные лица в социальных сетях будут брать деньги за продвижение продуктов или приложений, не исследуя их законность», - утверждает Клементс.

«Экосистема влиятельных лиц является сверхконкурентной, и рекламные акции даже от тех, у кого большая аудитория, можно купить почти бесплатно», - добавил он.

Использование социальных ситуаций

«Использование профилей TikTok для продвижения мошеннических приложений - это лишь одна из причин злоупотребления популярными каналами для получения прибыли от ничего не подозревающих фанатов», - отметил Бен Пик, старший консультант по безопасности приложений в nVisium, провайдере безопасности приложений из Фолс-Черч, штат Вирджиния.

«Лучший способ избежать уязвимости - это проверить загружаемое приложение и не переходить по ссылке прямо из профиля пользователя», - рекомендует эксперт.

«Проверяйте наличие чрезмерных разрешений и многочисленных отрицательных отзывов, чтобы предотвратить загрузку подобных мошеннических приложений или явно вредоносных программ», - добавил он.

Еще одним фактором, влияющим на загрузку этих вредоносных рекламных приложений, мог быть неизбежный запрет TikTok администрацией Трампа, который провалился, когда социальному приложению удалось заключить сделку с Oracle и Walmart, которая удовлетворила Вашингтон.

«Мы часто видим, как злоумышленники используют социальные ситуации в своих интересах», - отмечает Хэнк Шлесс, старший менеджер по решениям безопасности Lookout, поставщика мобильных фишинговых решений из Сан-Франциско.

«В этом случае, - сказал он в интервью, - они знают, что люди поспешили загрузить TikTok перед запретом, и эти новые пользователи ищут влиятельных лиц, за которыми они будут следовать, когда подписываются на приложение».

Обратите внимание на отзывы

Один из простейших способов не стать жертвой мошенничества с рекламным ПО - прочитать отзывы о приложении. «При загрузке приложения, очень важно прочитать отзывы о нем и проверить рейтинги», - говорит Джеймс МакКвиган, эксперт по вопросам безопасности KnowBe4.

«Обратите особое внимание на негативные отзывы», - добавил Клементс из Cerberus Sentinel. «Мошенники часто используют ботов или платят за ложные положительные отзывы», - пояснил он.

МакКвиган также сообщил, что при появлении запросов на установку приложения из рекламы в профиле или на веб-сайте очень важно проявить должную осмотрительность в отношении приложения, чтобы убедиться, что оно не является вредоносным». ***(Романов Роман. В популярных онлайн-магазинах приложений обнаружено мошенническое ПО, привлекшее более 500 тыс. долларов // Internetua (https://internetua.com/v-populiarnyh-online-magazinah-prilojeniy-obnarujeno-moshennicseskoe-PO-privlekshee-bolee-500-tys-dollarov). 24.09.2020).***

***

«Новая группа программ-вымогателей нацелена на крупные корпоративные сети, используя самодельные бэкдоры и вредоносное ПО для шифрования файлов на начальной и конечной стадиях атаки.

Исследователи отслеживают банду по кодовому имени OldGremlin. Их кампании, похоже, начались в конце марта и пока не получили глобального распространения.

Атаки, приписываемые этой группе, были выявлены только в России, но есть сильные подозрения, что OldGremlin в настоящее время работает в меньшем масштабе, чтобы отточить свои инструменты и методы, прежде чем выйти на мировой уровень.

Индивидуальные инструменты, творческий фишинг

OldGremlin использует собственные бэкдоры (TinyPosh и TinyNode) и программы-вымогатели (TinyCrypt, также известные как decr1pt) вместе со сторонним программным обеспечением для разведки и бокового движения (Cobalt Strike, скриншот командной строки, Mail PassView от NirSoft для восстановления пароля электронной почты).

Банда не требовательна к жертвам, поскольку они являются крупными предприятиями в России (медицинские лаборатории, банки, производители, разработчики программного обеспечения), что указывает на то, что она состоит из русскоязычных членов.

Злоумышленник начинает свои атаки с целевых фишинговых писем, которые предоставляют настраиваемые инструменты для первоначального доступа. Они используют действительные имена для адреса отправителя, выдавая себя за известных людей.

Исследователи из сингапурской компании по кибербезопасности Group-IB говорят, что во время одной из атак на банк OldGremlin разослал электронное письмо под предлогом организации интервью с журналистом популярной деловой газеты.

Фальшивый журналист назначил встречу с помощью приложения-календаря, а затем связался с жертвой, предоставив ссылку на предполагаемые вопросы интервью, размещенные в онлайн-хранилище. По ссылке скачивается бэкдор TinyPosh.

В другой атаке, направленной на клиническую лабораторию, актер выдал себя за «РосБизнесКонсалтинг» (РБК), крупный медиахолдинг в России, у которого возникли проблемы с оплатой медицинских услуг.

Похоже, они хорошо разбираются в социальной инженерии и используют текущие события, чтобы повысить надежность своего фишинга.

Например, 19 августа они представились генеральным директором Минского тракторного завода, проинформировав российских партнеров о том, что компания находится под следствием на предмет участия в антиправительственных акциях протеста в Беларуси, и попросили у них документы, требуемые прокуратурой.

Стоит отметить, что имя, используемое в адресе отправителя, не принадлежит фактическому генеральному директору завода. В рамках этой кампании было отправлено не менее 50 сообщений.

Цель состоит в том, чтобы закрепиться в сети целевой организации с помощью одного из двух бэкдоров (TinyNode или TinyPosh), которые позволяют расширить атаку с помощью дополнительных модулей, загружаемых с их сервера управления и контроля (C2). Протокол удаленного рабочего стола также используется для перехода к другим системам в сети.

Проведя некоторое время в сети, идентифицируя ценные системы, злоумышленник развертывает процедуру шифрования файлов. В случае с медицинской лабораторией злоумышленник получил учетные данные администратора домена и создал резервную учетную запись с такими же повышенными привилегиями для сохранения устойчивости в случае блокировки первоначальной.

OldGremlin перешла на этап шифрования через несколько недель после первоначального доступа, удалив резервные копии серверов и заблокировав сотни компьютеров в корпоративной сети.

В записке с требованием выкупа было запрошено около 50 000 долларов в криптовалюте за ключ дешифрования и предоставлен адрес электронной почты Proton для связи.

В общей сложности Group-IB обнаружила несколько атак, приписываемых OldGremlin, в период с мая по август 2020 года, все против целей в России, сообщил Group-IB BleepingComputer.

Эта тактика отличает группу от других участников угроз и ранее была замечена с финансово мотивированными группами Silence и Cobalt, которые также проводили небольшие операции в России и перед тем, как перейти к целям за пределами страны и за пределами бывшего советского пространства.

Как правило, российские хакеры избегают атак на организации в России и странах бывшего Советского Союза. Несколько крупных групп программ-вымогателей и злоумышленников категорически против этого…

Скулкин говорит, что OldGremlin является единственным русскоязычным агентом-вымогателем, который игнорирует это правило, и что их тактика и методы аналогичны тем, что используются продвинутыми хакерскими группами.

В своем сегодняшнем сообщении в блоге Group-IB предоставляет список индикаторов взлома OldGremlin, а также подробную информацию о тактике, методах и процедурах, наблюдаемых ниже в атаках, приписываемых этой новой

группе». ***(Ionut Ilascu. New ransomware actor OldGremlin uses custom malware to hit top orgs // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-ransomware-actor-oldgremlin-uses-custom-malware-to-hit-top-orgs/). 23.09.2020).***

***

«Операторы программы-вымогателя Maze применили тактику, ранее использовавшуюся бандой Ragnar Locker; для шифрования компьютера из виртуальной машины.

В мае мы ранее сообщали, что Ragnar Locker шифрует файлы через виртуальные машины VirtualBox Windows XP для обхода программного обеспечения безопасности на хосте.

Виртуальная машина монтирует диски хоста как удаленные общие ресурсы, а затем запускает вымогатель на виртуальной машине для шифрования файлов общего ресурса.

Поскольку на виртуальной машине не запущено какое-либо программное обеспечение безопасности и монтируются диски хоста, программа безопасности хоста не может обнаружить вредоносное ПО и заблокировать его.

Maze теперь использует виртуальные машины для шифрования компьютеров

Выполняя реагирование на инциденты для одного из своих клиентов, Sophos обнаружил, что Maze дважды пытался развернуть их программу-вымогатель, но был заблокирован функцией Intercept X компании Sophos.

В первых двух попытках злоумышленник Maze пытался запустить различные исполняемые файлы программ-вымогателей, используя запланированные задачи под названием «Безопасность Центра обновления Windows», «Патчи безопасности Центра обновления Windows» или «Обновление безопасности Google Chrome».

После двух неудавшихся атак Питер Маккензи из Sophos сообщил BleepingComputer, что злоумышленники использовали тактику, ранее использовавшуюся программой-вымогателем Ragnar Locker.

В своей третьей атаке Maze развернул файл MSI, который установил программное обеспечение VirtualBox VM на сервере вместе с настроенной виртуальной машиной Windows 7.

Как только виртуальная машина была запущена, как и в предыдущих атаках Ragnar Locker, запускался командный файл с именем startup_vrun.bat, который подготавливает машину с исполняемыми файлами Maze.

Затем компьютер выключается, и после перезапуска запускается vrun.exe для шифрования файлов хоста.

Поскольку виртуальная машина выполняет шифрование на подключенных дисках хоста, программное обеспечение безопасности не может обнаружить поведение и остановить его.

Исследователи SophosLabs отмечают, что это дорогостоящий метод атаки с точки зрения размера диска по сравнению с предыдущими атаками Ragnar Locker.

Поскольку для атаки виртуальной машины Ragnar Locker использовалась Windows XP, общий размер был всего 404 МБ. Поскольку Maze использовал Windows 7, занимаемая площадь была намного больше и составляла 2,6 ГБ.

Эта атака демонстрирует, как программы-вымогатели отслеживают тактику своих конкурентов и при необходимости применяют их.

Также следует отметить, что Рагнар Локер является частью «Картеля Лабиринта», поэтому возможно, что Рагнар предложил помощь Лабиринту в этом методе атаки». ***(Lawrence Abrams. Maze ransomware now encrypts via virtual machines to evade detection // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/maze-ransomware-now-encrypts-via-virtual-machines-to-evade-detection/). 17.09.2020).***

***

«По данным «Лаборатории Касперского», всё больше групп совершают целевые атаки на устройства на базе Linux с помощью специально разработанных инструментов.

За последние восемь лет такие операции проводили более десяти развитых кибергрупп, в том числе Barium, Sofacy, Lamberts, Equation, TwoSail Junk с зловредами LightSpy и WellMess. Вредоносные инструменты, нацеленные на Linux-системы, позволяют злоумышленникам делать атаки более эффективными и заражать большее количество устройств, а также скрываться в случае обнаружения атаки на дополнительных точках, таких как стационарные компьютеры разработчиков, серверы и корпоративный интернет вещей.

