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 – 2019

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І.Вернадського. – К., 2019. – №9 (вересень) . – 80 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

«У Службі безпеки України розповіли, досвід яких країн використовують у процесі реформування відомства…

"Під час підготовки пропозицій та проекту з реформування Служби безпеки України було враховано досвід іноземних спецслужб країн членів ЄС і НАТО. Зокрема, Великої Британії, Французької Республіки, Королівства Швеції, Польщі, Румунії, Литовської Республіки, США та інших", - повідомили у спецслужбі.

У СБУ додали, що одним з прикладів розбудови взаємодії з іноземними партнерами у межах впровадження реформи є розбудова національної системи кібербезпеки за технічного сприяння іноземних партнерів у межах угоди "Про реалізацію Трастового фонду Україна-НАТО".

"СБУ розроблено комплексний законопроект, яким передбачено викласти Закон України "Про Службу безпеки України" у новій редакції, а також внести зміни до низки інших законів України", - підсумували в СБУ…» ***(Маріанна Присяжнюк. У СБУ збираються використати досвід країн НАТО при реформі спецслужби // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/exclusive/1823917-u-sbu-zbirayutsya-vikoristati-dosvid-krayin-nato-pri-reformi-spetssluzhbi). 12.09.2019).***

***

«У Кабінеті Міністрів шукають ІТ-фахівців. У команді потребують фахівців різних рівнів. Про це заявив міністр Кабінету міністрів України Дмитро Дубілет на своїй сторінці у Facebook.

Дубілет також надав перелік цих вакансій, а також короткий опис вимог.

Зокрема, у Кабміні шукають керівників держапідприємств або проектів. Від кандидатів вимагають управлінський досвід і досвід роботи в ІТ.

Також є вакансії для таких спеціалістів — CTO, Tech Lead та Senior Dev. Кандидати мають володіти мовами програмування - Python, Ruby, JavaScript, Java, C++ – залежно від проектів.

Ще одна вакансія — бізнес-аналітик. Як пояснив Дубілет, в Кабінеті Міністрів багато бізнес-процесів, які треба дослідити, спростити та оцифрувати. Саме цим і займатимуться майбутні працівники.

Крім того, шукають спеціалістів з бази даних, DevOps (cloud computing, CI/CD, deployment process),а також спеціалістів з кібербезпеки. Від останніх вимагають досвід роботи за міжнародними стандартами та, можливо, КСЗІ…» ***(Кабмін шукає ІТ-шників: оприлюднили перелік вакансій // Телеканал новин «24» (https://24tv.ua/techno/kabmin_shukaye_it_shnikiv_oprilyudnili_perelik_vakansiy_n1203478). 10.09.2019).***

***

«У Київській малій академії наук в рамках науково-дослідної діяльності було створено відділення безпеки і оборони в рамках якого з'явилася секція кібербезпеки…

Напрямок презентували в рамках настановної сесії, присвяченій старту нового навчального року.

Захід пройшов 18 вересня в колонній залі КМДА за підтримки департаменту освіти і науки Київміськадміністрації.

Секція була створена разом з Інститутом спецзв'язку і захисту інформації НТУУ «КПІ імені Ігоря Сікорського» за підтримки Держспецзв'язку України.

Київська МАН вперше проводила сесію об'єднаними зусиллями всіх 15 відділень і 66 секцій установчі сесії у форматі наукового променаду.

Окремими локаціями були представлені «Школа лідерства і фасилітаціонних практик», «Школа юного вченого», «Школа бізнесу Grafit», а також всі бажаючі могли відкрити для себе новий проект розвитку і реалізації ідей талановитої молоді - «ДНК нації».

В ході заходу пройшло безліч конкурсів, вікторин, майстер-класів, шоу, міні-лекцій, лайфхак, флешмобів, лотерей, міні-тренінгів, його відвідало багато гостей – проректор КПІ Наталія Семинская, завкафедрою внешкольгного освіти університету ім. Драгоманова Олена Биковська, голова общественного ради при НКАУ Едуард Кузенецов, представники КДГІ…» ***(У Київській малій академії наук з'явилася секція кібербезпеки // Українські медійні системи (https://glavcom.ua/kyiv/news/u-kijivskiy-maliy-akademiji-nauk-zyavilasya-sekciya-kiberbezpeki-627482.html). 24.09.2019).***

***

«До порушення цифрових прав включили і указ Президента, згідно якого було заблоковано 240 сайтів.