Компании по всему миру, а также государственные учреждения, всё чаще используют Linux: это связано с распространением технологий виртуализации и контейнеризации. Кроме того, в некоторых организациях Linux — доминирующая десктопная среда, когда речь идёт о работе с конфиденциальными данными. К сожалению, ложное чувство защищённости создаёт распространённый миф о том, что эта операционная система не подвержена киберугрозам. Конечно, целевые атаки на Linux-системы пока ещё случаются не слишком часто, но каждая крупная группа уже создаёт для них специальное вредоносное ПО, такое как веб-оболочки, бэкдоры, руткиты и даже кастомизированные эксплойты. Эти атаки, несмотря на свою малочисленность или, наоборот, благодаря ей, оказываются весьма успешными и трудными для обнаружения. В результате злоумышленники получают не только доступ к заражённому устройству, но и возможность проникнуть на устройства под управлением Windows и macOS, что открывает перед ними широкие возможности.

Например, «Лаборатория Касперского» недавно рассказывала о мультиплатформенном фреймворке MATA. Кроме того, в июне 2020 года эксперты анализировали несколько образцов вредоносного ПО под Linux, которые использовала группа Lazarus в операциях Operation AppleJeus и TangoDaiwbo, совершаемых с целью кибершпионажа и кражи денег…». ***(Зафиксирован растущий интерес злоумышленников к Linux-системам // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5690977-Zafiksirovan-rastushhij-interes-zlo.html). 15.09.2020).***

***

«Легитимный коммерческий фреймворк Cobalt Strike, созданный для пентестеров и red team и ориентированный на эксплуатацию и постэксплуатацию, давно любим хакерами, начиная от правительственных APT-группировок и заканчивая операторами шифровальщиков. И хотя он недоступен для рядовых пользователей и полная версия оценивается примерно в 3500 долларов за установку, злоумышленники все равно находят способы его использовать (к примеру, полагаются на старые, пиратские, взломанные и незарегистрированные версии).

Эксперты Cisco Talos рассказывают, что во втором квартале текущего года фреймворк использовался в 66% вымогательских атак. Аналитики пишут, что инструмент ценится ИБ-специалистами и преступниками в первую очередь за возможность развертывать в сетях жертв listeners. Они используются для мониторинга того, как зараженные узлы взаимодействуют с управляющими серверами для получения пейлоадов и дальнейших команд от злоумышленников.

«Сила Cobalt Strike заключается в том, что он предлагает множество ответов на сложные вопросы, которые могут возникнуть у злоумышленника. Развернуть listeners и beacons? Без проблем. Нужен шелл-код? Легко. Необходимо создавать поэтапные/бесэтапные исполняемые файлы? Готово. Учитывая универсальность Cobalt Strike, его популярность неудивительна. Злоумышленники все больше полагаются в работе на Cobalt Strike, а не на массовое вредоносное ПО», — говорят исследователи Cisco Talos.

В своем отчете эксперты пишут, что проанализировали структуру атак с использованием фреймворка Cobalt Strike и разработали около 50 сигнатур для Snort и опенсорсного антивирусного движка ClamAV». ***(Мария Нефёдова. Операторы вымогателей используют Cobalt Strike в 66% случаев // Хакер (https://xakep.ru/2020/09/25/cobalt-strike-stats/). 25.09.2020).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Россиянину Егору Крючкову, задержанному в США, предъявили обвинение в сговоре с целью умышленного повреждения защищенного компьютера, сообщил американский минюст.

В обвинительном заключении указывается, что Крючков якобы пытался завербовать сотрудника компании в Неваде, чтобы тот внедрил вредоносное программное обеспечение (ПО) в компьютерную сеть компании для извлечения данных из сети…

После, как утверждается, он собирался вымогать деньги у компании под угрозой обнародования добытых данных.

В пресс-релизе минюста США сказано, что с 16 июля по 22 августа 2020 года Крючков вступил в сговор с сообщниками с целью вербовки сотрудника, который должен был бы внедрить в сеть своей компании вредоносное ПО.

Минюст не уточняет, какая компания должна была стать целью кибератаки, однако ранее основатель Tesla Илон Маск подтвердил, что речь идет о заводе по производству автомобильных литий-ионных аккумуляторов Gigafactory Nevada («Гигафабрика»)». **(*Наталья Ануфриева. Россиянину предъявили в США обвинение в сговоре с целью кибератаки // Деловая газета «Взгляд» (https://vz.ru/news/2020/9/5/1058780.html). 05.09.2020).***

***

«Россиянин Артем Лифшиц, который ранее был включен в санкционный список США, обвиняется Соединенными Штатами в сговоре с целью мошенничества. Об этом сообщается на сайте Министерства юстиции США.

Согласно заявлению ведомства, российский киберэксперт является участником мошеннической схемы, в которой украденные персональные данные американских граждан используются для открытия незаконных счетов в банках и на биржах криптовалют.

Ранее США ввели санкции в отношении трех россиян из-за вмешательства в американские выборы и кибератак. В черный список, помимо Лифшица, попали Антон Андреев и Дарья Асланова, которые также якобы связаны с проводившем манипуляции во время выборов «Агентством интернет-исследований». Минфин США отмечает, что Россия использует услуги целого ряда людей, чтобы «попытаться посеять раздор между политическими партиями и вызвать внутренние разногласия» в демократических странах…» ***(США обвинили попавшего под санкции российского киберэксперта в мошенничестве // ООО «Лента.Ру» (https://lenta.ru/news/2020/09/11/moshennik/). 11.09.2020).***

***

«Міністерство юстиції США в четвер пред'явило звинувачення проти трьох іранців за звинуваченнями в крадіжці інформації у компаній, що займаються аерокосмічними та супутниковими технологіями, від імені Вартових ісламської революції.

Обвинувальні висновки здійснені після ряду дій проти ймовірних іранських кібершпигунів, включаючи заяву, зроблену раніше в четвер, про те, що до організацій та осіб, пов'язаних з іранською хакерською групою, яку іноді називають APT39, застосовуються санкції міністерства фінансів, передає Reuters.

Обвинувачені - Саїд Пуркарь Арабі, 34 роки, Мохаммад Реза Еспархам, вік невідомий, і Мохаммад Баяті, 34 роки, нібито видавали себе за своїх колег або вчених, щоб змусити своїх жертв завантажити шкідливе програмне забезпечення, заявили в прокуратурі.

Спроби знайти контактну інформацію іранських підсудних не увінчалися успіхом. Повідомлення, відправлені на адреси електронної пошти, імовірно якими користувалися хакери або поверталися як недоставлені, або не поверталися негайно.

В якийсь момент, за даними прокуратури, у Арабі, Еспаргама і Баяті було більше 1800 облікових записів, включаючи цілі в галузі аерокосмічних і

супутникових технологій, а також співробітників міжнародних урядових організацій. В обвинувальному висновку не зазначені люди або організації, що стали об'єктом переслідування, але сказано, що вони були вихідцями з США, Великої Британії, Австралії, Ізраїлю і Сінгапуру.

Прокурори заявили, що ця трійця працювала на Корпус вартових ісламської революції Ірану, який Сполучені Штати вважають терористичною організацією…» ***(Оксана Лебедина. США звинуватили трьох іранців у зломі супутникової компанії // Дзеркало тижня. Україна (https://zn.ua/ukr/WORLD/ssha-zvinuvatili-trokh-irantsiv-u-zlomi-suputnikovoji-kompaniji.html). 18.09.2020).***

***

«Президент США Дональд Трамп готовий помилувати засновника WikiLeaks і викривача держтаємниць Джуліана Ассанжа в обмін на розкриття деталей щодо кібератаки на пошту комітету Демократичної партії. Про це заявила адвокатка Ассанжа Дженніфер Робінсон в суді Лондона, передає Reuters.

Зазначається, що пропозиція полягає в оприлюдненні подробиць зламу, який відбувся в 2016 році, й імен тих, хто стоїть за кібератакою. "Пропозиція, висунута конгресменом Рорабейкером, полягала в тому, що Ассанж встановлює джерело публікацій про вибори 2016 року в обмін на деяку форму помилування", – сказала Робінсон.

Як повідомляє адвокатка, вона спостерігала за зустріччю Ассанжа й тодішнім членом Палати представників США від Республіканської партії Дейном Рорабейкром в Посольстві Еквадора у Лондоні, яка відбулася в 2017 році. Саме тоді й відбулося ймовірне озвучення відповідної пропозиції…». ***(Трамп запропонував Ассанжу помилування в обмін на подробиці зламу пошти демократів, – адвоката // Західна інформаційна корпорація(https://zik.ua/news/world/tramp_zaproponuvav_assanzhu_pomyluvannia_v_obmin_na_podrobytsi_zlamu_poshty_demokrativ__advokatka_981058). 18.09.2020).***

***

«Американские власти сообщили о вынесении приговора 39-летнему Натану Фрэнсису Уайетту (Nathan Francis Wyatt), бывшему члену небезызвестной хакерской группы The Dark Overlord (TDO).

По данным правоохранителей, с 2016 года Уайетт был участником TDO, и это были «золотые годы» для группировки, когда хакеры регулярно взламывали крупные компании, похищали конфиденциальные данные, а затем требовали у жертв огромные выкупы. Если те отказывались платить, злоумышленники продавали украденную информацию на хакерских форумах, публиковали в интернете бесплатно или сообщали об утечке прессе, чтобы нанести урн репутации пострадавшей компании.

Согласно судебным документам, роль Уайетта в частности заключалась в том, что он связывался с жертвами и вел переговоры о выкупе. Следователи вычислили его, так как несколько раз Уайетт использовал для этих целей телефонные номера, зарегистрированные на его настоящее имя. В итоге в 2017 году

хакер был арестован в Великобритании, после чего в декабре 2019 года его экстрадировали в США.

Как теперь сообщили правоохранители, Уайетт признал себя виновным в сговоре с целью совершения кражи личных данных при отягчающих обстоятельствах, а также в компьютерном мошенничестве. Хакера приговорили к пяти годам тюремного заключения, а также обязали выплатить компенсацию потерпевшим в размере 1 467 048 долларов.

Напомню, что в 2018 году в Сербии был арестован другой участник The Dark Overlord. О задержанном было известно мало: в документах он фигурировал под инициалами S.S., ему было 38 лет, и он проживал в Белграде. Какую роль он исполнял в TDO – до сих пор неизвестно.

Информации о других арестах участников The Dark Overlord нет, то есть можно предположить, что большинство членов группы по-прежнему остается на свободе…». ***(Мария Нефёдова. Участник хак-группы The Dark Overlord приговорен к пяти годам тюрьмы // Xakep (https://xakep.ru/2020/09/22/the-dark-overlord-sentenced/). 22.09.2020).***

***

«Вчера правительство США выдвинуло обвинения против пяти граждан Китая, которые подозреваются в связи с хак-группой APT41 (она же Winnti, Suckfly, Wicked Panda, Barium и так далее), организовавшей атаки более чем на 100 компаний по всему миру.

Согласно обнародованным судебным документам, группировка взламывала компании по разработке ПО, производителей компьютерного оборудования, провайдеров телекоммуникационных услуг, компании, занимающиеся социальными сетями, компании по производству видеоигр, организации в сфере здравоохранения, некоммерческие организации, учебные заведения, аналитические центры и так далее. У жертв хакеры похищали проприетарные данные, включая исходные коды, сертификаты для подписания кода, данные о клиентах и другую ценную бизнес-информацию.

Компании-жертвы Winnti находились в таких странах, как США, Австралия, Бразилия, Чили, Гонконг, Индия, Индонезия, Япония, Малайзия, Пакистан, Сингапур, Южная Корея, Тайвань, Таиланд и Вьетнам. Также власти США заявили, что члены APT41 взломали компьютерные сети иностранных правительств в Индии и Вьетнаме и атаковали продемократических политиков и активистов в Гонконге. Кроме того, были зафиксированы попытки атак на правительство Великобритании, но они не увенчались успехом…

Согласно судебным документам, первые два члена APT41 были идентифицированы и обвинены еще в августе 2019 года, вскоре после публикации отчета FireEye. Копия обвинительного заключения от 2019 года гласит, что выдвинутые обвинения связаны с атаками на компании, занимающиеся ИТ и видеоиграми, а также взломом неназванного гражданина Соединенного Королевства. Двое подозреваемых были идентифицированы как 35-летний Чжан Хаоран (张浩然) и 35-летний Тан Дайлинь (谭戴林).

Еще трем членам группировки обвинения предъявили год спустя, в августе 2020 года. Судя по документам, 35-летний Цзян Личжи (蒋 立志), 39-летний Цянь Чуань (钱川) и 37-летний Фу Цян (付强) несут ответственность за большинство атак APT41.

Власти США уверены, это эти люди являются сотрудниками подставной компании Chengdu 404 Network Technology, которая действует под контролем и по приказу официальных лиц КНР. Так, судебные документы содержат логи перехваченных чатов между Цзяном Личжи и другими предполагаемыми хакерами, где Цзян прямо заявляет, что работает под руководством высокопоставленного чиновника из Министерства общественной безопасности Китая.

Все пятеро участников APT41 остаются на свободе, но теперь их имена внесены в список самых разыскиваемых ФБР киберпреступников.

ФБР, возглавлявшее это расследование, заявляет, что ранее в этом месяце получило судебный ордер и арестовало «сотни учетных записей, серверов, доменных имен, dead drop страниц управляющих серверов, которые использовались APT41 в прошлых операциях».

Помимо этого власти США предъявили обвинения и двум малайзийским бизнесменам, которых подозревают в сговоре с участниками Winnti с целью получения прибыли от атак на разработчиков игр. Эти двое были арестованы в понедельник, 14 сентября 2020 года, в Малайзии. В настоящее время готовятся документы для их экстрадиции в США.

Согласно судебным бумагам, 46-летний Вонг Онг Хуа (Wong Ong Hua) и 32-летний Лин Ян Чинг (Ling Yang Ching) владели Sea Gamer Mall — сайтом, продававшим цифровые валюты для различных онлайн-игр. По сведениям правоохранителей, порой игровую валюту бизнесменам предоставляли участники APT41, и она была похищена у игровых компаний». ***(Мария Нефёдова. Американские власти утверждают, что хак-группа Winnti взломала более 100 компаний // Хакер (https://xakep.ru/2020/09/17/winnti-members-charges/). 17.09.2020).***

***

«…У Каліфорнії (США) прокуратура просить федерального суддю засудити росіянина Євгена Нікуліна до 12 років в'язниці за хакерські атаки на соціальні мережі LinkedIn і Formspring і сервіс Dropbox…

У липні журі присяжних в Сан-Франциско визнало Нікуліна винним у викраденні даних 112 млн користувачів (тоді повідомлялось про 117 млн) сервісів, які він зламав. Присяжні вирішили, що він відповідальний за один із найбільших витоків даних в історії США.

Нікулін свою провину не визнає, його захист попросив обмежитися терміном, який він уже відбув під вартою, і депортувати його на батьківщину. Вирок йому оголосять 29 вересня.

Євген Нікулін був затриманий у Чехії восени 2016 року на підставі ордера Інтерполу, виданого за запитом США.

У США Нікуліна звинуватили в розкраданні інформації користувачів LinkedIn, Dropbox і низки інших сервісів.

Росія зверталася з вимогою екстрадиції Нікуліна за звинуваченням у крадіжці, організованій через інтернет. Однак влада Чехії видала хакера Вашингтону». ***(У США прокуратура просить 12 років в'язниці для російського хакера, який викрав 112 млн паролів від LinkedIn та Dropbox // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/25574/2020-09-24-u-ssha-prokuratura-prosit-12-rokiv-vyaznitsi-dlya-rosiiskogo-khakera-yakii-vikrav-112-mln-paroliv-vid-linkedin-ta-dropbox/). 24.09.2020).***

***

«Гражданин России Егор Крючков, обвиняемый в США попытке организовать кибератаку на компьютерную сеть компании Tesla, отказался признать свою вину, сообщает Associated Press. "Я не виновен", - заявил Крючков во время слушаний в зале федерального окружного суда штата Невада. Судья постановил оставить Крючкова под стражей до суда, назначенного на 1 декабря. Есть вероятность, что дата будет изменена, сообщает агентство. По словам прокурора, россиянину грозит до пяти лет тюремного заключения и штраф в размере $250 тыс. За тюремным сроком последует депортация. В материалах дела говорится, что Крючков находился в США по туристической визе, когда пытался завербовать сотрудника компании Tesla, чтобы тот установил программное обеспечение, позволяющее взломать компьютерную сеть. Он был арестован 22 августа в Лос-Анджелесе, когда направлялся в аэропорт, чтобы вылететь из страны. Крючков содержится под стражей в тюрьме округа Уошо в Рино без права внесения залога». ***(Гражданин России обвиняемый в кибератаке на сеть Tesla отказался признать свою вину // Fixygen (http://www.fixygen.ua/news/20200926/grazhdanin-rossii.html). 26.09.2020).***

***

«Министерство юстиции США сообщило о вынесении приговора 43-летнему нигерийскому мошеннику Олумиде Огунреми (Olumide Ogunremi), также известному как «Тони Уильямс». Его обвиняли в причастности к взлому компьютеров и краже личных данных.

Согласно судебным документам, с июля по декабрь 2013 года Огунреми и его сообщники атаковали по электронной почте правительственные агентства США и поставщиков Администрации общих служб (General Services Administration). Мошенники рассылали фишинговые email’ы и ссылки на сайты, которые имитировали реальные письма и ресурсы правительственных агентств США, включая Агентство по охране окружающей среды. Когда ничего не подозревающим люди посещали такие поддельные страницы и вводили там свои учетные данные, те оказывались в руках хакеров.

Украденные таким образом учетные данные использовались для доступа к почтовым ящикам сотрудников с целью заказа от их лица офисных товаров, в основном картриджей с тонером для принтеров. Продукцию мошенники закупали у поставщиков, уполномоченных вести дела с правительственными учреждениями США.

Злоумышленники просили продавцов доставить заказы своим людям в Нью-Джерси и другие места, где те быстро переупаковывались, а затем переправлялись заграницу, в точки продаж, контролируемые Огунреми и его сообщниками. Затем картриджи поступали в продажу на черном рынке. По данным Министерства юстиции, в общей сложности преступники обманули поставщиков офисной продукции на сумму около 1 000 000 долларов…». ***(Мария Нефёдова. Нигерийский хакер заработал более 1 000 000 долларов на картриджах для принтеров // Xakep (https://xakep.ru/2020/09/25/cartridges-scam/). 25.09.2020).***

***

Технічні аспекти кібербезпеки

«Группа специалистов опубликовала описание теоретической атаки на TLS, которая может использоваться для расшифровки HTTPS-соединений и чтения трафика. При этом исследователи признают, что атака Raccoon носит теоретический характер и крайне сложна в исполнении.

Raccoon представляет собой классическую атаку по времени (timing attack), то есть это side-channel атака, в ходе которой преступник пытается скомпрометировать систему с помощью анализа времени, затрачиваемого на исполнение тех или иных криптографических алгоритмов. В случае Raccoon атакующий наблюдает за обменом ключами и протоколом Диффи-Хеллмана с целью восстановления нескольких байт информации.

«Это помогает злоумышленнику создать систему уравнений, а затем использовать решатель для Hidden Number Problem (HNP) и вычислить pre-master secret между клиентом и сервером», —рассказывают исследователи.

Перед данной проблемой уязвимы все серверы, использующие протокол Диффи-Хеллмана для обмена ключами и установления TLS-соединений (TLS 1.2 и ниже). Уязвимость также затрагивает DTLS. Лишь TLS 1.3 эксперты сочли безопасным.

Атака Raccoon должна осуществляться на стороне сервера и не может выполняться со стороны клиента, например, через браузеры. Кроме того, атака должна выполняться для каждого отдельного соединения клиент-сервер и не может быть использована для восстановления приватного ключа сервера и одновременной расшифровки всех соединений.

Как уже было сказано выше, атаку Raccoon крайне трудно осуществить на практике. Исследователи считают, что настоящие хакеры скорее предпочтут использовать другие, более простые и эффективные векторы атак, а не Raccoon.

И хотя авторы называют свою атаку теоретической, некоторые вендоры, тем не менее, уже выпустили патчи, чтобы защититься от Raccoon, среди них: Microsoft (CVE-2020-1596), Mozilla, OpenSSL (CVE-2020-1968) и F5 Networks (CVE-2020-5929)». ***(Мария Нефёдова. Атаку Raccoon можно использовать для расшифровки HTTPS-трафика // Xakep (https://xakep.ru/2020/09/11/raccoon-2/). 11.09.2020).***

***

«Эксперты из Швейцарской высшей технической школы Цюриха, Технологического института Стивенса, а также Амстердамского свободного университета рассказали о созданной ими спекулятивной атаке BlindSide.

Данная атака работает независимо от архитектуры и тестировалась как на процессорах Intel, так и на процессорах AMD. Суть BlindSide заключается в злоупотреблении функцией повышающей производительность процессора и использования этого для обхода защитного механизма ASLR (Address Space Layout Randomization, «Рандомизация адресного пространства»).

Отдельно отмечается, что против BlindSide не помогают патчи, ранее выпущенные для таких известных спекулятивных багов, как Spectre и Meltdown.

Исследователи рассказывают, что обычно для обмана ASLR злоумышленнику нужно найти уязвимость, относящуюся к типу «утечек информации», чтобы исследовать память и найти нужное место, где запускается целевое приложение, а затем нацелить вредоносный код точно на выделенное адресное пространство. Как правило, такое «зондирование» памяти легко обнаруживается, и защитные механизмы блокируют атакующего, однако BlindSide позволяет перенести такую атаку в плоскость спекулятивного или упреждающего исполнения (speculative), и в результате злоумышленник может остаться незамеченным.

В сущности, спекулятивное исполнение призвано повысить производительность процессоров. Так, вместе с основным потоком процессор заранее выполняет и другие задачи, которые тоже могут пригодиться. По словам исследователей, этот механизм может использоваться и для «усиления серьезности распространенных уязвимостей, в том числе ошибок нарушения целостности информации в памяти». То есть, используя спекулятивное исполнение, BlindSide может эксплуатировать какую-то уязвимость снова и снова, тщательно исследуя память, пока в итоге не будет осуществлен обход ASLR.