Такі результати оприлюднені у “Моніторингу порушень цифрових прав в Україні” від громадської організації “Платформа прав людини”...

Так серед порушень загального характеру опинились Укази Президента за 2017 та 2018 роки, які передбачають блокування 240 сайтів на три роки. Також згідно з ухвалою Печерського суду у серпні було закрито доступ до 17 інформаційних сайтів, серед яких популярні blogs.korrespondent.net, informator.news, ukrpress.info.

У Лабораторії цифрової безпеки також повідомили, що багато ресурсів блокується для жителів тимчасово непідконтрольних територій України.

Неприємним обмеженням виявилось блокування мережею Facebook пабліку про українську мову Mova, котрий мав близько 520 тисяч підписників.

Зафіксували аналітики і кілька кібератак. Зокрема, зловмисники зламали сервер Чорноморської ТРК та здійснили атаку на сайт видання “Гордон”. Також кіберзлочинцям вдалось зламати сайт видання “Новое время” та опублікувати там фейковий матеріал. Про блокування Instagram сторінки через діяльність інтернет-тролів повідомив і мер Києва Віталій Кличко.

До приватних атак на цифрові права у моніторингу віднесли шахрайське отримання банківських даних та продажі баз даних користувачів стороннім особам.» ***(Катерина Бенке. В серпні цього року зафіксували 20 випадків порушення цифрових прав // ІА «Погляд» (https://www.poglyad.tv/108641-2/). 20.09.2019).***

***

«Валерия Гонтарева, экс-глава Национального банка Украины, рассказала об отношениях с известным украинским журналистом,

проводившим громкие расследования о государственных чиновниках-коррупционерах, и народного депутата Украины от партии "Слуга народа" Александром Дубинским.

Гонтарева обвиняет Дубинского в кибератаке. Дело в том, что, по словам Гонтаревой, Дубинский направил тысячи писем одинакового содержания на электронную почту Лондонской школы экономики, в которой экс-глава Нацбанка преподает. Во всех письмах была одна и та же информация о том, что Гонтарева большой коррупционер и враг украинского народа. Также Гонтарева добавила, что раньше письма были подписаны Дубинским как журналистом телеканала "1+1", а теперь "этот спам" подписан заместителем главы комитета по финансам в Верховной Раде.

По мнению Гонтаревой, такое поведение народного избранника является позорным.

Известно, что представители управление Лондонской школы экономики подтвердили наличие таких писем с подобным содержанием и заявили о том, что никаких мер относительно Гонтаревой не было принято и не будет. Также в учреждении сообщили, что никто не отвечал ни на одно пришедшее письмо…» ***(Под Гонтаревой горит земля: скандальная чиновница набросилась на журналиста у всех на виду // akcenty.com.ua (https://akcenty.com.ua/politics/28553-pod-gontarevoy-gorit-zemlya-skandalnaya-chinovnica-nabrosilas-na-zhurnalista-u-vseh-na-vidu). 19.09.2019).***

***

«В стране впервые состоялся масштабный марафон по поиску багов в государственной системе. Prozorro пригласило “белых” хакеров, чтобы проверить систему закупок на уязвимость к кибератакам…

Украина стала девятой страной в мире, которая публично провела bug bounty в государственном секторе. В мире опыт проведения подобных мероприятий имеют только Великобритания, Швейцария, Сингапур, США, Нидерланды, Россия, Франция и Япония.

Больше всего с белыми хакерами сотрудничают в Америке. Собственные bug bounty программы имеют Пентагон, армия США Воздушные силы США.

В ЕС опыт проведения bug bounty в государственном секторе только зарождается. В Великобритании в прошлом году белые хакеры проверили правительственные веб-сайты. В Гааге в этом году bug bounty проведет городской совет. В Швейцарии в этом году белые хакеры проверили национальную систему электронного голосования. В Сингапуре только второй год как действует bug bounty программа.