За счет того, что атака происходит в сфере спекулятивного исполнения, все неудачные попытки никак не влияют на процессор и стабильность его работы, и в целом они практически незаметны. Для реализации такой атаки хакеру понадобится лишь простая уязвимость, связанная с нарушением целостности информации в памяти. Сами исследователи использовали для этого проблему переполнения буфера в ядре Linux. Видео ниже демонстрирует тестовую атаку в действии». ***(Мария Нефёдова. Атака BlindSide позволяет обойти ASLR // Xakep (https://xakep.ru/2020/09/15/blindside/). 15.09.2020).***

***

«Исследователь безопасности Марсель Афрахим продемонстрировал способ, с помощью которого можно злоупотреблять службой хостинга сайтов и web-приложений Google App Engine для создания неограниченного количества фишинговых страниц, оставаясь при этом незамеченным.

Обычно мошенники используют облачные сервисы для создания вредоносного приложения, которому назначается поддомен. Затем они размещают

там фишинговые страницы или могут использовать приложение в качестве C&C-сервера для доставки вредоносного ПО.

Но структуры URL-адресов обычно создаются таким образом, чтобы их можно было легко отслеживать и блокировать с помощью продуктов корпоративной безопасности. Таким образом, ИБ-специалист может блокировать трафик к конкретному приложению, просто блокируя запросы к определенному поддомену и от него.

Однако в случае с Google App Engine ситуация немного другая. Домен Google appspot.com, на котором размещены приложения, имеет следующую структуру URL — «VERSION-dot-SERVICE-dot-PROJECT_ID.REGION_ID.r.appspot.com». В этом случае поддомен представляет собой не только приложение, но и поля версии приложения, имени службы, идентификатора проекта и идентификатора региона.

Если какое-либо из данных полей является неверным, Google App Engine не будет отображать страницу «404 Not Found», а вместо этого покажет страницу приложения по умолчанию.

Существует множество настроек поддоменов, позволяющих получить доступ к вредоносному приложению злоумышленника. Пока у каждого поддомена есть действительное поле «project_ID», недействительные варианты других полей могут использоваться по усмотрению злоумышленника для создания длинного списка поддоменов, которые все ведут к одному и тому же приложению.

Например, как продемонстрировал Афрахим, оба приведенных ниже URL-адреса, которые выглядят совершенно по-разному, представляют одно и то же приложение, размещенное на Google App Engine.

https[:]//random123-random123-random123-dot-bad-app-2020.ue.r.appspot

https[:]//insertanythingyouwanthere-xyz123-xyz123-dot-bad-app-2020.ue.r.appspot

Кроме того, большое количество вариантов поддоменов делает бесполезным подход к блокировке, основанный на индикаторах взлома». ***(Мошенники злоупотребляют Google App Engine для создания фишинговых страниц // SecurityLab.ru (https://www.securitylab.ru/news/512303.php). 21.09.2020).***

***

«Сотрудник Avast взломал кофеварку через Wi-Fi. При этом потратил на взлом всего несколько минут. После этого хакер заставил аппарат майнить криптовалюту, а также в целом парализовал работу прибора с требованием выкупа.

Эксперт по кибербезопасности Мартин Хрин отметил, что кофеварка построена на базе популярных микроконтроллеров, информации о которых в сети более чем достаточно, передает slashgear.com.

Как это удалось

Эксперт объяснил, что кофеварка не использует для запуска шифрование, поэтому программист перехватил ее прошивку при обновлении, немного модифицировал и загрузил на устройство.

После запуска прибор немного взбунтовался, бесконтрольно разливая кипяток. А также начал выводить на дисплей требование перевода денег. Также на мониторе указан URL для восстановления нормальной работы.

Кроме того, Мартин запустил на устройстве майнинг криптовалюты Monero. Правда, учитывая низкую производительность встроенного микроконтроллера, больших прибылей это ему не принесло.

Цель

Как объяснил программист, так он пытался обратить внимание производителей на необходимость обеспечить безопасность любых разумных устройств, поскольку для взлома многих из них хакерам достаточно базовых знаний алгоритмов работы электроники». ***(Ирина Полицкая. Программист взломал кофеварку и заставил майнить криптовалюту // Телеканал новостей «24» (https://techno.24tv.ua/ru/programmist-vzlomal-kofevarku-zastavil-majnit-novosti-tehnologij_n1423997). 28.09.2020).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Метод злому комп'ютерів називається атакою Pass-the-hash і є поширеним в кіберсередовищі

Спеціалісти розкрили спосіб злому Windows за допомогою саморобних тем оформлення. Про це повідомляє видання Bleeping Computer з посиланням на експерта з кібербезпеки Джиммі Бейн (Jimmy Bayne).

Спеціаліст знайшов спосіб віддаленого злому комп'ютерів під управлінням Windows за допомогою файлів тем оформлення, що мають розширення.theme. Для цього зловмиснику досить відредагувати файл теми, додавши туди інформацію для підключення до певного віддаленого сервера.

Подібний метод злому комп'ютерів називається атакою Pass-the-hash і є поширеним в кіберсередовищі.

Бейн зазначив, що на початку року розповідав про небезпечну уразливість Microsoft, однак в компанії відповіли, що не вважають описану фахівцем проблему актуальною.

Журналісти підкреслили, що за допомогою тем оформлення для Windows користувачі ОС можуть тонко налаштувати візуальний інтерфейс операційної системи, змінивши стандартні зображення робочого столу, заставку, курсор, системні звуки. Користувачі ОС також можуть поділитися з іншими власниками копії Windows створеної власноруч темою.

Раніше видання Bleeping Computer розповіло про спосіб заразити комп'ютер під управлінням Windows за допомогою вбудованого антивіруса. Нововведення, доступне в одному з останніх системних апдейтів ОС, дозволяло завантажити на пристрій шкідливу програму. При цьому антивірус зберігає працездатність і зможе виявити заражене ПО». ***(Windows зламали за допомогою тем оформлення // Українські медійні системи (https://glavcom.ua/world/hitech/windows-zlamali-za-dopomogoyu-tem-oformlennya-704197.html). 09.09.2020).***

****

«Злоумышленники, которые активно используют критическую уязвимость удаленного выполнения кода, затрагивающую более 600 000 сайтов WordPress с уязвимыми версиями плагинов File Manager, также были замечены в защите сайтов, которые они взломали, от атак других злоумышленников.

Эта критическая уязвимость позволяет злоумышленникам, не прошедшим проверку подлинности, загружать вредоносные файлы PHP и выполнять произвольный код после успешной эксплуатации [1, 2, 3]. Команда разработчиков File Manager устранила этот недостаток в выпуске File Manager 6.9.

Несмотря на то, что уязвимость была исправлена в течение нескольких часов после того, как разработчики были проинформированы дежурным сотрудником службы безопасности Seravo Вилле Корхоненом, который обнаружил уязвимость нулевого дня и продолжающиеся атаки, пытающиеся ее использовать, исследователи из охранной фирмы WordPress Defiant обнаружили более 1,7 миллиона сайтов. зондирование злоумышленниками в период с 1 по 3 сентября.

В обновленном отчете, опубликованном сегодня, аналитик угроз Defiant Рам Галл говорит, что злоумышленники не прекратили свою осаду, и общее количество сайтов WordPress, подвергшихся атаке, достигло 2,6 миллиона.

Команда разработчиков File Manager устранила активно используемую критическую уязвимость с выпуском File Manager 6.9.

Продолжающиеся атаки

По данным Defiant, в настоящее время множество злоумышленников нацелены на эту уязвимость на сайтах, на которых работают уязвимые версии плагина File Manager, но двое из них добились наибольшего успеха в развертывании вредоносных программ на уязвимых сайтах.

Одним из них является bajatax, марокканский злоумышленник, ранее известный своей склонностью к краже учетных данных пользователей с веб-сайтов электронной коммерции PrestaShop.

Как только ему удается скомпрометировать сайт WordPress в рамках продолжающихся атак, bajatax внедряет вредоносный код, который собирает и извлекает учетные данные пользователя через Telegram при любой попытке входа в систему, чтобы впоследствии продать их тому, кто предложит самую высокую цену.

Другой внедряет бэкдор в рандомизированную папку и в корневой веб-сайт сайта, оба замаскированные как файлы.ico, чтобы снизить вероятность того, что администратор сайта обнаружит оба и перекрывает доступ злоумышленника к сайту.

Как объясняет Галл, PHP-инфектор, используемый вторым злоумышленником, представляет собой вариант заражения, ранее использовавшегося для развертывания криптомайнеров и проведения SEO-спам-кампаний через взломанные сайты.

Борьба за контроль

Оба они были замечены Defiant при попытке заблокировать попытки использования других злоумышленников путем защиты паролем уязвимого файла connector.minimal.php на сайтах, которые они заразили…

«Вышеупомянутые злоумышленники были наиболее успешными благодаря своим усилиям по блокировке других злоумышленников и коллективно используют несколько тысяч IP-адресов в своих атаках».

NinTechNet, которая также сообщала о попытках использования эксплойтов, когда начинались атаки, также обнаружила попытки злоумышленников заблокировать доступ других лиц к компрометации уже зараженного сайта с помощью защиты паролем файлов, которые могут быть записаны уязвимостью File Manager.

В целом, исследователи Defiant увидели, что атаки, пытающиеся использовать эту уязвимость, исходят из более чем 370000 отдельных IP-адресов, при этом активность доступа к бэкдору практически не перекрывается.

«Единственным исключением является IP 51.83.216.204, который, похоже, является сторонней организацией, которая оппортунистически проверяет наличие обоих этих бэкдоров, а затем пытается добавить собственный бэкдор, но без особого успеха», - добавил Гал». ***(Sergiu Gatlan. Hackers are fighting a war over 300K vulnerable WordPress sites // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hackers-are-fighting-a-war-over-300k-vulnerable-wordpress-sites/). 10.09.2020).***

***

«Корпорация Intel устранила девять уязвимостей в системе безопасности, выпустив сентябрьское обновление платформы 2020 г., одна из которых является критической уязвимостью для платформ Active Management Technology (AMT) и Intel Standard Manageability (ISM).

Intel ATM является частью платформы Intel vPro, которая включает в себя процессоры Intel Core vPro и Intel Xeon, и в основном используется ИТ-отделами для удаленного обнаружения, восстановления и управления корпоративными сетевыми системами.

Эти проблемы были подробно описаны в пяти рекомендациях по безопасности, опубликованных Intel в ее Центре безопасности продуктов, с исправлениями, которые были доставлены клиентам через процесс Intel Platform Update (IPU) до раскрытия.

Intel также предоставляет списки затронутых продуктов и поддержку уязвимых продуктов в конце каждого информационного сообщения вместе с контактными данными для сообщения о других проблемах безопасности, которые могут повлиять на продукты или технологии Intel.

Повышение удаленных привилегий Intel AMT

Уязвимость AMT, отслеживаемая как CVE-2020-8758, оценена Intel как критическая проблема безопасности с базовой оценкой CVSS 9,8 и может позволить повысить привилегии уязвимых систем после успешной эксплуатации.

Уязвимость возникает из-за неправильных ограничений буфера в сетевой подсистеме, и она может позволить злоумышленникам, не прошедшим проверку

подлинности, «повысить привилегии в системах с поддержкой AMT в корпоративной сети».

«Для клиентов, использующих системы Intel vPro без поддержки AMT, аутентифицированный пользователь с локальным доступом к системе может по-прежнему иметь возможность повышать привилегии», - сказал Джерри Брайант, директор по коммуникациям Intel.

«Если платформа настроена на использование удаленного доступа, инициированного клиентом (CIRA), а обнаружение среды настроено так, чтобы указывать, что платформа всегда находится за пределами корпоративной сети, система находится в режиме только CIRA и не подвергается воздействию сетевого вектора».

Все версии Intel AMT и Intel ISM до 11.8.79, 11.12.79, 11.22.79, 12.0.68 и 14.0.39 уязвимы для атак CVE-2020-8758. К счастью, по словам Брайанта, уязвимость в настоящее время не используется в дикой природе.

В июне Intel исправила две другие критические уязвимости повышения привилегий AMT с рейтингом 9,8 CVSS (CVE-2020-0594 и CVE-2020-0595), что повлияло на нестандартные конфигурации, в которых AMT был настроен на использование интернет-протокола версии 6 (IPv6).

Рекомендации по обновлению платформы Intel за сентябрь 2020 г.

Сегодняшние рекомендации Intel по безопасности перечислены в таблице ниже с информацией об их рейтинге серьезности диапазона CVSS, чтобы помочь пользователям определить приоритетность развертывания исправлений.

Корпорация Intel рекомендует проверить ссылки для загрузки, указанные в рекомендациях, или узнать у производителей вашей системы и поставщиков ОС, как получить эти обновления…

Полный список сайтов поддержки производителей компьютеров, с которых можно получить большинство обновлений, можно найти здесь.

Intel не известно ни о каких проблемах, решаемых сегодня, которые активно используются в дикой природе, но клиентам по-прежнему рекомендуется как можно скорее установить выпущенные сегодня обновления безопасности, чтобы заблокировать будущие атаки». ***(Sergiu Gatlan. Intel fixes critical flaw in corporate remote management platform // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/intel-fixes-critical-flaw-in-corporate-remote-management-platform/). 08.09.2020).***

***

«Уязвимость «BLURtooth» позволяет злоумышленникам в радиусе действия беспроводной сети обходить ключи аутентификации и отслеживать устройства, использующие реализации Bluetooth 4.0–5.0.

Обнаружена высокозащищенная уязвимость Bluetooth, которая может позволить неаутентифицированному злоумышленнику в радиусе действия беспроводной сети подслушивать или изменять связь между сопряженными устройствами.

Недостаток (CVE-2020-15802), независимо обнаруженный исследователями из Федеральной политехнической школы Лозанны (EPFL) и Университета Пердью,

обозначается как «BLURtooth». Проблема существует в процессе сопряжения для реализаций Bluetooth 4.0–5.0. Этот процесс сопряжения называется кросс-транспортным ключом (CTKD).

«Устройства… использующие [CTKD] для сопряжения уязвимы для перезаписи ключа, что позволяет злоумышленнику получить дополнительный доступ к профилям или службам, которые не ограничены, за счет снижения надежности ключа шифрования или перезаписи аутентифицированного ключа неаутентифицированным ключом», - говорит к совету по безопасности в среду Координационного центра Carnegie Mellon CERT.

Атака BLURtooth

Существует два типа протоколов Bluetooth, связанных с атакой: старый Bluetooth Classic (также известный как Bluetooth Basic Rate / Enhanced Data Rate или BR / EDR) и новый Bluetooth Low Energy (BLE). В то время как BR / EDR в основном используются для аудиоприложений, таких как беспроводные телефонные соединения, беспроводные наушники и беспроводные динамики, BLE чаще встречается в носимых устройствах, интеллектуальных устройствах Интернета вещей, оборудовании для мониторинга фитнеса и аксессуарах с батарейным питанием, таких как клавиатура.

Процесс CTKD используется, когда два двухрежимных устройства соединяются друг с другом - «двухрежимный» означает, что они поддерживают как BLE, так и BR / EDR. Этот процесс означает, что устройствам нужно всего лишь соединиться через BLE или BR / EDR, чтобы получить ключи шифрования, называемые ключами связи, для обоих типов транспорта за один раз.

Однако дыра в CTKD позволяет снизить «стойкость» этих ключей шифрования Link Key (дополнительные технические подробности о том, где именно в CTKD существует уязвимость, а также конкретные шаги, необходимые для ее использования, пока недоступны). Это, в свою очередь, дает злоумышленнику возможность связать свои собственные устройства с целевым устройством без аутентификации.

Чтобы эта атака была успешной, злоумышленник должен находиться в пределах радиуса действия уязвимого Bluetooth-устройства. Это может варьироваться от 330 футов для устройств Bluetooth 4.0 до 800 футов для Bluetooth 5.0.

Чтобы быть уязвимым, устройство должно поддерживать транспорты BR / EDR и BLE, а также поддерживать CTKD. Он также должен обеспечивать прозрачное выполнение спаривания или связывания без аутентификации или слабой стойкости ключа по крайней мере для одного из типов транспорта; это позволяет злоумышленникам вмешиваться между двумя транспортами, выдавая себя за ранее сопряженное устройство. Таким образом, это позволяет их неаутентифицированным ключам шифрования заменять аутентифицированные ключи.

«Если устройство, подделывающее идентификационные данные другого устройства, становится парным или связанным на транспорте, и CTKD используется для получения ключа, который затем перезаписывает ранее существовавший ключ большей силы или который был создан с использованием

аутентификации, тогда может произойти доступ к аутентифицированным службам, Согласно сообщению по безопасности, опубликованному в среду Bluetooth Special Interest Group (SIG), организацией, которая курирует разработку стандартов Bluetooth. «Это может позволить атаку типа «злоумышленник посередине» (MITM) между устройствами, ранее связанными с использованием аутентифицированного спаривания, когда эти одноранговые устройства оба уязвимы».

Затем злоумышленник может перехватить связь между двумя устройствами, что позволит им шпионить за сообщениями или, возможно, даже изменять их.

Устранение проблем с Bluetooth

Bluetooth SIG рекомендует, чтобы потенциально уязвимые реализации Bluetooth вводили ограничения на CTKD, которые были предусмотрены в базовой спецификации Bluetooth версии 5.1 и более поздних. Эти ограничения предотвращают перезапись аутентифицированного ключа или ключа заданной длины неаутентифицированным ключом или ключом уменьшенной длины.

«Bluetooth SIG также широко сообщает подробности об этой уязвимости и способах ее устранения нашим компаниям-членам и призывает их быстро интегрировать любые необходимые исправления», - сообщает Bluetooth. «Как всегда, пользователи Bluetooth должны убедиться, что они установили последние рекомендуемые обновления от производителей устройств и операционных систем»…». ***(Lindsey O'Donnell. Bluetooth Bug Opens Devices to Man-in-the-Middle Attacks // Threatpost (https://threatpost.com/bluetooth-bug-mitm-attacks/159124/). 10.09.2020).***

***

«Хакеры сканируют Сеть на предмет уязвимых сетевых хранилищ (NAS) с несколькими версиями прошивки QNAP с целью проэксплуатировать трехлетнюю уязвимость удаленного выполнения кода.

По словам исследователей из Qihoo 360 Network Security Research Lab (NetLab), эксплуатация уязвимости позволяет удаленным неавторизованным злоумышленникам выполнить проверку подлинности с помощью исполняемого файла authLogout.cgi, поскольку он не может корректно проверить вводимые данные (не отфильтровывает специальные символы) и вызывает системную функцию для запуска командной строки, что позволяет удаленно выполнить код.

Эксперты сообщили QNAP PSIRT 13 мая о своих находках, и три месяца спустя им сообщили, что компания исправила проблему в версии прошивки 4.3.3, выпущенной 21 июля 2017 года.

«В данной версии системная функция заменена на qnap_exec, а функция qnap_exec определена в /usr/lib/libuLinux_Util.so.0. Использование execv для выполнения специальной команды позволило избежать внедрения команды», — пояснили специалисты.

Злоумышленники, стоящие за этими продолжающимися атаками, еще не полностью автоматизировали процесс и осуществляют некоторые части процесса вручную. В 360 Netlab еще не определили конечную цель злоумышленников, но обнаружили, что они развертывают одни и те же две полезные нагрузки на всех скомпрометированных устройствах, одной из которых является обратная оболочка,

работающая порте TCP/1234». ***(Хакеры внедряют бэкдоры в NAS QNAP с помощью 3-летней RCE-уязвимости // SecurityLab.ru (https://www.securitylab.ru/news/511633.php). 01.09.2020).***

***

«Эксперты из Университета Пердью предупредили, что миллиарды смартфонов, планшетов, ноутбуков и IoT-устройств, использующие Bluetooth Low Energy (BLE), уязвимы перед новой атакой BLESA (Bluetooth Low Energy Spoofing Attack).

Напомню, что BLE представляет собой «облегченную» версию стандарта Bluetooth, созданную для экономии заряда аккумулятора при активности Bluetooth-соединений. Благодаря улучшенному энергосбережению BLE получил широкое распространение и стал использоваться практически во всех устройствах, работающих от аккумуляторов.

Подавляющее большинство проблем, ранее выявленных в BLE, были обнаружены в механизме сопряжения, но исследователи практически игнорировали другие части протокола. Исправить это решила группа из семи экспертов из Университета Пердью, поставившая перед собой задачу изучить другие аспекты BLE. В частности, работа исследователей сосредоточилась вокруг процесса «повторного подключения» (reconnection).

Эта операция выполняется после того, как два BLE-устройства (клиент и сервер) аутентифицировали друг друга в ходе сопряжения. Повторное подключение происходит в том случае, если устройства вышли за пределы диапазона, а затем снова вернулись в зону действия BLE. При повторном подключении устройства должны повторно проверить криптографические ключи друг друга, ранее согласованные во время сопряжения, повторно подключиться друг другу и продолжать обмен данными.

Исследовательская обнаружили, что спецификация BLE описывает процесс повторного подключения весьма размыто, и в результате при реализации reconnection в разных имплементациях BLE возникают две системные проблемы в цепочке поставок:

- зачастую аутентификация во время повторного подключения устройства оказывается необязательной;
- аутентификацию можно обойти, если устройству пользователя не удается вынудить IoT-устройство аутентифицировать передаваемые данные.

В итоге эти проблемы открывают возможность для проведения атаки BLESA, в ходе которой находящийся неподалеку злоумышленник обходит проверки при повторном подключении и передает поддельные данные на BLE-устройство, вынуждая людей и автоматику принимать ошибочные решения. Простую демонстрацию BLESA в действии можно увидеть ниже.