В Украине впервые белые хакеры тестировали такую масштабную систему, как Prozorro. Призовой фонд хакерам составил $7 000 денежного вознаграждения и грант $10 000 на сертификацию в учебном центре Softprom by ERC.

Хакеров отбирали на открытом конкурсе. К участию приглашались украинцы с соответствующим опытом в кибербезопасности и баг-хантинге. Их отбирала комиссия из представителей Prozorro, bug bounty платформы HackenProof, компании OptiData и облачного провайдера De Novo.

Марафон по поиску багов проходил в закрытом режиме. Хакеры одновременно атаковали систему в течение 7 часов. Чтобы не помешать проведению торгов, киберспециалисты работали в тестовой среде. В результате белые хакеры прислали 16 уникальных отчетов. Они будут анализироваться на предмет валидности и потенциальных уязвимостей ИТ-командой. Никакой уязвимости в центральной базе данных о закупках и модуле аукционов хакеры не обнаружили.

Участие в bug bounty марафоне Prozorro приняли 12 хакеров с украинским гражданством из областей и из-за рубежа. Самому младшему участнику было всего 15 лет, но он уже имеет опыт участия в bug bounty Google, SoundCloud и еще ряда компаний.» ***(В Украине впервые состоялся марафон по поиску багов в государственной IT-системе // ООО «Файненс.юа (https://news.finance.ua/ru/news/-/457013/v-ukraine-vpervye-sostoyalsya-marafon-po-poisku-bagov-v-gosudarstvennoj-it-sisteme). 26.09.2019).***

***

Національна система кібербезпеки

«В Україні немає жодного дієвого механізму, який би насправді забезпечував планування, контроль і координацію діяльності всіх державних і недержавних установ із захисту інформаційної безпеки держави. Про це в ефірі Радіо Культура розповів військовий, політичний і державний діяч Ігор Смешко.

Ігор Смешко зазначив, що у законодавстві всіх цивілізованих країн світу існує визначене поняття "інформаційна безпека".

"У 1982 році президент США Рональд Рейган своєю таємною директивою якраз і ввів розуміння того, що інформація поряд із воєнним, економічним, дипломатичним елементами — є складовими державної сили. Інформація повинна захищатися і бути під опікою держави. В Америці Рада національної безпеки, Державний департамент, Міністерство оборони, Директор Центральної розвідки — щодня опікуються цими елементами. Посилюють свій захист інформаційної безпеки і піклуються про те, щоб точка зору про США відповідним чином в її інтересах через представництва розподілялася у світі", — розповів він.

За словами Ігоря Смешка, в Україні є тільки проголошені гасла, а не дієві механізми забезпечення інформаційної безпеки. "В нас навіть була введена доктрина інформаційної безпеки, в нас була введена стратегія кібербезпеки. Проте, як на мене, в нас є проголошені гасла, але немає жодного дієвого механізму, який би насправді забезпечував планування, контроль і координацію діяльності всіх державних і недержавних установ щодо захисту інформаційної безпеки нашої держави", — розповів він.

За його словами, в національній доктрині країни-агресора, яка вже зайняла частину нашої території і яка веде проти нас війну, немає існування України як окремого народу.

"В риториці вищого політичного керівництва держави, яка веде з нами війну, йдеться про те, що ми — фейкова держава. Де в нас є скоординована політика для

того, щоб щодня підтверджувати нашим громадянам те, що ми здатні збудувати міцну демократичну державу, яка дасть добробут, високий рівень стандартів і захист індивідуальних прав?", — ставить питання Ігор Смешко.» ***(Смешко: В Україні є тільки проголошені гасла, а не дієві механізми забезпечення інформбезпеки (відео) // Информационное агентство ЦК (http://expert.org.ua/politika/2019/smeshko-v-ukrayini-ie-tilki-progolosheni-gasla-ne-diievi-mehanizmi-zabezpechennya). 25.09.2019).***

***

Правове забезпечення кібербезпеки в Україні

«Народные депутаты пытаются законодательно закрепить устаревшую норму о подтверждении соответствия комплексной системы защиты информации государственных информационных ресурсов по результатам государственной экспертизы. Норму «пропихивают» через законопроект, не имеющий к кибербезопасности отношения и даже не проходящий рассмотрение в профильном комитете ВРУ по вопросам цифровой трансформации, – законопроект №1055-1 «Об аренде государственного и коммунального имущества».