Ученые отмечают, что BLESA представляет угрозу не для всех имплементаций BLE. Так, уязвимыми были признаны BlueZ (используется IoT-девайсами на базе Linux), Fluoride (Android), а также iOS BLE. Но BLE на Windows-устройствах оказался неподвержен проблеме.

«По состоянию на июнь 2020 года, Apple признала проблему уязвимостью (CVE-2020-9770) и уже устранила ее. Реализация Android BLE на нашем тестовом устройстве (Google Pixel XL под управлением Android 10) по-прежнему уязвима», — пишут исследователи.

В свою очередь, разработчики BlueZ уже пообещали, что пересмотрят свой код и сделают повторные подключения неуязвимыми перед BLESA.

К сожалению, эксперты предсказывают, что исправление проблемы BLESA станет настоящей головной болью для системных администраторов. Дело в том, что множество IoT-устройств, проданных за последнее десятилетие, попросту не имеет встроенных механизмов обновления, а значит, эти устройства останутся без патчей.

Кроме того, обычно защита от Bluetooth-атак подразумевает, что сопряжение устройств должно проводиться в контролируемых средах. Однако защита от BLESA — это более сложная задача, так как атака нацелена на операцию повторного подключения. К примеру, злоумышленники могут спровоцировать отказ в обслуживании, чтобы принудительно разорвать соединение Bluetooth, а затем запустить повторное подключение и выполнить атаку». ***(Мария Нефёдова. Миллиарды устройств с Bluetooth уязвимы перед атакой BLESA // Xakep (https://xakep.ru/2020/09/16/blesa/). 16.09.2020).***

***

«Компания Palo Alto Networks устранила уязвимости в PAN-OS, операционной системе, использующейся межсетевыми экранами следующего поколения (NGFW) Palo Alto Networks. Уязвимости были обнаружены экспертами Positive Technologies. Эксплуатируя их, злоумышленник может получить доступ к конфиденциальным данным или продолжить развивать атаку и проникнуть во внутренние сегменты сети компании, использующей уязвимые средства защиты.

Уязвимость CVE-2020-2037 с оценкой 7,2 относится к классу Command Injection. Она позволяет удаленному пользователю выполнять произвольные команды в операционной системе межсетевого экрана. Для атаки необходима авторизация в веб-интерфейсе управления данным ПО. После этого атакующий может перейти в определенный раздел межсетевого экрана, разместить вредоносный код в одной из веб-форм и получить максимальные привилегии в операционной системе.

Следующая обнаруженная уязвимость CVE-2020-2036 с оценкой 8,8 относится к классу XSS (XSS – Cross-Site Scripting – межсайтовое выполнение сценариев) – внедрение в страницу вредоносного кода, который будет выполнен на компьютере пользователя при открытии им этой страницы). Если потенциальная жертва, которая авторизована в панели администратора, откроет специально сформированную вредоносную ссылку, то злоумышленник сможет выполнять любые действия от ее имени в контексте приложения Palo Alto, проводить спуфинг страницы и развивать атаки. Атака возможна из интернета, но если панель администратора расположена внутри, злоумышленнику понадобится знать адрес панели администратора внутри сети.

Еще одна уязвимость CVE-2020-2038 с оценкой 7,2 значительно расширяла уже имеющуюся допустимую функциональность (речь идет о Command Injection). По умолчанию при работе с данным интерфейсом установлены ограничения на вызов системных команд. Исключением являются некоторые базовые из них (например, ping), однако, используя недостаточную фильтрацию пользовательских данных, можно внедрить любые команды ОС. Таким образом, злоумышленник, имеющий API-ключ или пользовательские данные для его генерации, мог выполнять произвольные системные команды с максимальными привилегиями.

Наконец, четвертая обнаруженная экспертами Positive Technologies уязвимость (CVE-2020-2039, рейтинг 5,3) могла позволить неавторизованному пользователю загружать файлы произвольного содержимого и размера в определенную директорию на сервере, что может привести к недоступности устройства (DoS). Для ее эксплуатации злоумышленник может загружать неограниченное количество файлов различного размера, что приведет к полному исчерпанию свободного места в системе. Из-за отсутствия свободного места веб-панель администрирования устройства становится недоступной.

Для устранения уязвимостей необходимо обновить программное обеспечение межсетевого экрана до последней версии согласно рекомендациям, указанным на сайте производителя». ***(Уязвимости в ПО брандмауэров Palo Alto могут угрожать безопасности внутренних сетей // Компьютерное Обозрение (https://ko.com.ua/uyazvimosti_v_po_brandmaujerov_palo_alto_mogut_ugrozhat_bezopasnosti_vnutrennih_setej_134487). 14.09.2020).***

***

«Компания Mozilla исправила три опасные уязвимости в версиях браузеров Firefox 81 и Firefox Extended Support Release (ESR) 78.3 Mozilla. Эксплуатация некоторых из проблем позволяет удаленно запускать произвольный код.

Две опасные уязвимости (CVE-2020-15674 и CVE-2020-15673) были исправлены в средствах защиты памяти браузера, предотвращающих такие проблемы с доступом к памяти, как переполнение буфера. Первая проблема (CVE-2020-15674) затрагивает версию Firefox 80, а вторая (CVE-2020-15673) — версии Firefox 80 и Firefox ESR 78.2.

«Некоторые из проблем свидетельствовали о повреждении памяти, и мы предполагаем, что при достаточных усилиях злоумышленники могли использовать их для запуска произвольного кода», — говорится в сообщении Mozilla Foundation.

Как сообщили специалисты Mozilla, данные проблемы можно использовать для сбора конфиденциальных данных с сайтов в других окнах или для внедрения данных или кода на эти сайты без каких-либо дополнительных действий со стороны пользователя.

С выпуском Firefox 81 также была исправлена опасная уязвимость в реализации библиотеки web-графики (WebGL) — JavaScript API для визуализации интерактивной 2D- и 3D-графики в любом совместимом web-браузере.

Проблема (CVE-2020-15675) представляет собой уязвимость использования памяти после освобождения. Если после освобождения области памяти программа

не очищает указатель на эту память, злоумышленник может воспользоваться этим для взлома программы». ***(Mozilla устранила три опасные уязвимости в версии Firefox 81 // SecurityLab.ru (https://www.securitylab.ru/news/512390.php). 23.09.2020).***

***

«Системные администраторы, использующие Samba в качестве контроллера домена, должны в срочном порядке обновить свои установки, поскольку они также подвержены недавно обнаруженной уязвимости ZeroLogon.

ZeroLogon (CVE-2020-1472) представляет собой уязвимость повышения привилегий в Microsoft Windows Server. Проблема существует из-за ненадежного криптографического алгоритма в механизме аутентификации Netlogon. С ее помощью атакующий может имитировать любой компьютер в сети при аутентификаци на контроллере домена, отключать функции безопасности Netlogon и изменять пароль в базе данных Active Directory контроллера домена.

Уязвимость была частично исправлена еще в августе, но подробности о ней стали известны только недавно. Агентство по кибербезопасности и безопасности инфраструктуры Министерства внутренней безопасности США потребовало от правительственных органов исправить Zerologon к 21 сентября.

Согласно уведомлению разработчиков проекта с открытым исходным кодом Samba, уязвимость также затрагивает некоторые его конфигурации и позволяет атакующим получить доступ к домену на уровне администратора.

По словам разработчиков проекта Эндрю Бартлетта (Andrew Bartlett) и Дугласа Бэгнэлла (Douglas Bagnall), уязвимость затрагивает не все версии Samba и не все конфигурации. К примеру, проблема не затрагивает конфигурацию по умолчанию в версии 4.8 и более поздних.

Под угрозой находится Samba, запущенная как Active Directory или классический контроллер домена NT4. Администраторам, использующим Samba в качестве файлового сервера, также рекомендуется установить обновление». ***(Уязвимость ZeroLogon затрагивает некоторые версии Samba // SecurityLab.ru (https://www.securitylab.ru/news/512378.php). 23.09.2020).***

***

«Плата исследователям безопасности за поиск уязвимостей в программном обеспечении или сервисах становится все более распространенным явлением. Программы «bug bounty» позволяют специалистам получать деньги за обнаружение проблем, в то время как организации получают выгоду от возможности усилить свою безопасность.

Американская компания HackerOne, запускающая программы вознаграждения за обнаружение уязвимостей для организаций, включая Министерство обороны США и Google, опубликовала новые данные о количестве уязвимостей, обнаруженных хакерами, и о суммах вознаграждений. На сегодняшний день зарегистрировано более 181 тыс. уязвимостей, а участникам программ выплачено в общей сложности более $100 млн.

За последний год исследователям безопасности по всему миру было присуждено вознаграждение на сумму более $44,75 млн, что на 86% больше, чем в прошлом году. Средняя сумма вознаграждения за обнаружение критических уязвимостей увеличилась до $3650, что на 8% больше, чем в прошлом году, тогда как средняя сумма, выплачиваемая за уязвимость, составляет $979. Сообщения о критических уязвимостях составляют около 8% всех отчетов, а отчеты об опасных проблемах — 21%.

Как сообщили эксперты, «участие в программах вознаграждения за обнаружение уязвимостей остается постоянным и стабильным источником дохода» для некоторых зарегистрированных специалистов. Каждый пятый участник признал, что поиск уязвимостей — единственный источник дохода.

Пандемия коронавирусной инфекции (COVID-19) привела к всплеску злонамеренных атак на организации, но она также вызвала увеличение числа хакеров, стремящихся помочь найти и исправить уязвимости. Таким образом, количество регистраций новых участников программ bug bounty увеличилось на 59% за несколько месяцев после начала пандемии, а количество сообщений об обнаруженных уязвимостях увеличилось на 28%». ***(Хакеры стали больше зарабатывать за участие в программах bug bounty // SecurityLab.ru (https://www.securitylab.ru/news/512371.php). 23.09.2020).***

***

«Файлы Windows MSI открывают доступ злоумышленникам, хотя в основном ошибка была исправлена в июле.

Уязвимость Citrix Workspace, исправленная в июле, имеет вторичный вектор атаки, который позволяет злоумышленникам повышать привилегии и удаленно выполнять произвольные команды под учетной записью SYSTEM.

Ошибка (CVE-2020-8207) существует в службе автоматического обновления приложения Citrix Workspace для Windows. Согласно рекомендациям Citrix, это может позволить локальное повышение привилегий, а также удаленную компрометацию компьютера, на котором запущено приложение, когда включен общий доступ к файлам Windows (SMB).

По словам Pen Test Partners (MSI - это расширение имени файла пакетов установщика Windows), недавно было обнаружено, что эта ошибка, хотя в основном исправлена за лето, все еще позволяет злоумышленникам злоупотреблять установщиками MSI, подписанными Citrix. Это превращает ошибку в уязвимость удаленного внедрения в командную строку.

Служба обновлений изначально полагалась на ошибочный хэш файла в полезной нагрузке JSON, чтобы определить, следует ли продолжать обновление или нет, позволяя злоумышленникам загружать свой собственный код, используя слабый хэш. Чтобы решить эту проблему, последние каталоги обновлений теперь загружаются напрямую с серверов обновлений Citrix, а служба «перекрестно ссылается на хэши с файлом, который запрашивается для установки из атрибута UpdateFilePath», - пишут исследователи из Pen Test Partners в сообщение в понедельник.

«Если файл обновления подписан, действителен и хэш файла обновления соответствует одному из файлов в манифесте, файл обновления выполняется для выполнения обновления», - пояснили они.

Однако патч не препятствовал удаленному подключению, чтобы ограничить поверхность атаки.

«В каталоге есть исполняемые файлы и файлы MSI для установки», - заявили в компании. «С другой стороны, файлы MSI не могут выполняться так же, как исполняемые файлы, поэтому служба обновления должна обрабатывать их по-другому».

При просмотре кода запуска установщика исследователи обнаружили, что приложение проверяет расширение файла, запрашиваемого для обновления, и, если оно заканчивается на MSI, предполагается, что это файл установщика Windows. Поскольку файл MSI проверяется на наличие действительной подписи и имеет перекрестную ссылку с текущим каталогом, злоумышленники не могут напрямую устанавливать произвольные файлы MSI.

Несмотря на то, что файлы MSI подписаны и хешированы для предотвращения изменений, одной из функций, поддерживаемых установщиком Windows, является преобразование MSI (MST).

«Как следует из названия, MSI Transforms поддерживает изменение или преобразование базы данных MSI каким-либо образом перед установкой», - заявляют Pen Test Partners. «Администраторы домена обычно используют эту функцию для распространения файлов MSI в средах Active Directory, которые не всегда работают автоматически, если выполняются самостоятельно. Например, может быть создан MST, который будет вводить код активации продукта перед установкой».

Чтобы применить MST, пользователи должны указать путь к файлу преобразования в командной строке, которая объединяет основной файл MSI с изменениями, присутствующими в файле MST во время процесса установки.

В этом и заключается ошибка: «Поскольку мы можем контролировать аргументы, передаваемые в msiexec, мы можем включить путь к вредоносному преобразованию, но с использованием официального подписанного MSI-файла Citrix, который присутствует в файле каталога», - заявили исследователи.

Вредоносные преобразования могут быть созданы с помощью существующего инструмента под названием Microsoft Orca, который они добавили, или с помощью специального инструмента. Затем, чтобы воспользоваться уязвимостью, злоумышленники поместили исходный установщик MSI и MST в общий сетевой ресурс, готовый для машины жертвы.

«И локальный, и удаленный методы повышения привилегий могут быть использованы только тогда, когда экземпляр CitrixReceiverUpdate.exe, как и раньше, работает на хосте жертвы», - заключили исследователи. «Я думаю, что на этот раз использовать удаленный вектор проще, поскольку вы можете разместить файлы MSI и MST в общей сетевой папке под контролем злоумышленника».

Пользователи Citrix Workspace для Windows должны обновить свои приложения до последней версии, содержащей исправленный патч». ***(Tara Seals.***

Known Citrix Workspace Bug Open to New Attack Vector // Threatpost (https://threatpost.com/citrix-workspace-new-attack/159459/). 22.09.2020).

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«…В новой версии браузера Vivaldi… встроенный блокировщик рекламы и слежки теперь поддерживает правила, повышающие безопасность работы в интернете…

Еще несколько улучшений, добавленных благодаря запросам пользователей: поддержка блокировки всей страницы – встроенный блокировщик рекламы и слежки теперь поддерживает блокировку страницы целиком. Пользователи, которые добавляют собственные наборы правил, теперь могут использовать параметр ‘document’ в правилах, чтобы блокировать целые страницы. Это шаг к большей совместимости с набором правил uBlock Origin». ***(Браузер Vivaldi помогает лучшей идентификации веб-сайтов для предотвращения фишинга // Компьютерное Обозрение (https://ko.com.ua/brauzer_vivaldi_pomogaet_luchshej_identifikacii_veb-sajtov_dlya_predotvrashheniya_fishinga_134415). 08.09.2020).***

***

«Инженеры Mozilla работают над новой функцией безопасности для браузера Firefox, которая усложнит вредоносным web-страницам инициирование автоматических загрузок и внедрение вредоносных файлов на компьютеры пользователей.

Речь идет о хорошо известных атаках типа drive-by (скрытые загрузки), осуществляемых, когда пользователь посещает сайт с вредоносным кодом, устанавливающим вредоносное ПО на устройство пользователя.

Хотя в популярных браузерах, таких как Chrome, Firefox или Internet Explorer уже реализованы различные меры защиты от drive-by-атак, полностью предотвратить их не представляется возможным, поскольку производители не могут полностью блокировать легитимные функции в браузерах, которые эксплуатируются в подобных атаках.

В качестве одной из таких защитных мер является блокировка загрузок, инициированных всплывающими фреймами (iframe) с атрибутом sandbox (атрибут позволяет установить ряд ограничений на контент загружаемый во фрейме, к примеру, блокировать формы и скрипты), которые часто используются для загрузки рекламы и встроенных виджетов на сторонних сайтах. Идея объясняется тем, что сайты редко инициируют загрузки через такие фреймы, поскольку большинство виджетов обычно используется для встраивания контента.

Впервые функция блокировки загрузок, инициированных через фреймы с атрибутом sandbox, появилась в версии Google Chrome 73, выпущенной в марте

2019 года, опция была полностью удалена в выпуске Chrome 83 в мае нынешнего года.

Теперь же об аналогичных планах сообщили разработчики Firefox. Начиная с версии Firefox 82, запланированной к выходу в октябре 2020 года, браузер начнет блокировать все загрузки файлов, источником которых является фрейм с атрибутом sandbox. Исключение составят случаи, когда владелец сайта или провайдер web-виджета разрешат загрузку». ***(В Firefox появится новая функция защиты от автоматической загрузки вредоносных файлов // SecurityLab.ru (https://www.securitylab.ru/news/511747.php). 04.09.2020).***

***

«Группа из Сингапурского университета технологии и дизайна (SUTD), которую возглавляет доцент Судипта Чаттопадхай (Sudipta Chattopadhyay), разработала и внедрила инструментарий Greyhound, используемый для обнаружения набора из 11 критических уязвимостей протокола Bluetooth Low Energy (BLE).

Было обнаружено, что эти уязвимости, получившие коллективное название SweynTooth, могут вызывать сбой, перезагрузку или обход функций безопасности как минимум 12 устройств на базе BLE от восьми поставщиков, используемых в нескольких сотнях IoT-продуктов, включая кардиостимуляторы, носимые фитнес-трекеры и дверные замки.

С тех пор как код SweynTooth был сделан общедоступным, несколько производителей продуктов IoT использовали его для проверки безопасностью своих продуктов. В одном только Сингапуре сообщалось об 32 медицинских устройствах, оказавшихся уязвимыми к SweynTooth, и 90% их производителей уже предприняли необходимые превентивные действия.

Агентство кибербезопасности и Управление здравоохранения Сингапура, а также Департамент внутренней безопасности и Управление по контролю за продуктами и лекарствами США, сотрудничают с исследовательской группой SUTD, чтобы лучше уяснить масштабы выявленной проблемы. Они также развернули публичную кампанию по информированию производителей медицинского оборудования, медицинских учреждений и конечных пользователей о потенциальных рисках.

Исследование коллектива SUTD было представлено на ежегодной технической конференции USENIX в июле, его презентация также пройдёт в следующем месяце в рамках Международной кибернедели Сингапура.

Структура Greyhound сделана модульной, что открывает возможности адаптировать её для тестирования разнообразных протоколов — как уже используемых в IoT, так и перспективных, включая 5G и NarrowBand-IoT, требующих тщательного и систематического аудита безопасности». ***(Набор уязвимостей BLE представляет опасность для медицинской техники // Компьютерное Обозрение (https://ko.com.ua/nabor_uyazvimostej_ble_predstavlyaet_opasnost_dlya_medicinskoj_tehniki_134597). 22.09.2020).***

***

«Дин Паппас, менеджер по связям с разработчиками в Ethereum Classic Labs (ETC Labs) сообщил, что их командой готовится выпуск инструмента MESS для предотвращения атаки 51% на сеть Ethereum Classic. Согласно опубликованному сообщению на Medium, Modified Exponential Security Scoring, или MESS, представляет собой алгоритм окончательности, разработанный командой ETC Core в сотрудничестве с поставщиками средств кибербезопасности OpenRelay и ChainSafe. Новое решение сделает атаки 51% на блокчейн Ethereum Classic на 3000% дороже, чем сегодня. Злоумышленникам теперь придется потратить не менее $20 млн на выполнение злонамеренной деятельности. Даже с такими затратами будет нелегко собрать достаточно высокий хешрейт для осуществления атаки. Концепция MESS построена на принципе «выигрывает самая тяжелая цепь», в которой ноды ищут кратчайший способ связи друг с другом из-за чего злоумышленнику не предоставляется возможность получения контроля над ETC, построив длинную цепочку. Паппас подчеркнул, что MESS будет реализован без разделения цепочки и в ближайшее время. Новый инструмент еще необходимо проверить в тестовой среде с моделированием гипотетических атак и 150 узлами. Реализация разработана в рамках сетевого клиента Core-Geth. Ранее сеть Ethereum Classic неоднократно подвергалась атакам 51%. В ходе злонамеренных действий злоумышленникам удавалось инициировать раскол сети ETC. После многочисленных эффективных атак некоторые централизованные биржи приостановили ввод и вывод средств для держателей токенов ETC». ***(Сергей Ковалев. В ETC Labs анонсировали выпуск инструмента MESS для предотвращения атаки 51% на сеть Ethereum Classic // BitBetNews.com (https://www.bitbetnews.com/news-crypto/v-etc-labs-anonsirovali-vypusk-instrumenta-mess-dlja-predotvrashhenija-ataki-51-na-set-ethereum-classic.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+bitbetnews+%28%D0%91%D0%BB%D0%BE%D0%B3+%D0%BE+%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B2%D0%B0%D0%BB%D1%8E%D1%82%D0%B0%D1%85+bitbetnews.com%29). 21.09.2020).***

***

«Oracle объявила о запуске облачных сервисов Cloud Guard и Maximum Security Zones. Благодаря Oracle Maximum Security Zones корпорация становится первым провайдером публичных облачных сервисов, который с самого начала работы клиента в облаке автоматически применяет основанные на лучших практиках политики безопасности. Это позволяет предотвратить ошибки при конфигурации и обеспечить безопасное развертывание рабочих нагрузок. Oracle Cloud Guard осуществляет непрерывный мониторинг конфигураций и действий для выявления и автоматического устранения угроз при выполнении повседневных операций во всех региональных ЦОДах Oracle Cloud. С этими новыми инструментами Oracle является единственным провайдером облачных сервисов, который без дополнительной платы предлагает своим клиентам панель управления состоянием облачной безопасности (Cloud Security Posture Management, CSPM), а

также множество встроенных инструментов автоматического реагирования на угрозы для быстрого и эффективного снижения рисков.