На это обратил внимание эксперт по кибербезопасности, ведущий разработчик компании ИТ-Лаборатория Александр Галущенко…

– Пока все прогрессивные специалисты пытаются навести порядок в нашей сфере, некая группа лиц, продвигая якобы законы по аренде государственной собственности, по-тихому, отдаёт в руки государства и некого «регулятора» бразды правления, – написал Александр Галущенко.

Эксперт обратил внимание на переходные положения законопроекта Об аренде государственного и коммунального имущества». Документом, подписанным нардепами-«слугами народа» Мовчаном, Мотовиловцем и Пидласой, предлагается внести изменения в статью 8 действующего ЗУ «О защите информации в информационно-телекоммуникационных системах». Народные избранники предлагают, чтобы «государственные информресурсы или информация с ограниченным доступом, требование относительно защиты которой установлено законом, должны обрабатываться в системе с применением комплексной системы защиты информации с подтвержденной соответствием или в ЕТС, которая соответствует требованиям стандарта ISO / IEC 27001, что подтверждается сертификатом соответствия», а фразу «Подтверждение соответствия осуществляется по результатам государственной экспертизы в порядке, установленном законодательством» переписать – «Подтверждение соответствия комплексной системы защиты информации осуществляется по результатам государственной экспертизы в порядке, установленном законодательством».

Таким образом, использование СУИБ (стандарта ISO / IEC 27001) предлагается сделать возможным только для электронных торговых систем (для проведения аукциона в электронной форме) и законодательно закрепить норму о подтверждении КСЗИ путем государственной экспертизы…

К слову, нормы, которые пытаются легитимизировать через переходящие положения законопроекта «Об аренде государственного и коммунального имущества», противоречит норме другого законопроекта, также внесенного «слугами народа», правда законопроекта «профильного» – №2043 «О внесении изменений в Закон Украины "О защите информации в информационно-телекоммуникационных системах" (относительно подтверждения соответствия информационной системы требованиям по защите информации)». «Профильным» законопроектом предполагается, что «подтверждение соответствия осуществляется по результатам государственной экспертизы, которая проводится с учетом отраслевых требований и норм информационной безопасности в порядке, установленном законодательством». Третью часть статьи 8 также предлагается переписать – исключить слова «сертификат соответствия или», а слова «Подтверждение соответствия и проведение» заменить словом «Проведение». То есть, в новом законопроекте часть третья статьи 8 будет выглядеть так: «Для создания комплексной системы защиты государственных информационных ресурсов или информации с ограниченным доступом, требование по защите которой установлено законом, используются средства защиты информации, которые имеют положительное экспертное заключение по результатам государственной экспертизы в сфере технической и / или криптографической защиты информации. Проведение государственной экспертизы этих средств осуществляются в порядке, установленном законодательством»…» ***(Владимир Кондрашов. Нардепы пытаются закрепить устаревшие нормы кибербезопасности через «левый» закон // Internetua (https://internetua.com/nardepy-pytauatsya-zakrepit-ustarevshie-normy-kiberbezopasnosti-cserez-levyi-zakon). 18.09.2019).***

***

Кібервійна проти України

«ПАО «Укрпошта» оценила убыток от атаки вируса Petya в июне 2017-го года в сто миллионов гривен, а на преодоление последствий атаки у «почтовиков» ушло около трех месяцев.

Об этом говорится в замечаниях к аудиторскому отчету по результатам государственного финансового аудита акционерного общества «Укрпошта» за период с первого января 2016-го по 31 декабря 2018-го года…

Согласно документу, «кибератака с применением вируса» в июне 2017-го года привела к блокировке работы основных ИТ-систем Укрпочты и для возобновления полноценного функционирования систем потребовалось порядка трёх месяцев.

– Потеря доходов оценивается на уровне 100 миллионов гривен, – отмечается в документе.