Все больше компаний переносят критичные для бизнеса нагрузки в облако. Растущая популярность облаков привела к возникновению новых слепых зон безопасности. За последние два года они стали причиной более 200 утечек данных, из-за которых были скомпрометированы более 30 млрд. записей. По прогнозам Gartner, к 2025 г. 99% инцидентов безопасности в облаке будут происходить по вине клиентов. Сегодня от облачных пользователей и администраторов ожидают, что они понимают, как работают облачные сервисы, умеют правильно производить их настройку и осуществлять поддержку облачных сред. Организации, в которых произошла утечка данных из-за ошибок в конфигурации, понесли существенный ущерб вследствие потери репутации, затрат на восстановление данных и выплат штрафов. Oracle Maximum Security Zones и Oracle Cloud Guard воплощают десятилетия опыта по обеспечению корпоративной безопасности и интегрируют лучшие практики в публичное облако Oracle в автономном режиме. Они позволяют клиентам наращивать облачные активы безопасным образом с первого дня использования.

Сервис Oracle Cloud Guard уже доступен во всех коммерческих региональных ЦОДах компании. Он выполняет функции агрегатора журналов и событий и непосредственно интегрируется со всеми основными сервисами Oracle Cloud Infrastructure для вычислений, хранения информации и организации сети (Compute, Networking, Storage). Кроме того, он автоматически предоставляет компоненты для целеуказания, контроля параметров и реагирования.

Oracle Maximum Security Zones позволяет использовать средства управления доступом IaaS для ограничения потенциально вредоносных действий или конфигураций благодаря новому определению политик, которое применяется к выбранным наборам ресурсов облачной системы. Этот новый сервис Oracle Cloud Infrastructure позволяет с самого начала гарантировать безопасность ресурсов благодаря применению лучших практик для наиболее ответственных нагрузок. Oracle Maximum Security Zones включает в себя политики для нескольких основных сервисов Oracle Cloud Infrastructure, включая Object Storage, Networking, Encryption, DBaaS и File Storage.

Новые сервисы предназначены для совместного использования и расширяют возможности, предоставляемые публичными облачными системами Oracle второго поколения, для которых безопасность является краеугольным камнем». ***(Новые сервисы Oracle позволяют снизить риски безопасности клиентов облачных систем // Компьютерное Обозрение (https://ko.com.ua/novye_servisy_oracle_pozvolyayut_snizit_riski_bezopasnosti_klientov_oblachnyh_sistem_134596). 22.09.2020).***

***

«Федеральная комиссия по регулированию в области энергетики США (Federal Energy Regulatory Commission, FERC) и корпорация North American Electricity Reliability Corporation (NERC) выпустили доклад, в котором

представлены лучшие практики в области реагирования и восстановления систем после кибератак.

Доклад базируется на исследовании, проведенном сотрудниками FERC, NERC и региональных представительств NERC. В ходе исследования использовалась информация, предоставленная специалистами восьми американских электроэнергетических компаний разных масштабов и функций.

Как выяснилось в ходе исследования, какой-либо универсальной модели реагирования и восстановления после инцидента безопасности, которая стала бы панацеей, не существует. Планы реагирования на инциденты у компаний, принявших участие в исследовании, во многом схожи, например, они базируются на одном и том же фреймворке NIST (SP 800-61). Однако есть и некоторые различия. К примеру, некоторые предприятия разработали собственные планы реагирования на инциденты, которые могут затронуть конкретно их операционные и рабочие сети.

В своем докладе FERC и NERC выявили практики, которые электроэнергетическим компаниям рекомендуется принять во внимание при составлении плана реагирования на инциденты.

На этапе подготовки плана авторы доклада рекомендуют четко распределить роли между сотрудниками и наделить их полномочиями по принятию мер, чтобы в случае инцидента безопасности избежать ненужных проволочек. Компании должны обеспечить персоналу достойную подготовку и возможность постоянно обновлять свои навыки.

На этапе обнаружения и анализа инцидентов рекомендуется использовать определение исходных данных для обнаружения потенциальных инцидентов и дерево решений или блок-схему для быстрой оценки того, будет ли достигнут ли определенный порог риска и квалифицируются ли определенные обстоятельства как событие.

На этапе локализации и ликвидации инцидентов следует учитывать влияние принятых мер по сдерживанию инцидента. Организация должна иметь полное представление о потенциальном воздействии, например, изоляции операционных сетей в случае инцидента. Следует также учитывать, что присутствующее в среде вредоносное ПО может инициировать деструктивные действия, которые автоматически запустятся мерами, направленными на сдерживание инцидента». ***(FERC и NERC представили лучшие практики в области реагирования на инциденты // SecurityLab.ru (https://www.securitylab.ru/news/512309.php). 21.09.2020).***

***

«В отчете на этой неделе Microsoft заявила, что нарушила работу национальной группы угроз, которая использовала облачную инфраструктуру Azure для кибератак.

Microsoft ссылается на актера по имени Gadolinium и говорит, что он был активен около десяти лет, нацеливаясь на организации, работающие в морской индустрии и в сфере здравоохранения; совсем недавно хакеры расширили свою

деятельность на высшие учебные заведения и региональные государственные учреждения.

Злоупотребление облачными сервисами

Основываясь на обнаружении различных компонентов, обслуживающих вредоносную деятельность Gadolinium, Microsoft Threat Intelligence Center (MSTIC) идентифицировал 18 приложений Azure Active Directory, которые группа использовала для своей инфраструктуры управления и контроля.

Они были частью специальной версии инструментария для постэксплуатации PowerShell Empire, который позволял им развертывать вредоносные модули на скомпрометированном компьютере с помощью вызовов Microsoft Graph API…

Ранее в этом году, в апреле, компания удалила 18 приложений Azure Active Directory, тем самым прервав, пусть даже временно, вредоносную деятельность Gadolinium.

Атаки этой группы угроз начинаются с целевых фишинговых писем для доставки вредоносных документов (PowerPoint в 2020 году), которые обычно сбрасывают файл с двумя полезными нагрузками.

Цепочка атак продолжается с извлечением и развертыванием модифицированной версии PowerShell Empire, замаскированной под файл изображения PNG. Это позволяет злоумышленнику загрузить больше модулей на взломанный компьютер и установить бэкдор-канал.

Роль приложения Azure Active Directory заключалась в том, чтобы настроить системы-жертвы, чтобы они могли получать команды от учетной записи хранения OneDrive, управляемой злоумышленником, и передавать данные в нее.

Такая конфигурация делает особенно трудным обнаружение вредоносной активности на сетевом уровне из-за задействованных легитимных инструментов и служб, говорится в отчете Microsoft в четверг.

Хотя Microsoft не предоставляет подробных сведений о гадолинии, помимо его долговечности и целей, представляющих интерес, исследовательский институт Fraunhofer FKIE перечисляет его под другими псевдонимами от различных компаний, занимающихся кибербезопасностью: APT40, BRONZE MOHAWK, Gadolinium, Kryptonite Panda.

В прошлых отчетах FireEye группа называлась APT40, TEMP.Periscope и TEMP.Jumper, подозревая, что она является китайским субъектом кибершпионажа. В исследовании, опубликованном в марте 2018 года, компания сообщает, что фирма Proofpoint, занимающаяся кибербезопасностью, отслеживает этого актера кибершпионажа как Левиафана». ***(Ionut Ilascu. Microsoft disrupts nation-state hacker op using Azure Cloud service // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/microsoft-disrupts-nation-state-hacker-op-using-azure-cloud-service/). 25.09.2020).***

***

«Microsoft анонсировала новое руководство по безопасности, чтобы помочь специалистам по кибербезопасности быстрее обнаруживать соответствующие ошибки в своих ежемесячных бюллетенях по безопасности.

Microsoft обновила свое руководство по обновлению безопасности, которым пользуются десятки миллионов профессионалов в области кибербезопасности во второй вторник каждого месяца, также известный как вторник исправлений. Обновление, по словам Microsoft, предназначено для более интуитивного взаимодействия с пользователем.

В своем последнем обновлении, выпущенном за три недели до вторника патчей 13 октября, Microsoft может похвастаться улучшенным пользовательским интерфейсом и более современными пользовательскими интерфейсами, улучшенными возможностями фильтрации и настройки для представлений данных, а также улучшенной поддержкой нескольких языков.

Обновление призвано «помочь защитить наших клиентов, независимо от того, какие продукты или услуги Microsoft они используют в своей среде», - говорится в сообщении в блоге Microsoft Security Response Center во вторник.

Скотт Кавеза, менеджер по исследованиям в Tenable, сказал, что обновление было плюсом. «Здесь есть все старые функции, а новый пользовательский интерфейс станет более удобным и интуитивно понятным, если вы привыкнете к новому формату», - сказал он Threatpost. Он добавил, что обновленный интерфейс сократил ручные усилия, необходимые для определения того, какие исправления применимы к их системам.

«Лучшая новость заключается в том, что они понимают, что система нуждается в улучшении», - сказал Дастин Чайлдс, менеджер по связям с общественностью Zero Day Initiative. «Приятно иметь возможность выбирать столбцы для просмотра, но чего по-прежнему не хватает, так это моментального обзора рисков для конкретного выпуска. Например, во вторник патчей мой первый вопрос: сколько из этих ошибок подвергается активной атаке? Какие из них широко известны? Какие из них серьезны и требуют особого внимания? Эти данные есть, но чтобы добраться до них, нужно еще немного покопаться. Надеюсь, Microsoft продолжит улучшать процессы, которые они используют для передачи исправлений безопасности. С таким количеством патчей, которые они выпускают в этом году, у них, безусловно, будут широкие возможности для практики», - сказал Чайлдс.

На протяжении многих лет Microsoft изменяла способ предоставления обновлений безопасности для обширного каталога продуктов. Например, в 2017 году Microsoft представила новую систему с поддержкой API, которая поможет клиентам автоматизировать некоторые аспекты установки исправлений. Усилия были встречены смесью приветствий и насмешек.

Другие улучшения, перечисленные Microsoft в этом последнем обновлении, включают:

Селектор столбцов с поддержкой экспорта для создания и загрузки настраиваемых отчетов.

Несколько таблиц с представлениями данных, ориентированными на сценарий

Таблица «Уязвимости», в которой перечислены все детали CVE.

Таблица «Загрузки», содержащая информацию о пакетах для обновлений безопасности.

Таблица «Все», в которой представлены данные и параметры настройки.

До сих пор некоторые специалисты по безопасности критически относились к тому, как новое руководство по обновлению безопасности обрабатывает экспорт данных в электронные таблицы.

Но другие пользователи Twitter считают это большим улучшением.

«Прекрасная возможность группировать обновления по CVE», - сказал Кавеза. «Многие сотрудники службы безопасности ищут уязвимости в своих исправлениях, и новая вкладка «Уязвимости »действительно помогает в этом. В разделе «Развертывания» также отмечается, какие обновления требуют перезагрузки и были ли обнаружены какие-либо известные проблемы, и это важно для любого системного администратора. С новым руководством планирование и планирование развертываний может быть намного проще и более рациональным, если все эти ключевые детали будут собраны в одном месте». ***(Tom Spring. Microsoft Overhauls Patch Tuesday Security Update Guide // Threatpost (https://threatpost.com/microsoft-overhauls-security-update-guide/159449/). 22.09.2020).***

***