Эта сумма составляет почти половину из 202,8 миллиона гривен убытков Укрпочты в 2017-м году.

Четвертого июля 2017-го в «Голосе Украины» появилось заявление почтового оператора о «наступлении обстоятельств непреодолимой силы». В нем ПАО «Украпошта» официально сообщала, что в результате кибератаки произошло блокирование серверов и рабочих станций национального оператора почтовой связи.

– Эти обстоятельства влияют на способность ПАО «Укрпошта» выполнять свои обязательства по заключенным договорам (договорам, контрактам), составлять и подавать отчетность в случаях, предусмотренных действующим законодательством, осуществлять надлежащее начисление и уплату налогов, сборов, выполнять другие соответствующие права и обязанности, – говорилось в заявлении.

В публикации также пообещали дополнительно сообщить о стабилизации работы Укрпочты, но соответствующее заявление нам найти так и не удалось.

В то же время в апреле 2018 года пресс-служба Укрпочты сообщала в СМИ о размере ущерба от кибератаки, оперируя теми же цифрами, но о затраченном времени на восстановление почему-то умолчала…» ***(Владимир Кондрашов. Укрпочта списала на атаку вируса Petya 100 миллионов гривен // Internetua (http://internetua.com/ukrpocsta-spisala-na-ataku-virusa-petya-100-millionov-griven). 03.09.2019).***

***

«…Злоумышленники из киберпреступной группировки Electrum вызвавшие перебои в подаче электроэнергии на Украине в 2016 году, возможно, надеялись нанести гораздо больший ущерб. К такому мнению пришли исследователи из ИБ-компании Dragos.

Преступники использовали вредоносное ПО под названием Crashoverride (Industroyer) для атаки на промышленные системы управления (ICS) на электростанциях на Украине. 18 декабря 2016 года в результате кибератаки произошел сбой в автоматике управления, который нарушил энергоподачу в северную часть правобережья Киева и прилегающие районы Киевской области. Подачу энергии возобновили примерно через час после инцидента.

По словам специалиста Джо Словик (Joe Slowik), злоумышленники могли вызвать более масштабные отключения и нанести огромный ущерб, если бы не ошибки в коде вредоноса. Вредоносное ПО содержало модуль, предназначенный для того, чтобы злоумышленники могли контролировать автоматические выключатели и прерывать подачу электроэнергии, манипулируя устройствами связи с объектом. Также внутри был модуль, который удалял конфигурации и другие файлы, затрудняя восстановление системы.

В ходе анализа исследователи также обнаружили инструмент, эксплуатирующий уязвимость (CVE-2015-5374) в защитных реле Siemens SIPROTEC для вызова отказа в обслуживании системы. Инструмент должен был отключить реле, которое обеспечивает защиту от перегрузки после восстановления питания. Это могло привести к скачкам напряжения в передающем оборудовании, нанести физические повреждения и отключить системы как минимум на несколько месяцев. В данном случае бы понадобился ремонт и замена устройств.

Однако злоумышленникам не удалось отключить защитные реле из-за некоторых ошибок в коде инструмента. Более того, хакеры попытались нарушить работу сотен систем управления в целевой организации, но не смогли скомпрометировать столько, сколько планировали. В результате атака получилась намного слабее, чем они ожидали.

Даже если бы DoS-атаки на реле SIPROTEC были бы успешными, неясно, смогла бы Electrum достичь своей предполагаемой цели — причинить физический ущерб. Промышленные среды могут иметь различные системы и механизмы защиты, которые смягчили бы атаку, полагает Словик.» ***(Ущерб от атаки на киевскую электростанцию в 2016 году мог быть намного больше // SecurityLab.ru (https://www.securitylab.ru/news/501101.php). 13.09.2019).***

***

Боротьба з кіберзлочинністю в Україні

«Гражданин Украины получил три года лишения свободы с испытательным сроком в один годи и с лишением права заниматься деятельностью, связанной с использованием электронно - вычислительных машин (компьютеров), систем и компьютерных сетей сроком на один год. Мужчина получил доступ к почте и, в результате, к странице на Facebook потерпевшей…

Согласно материалам дела, ранее несудимый уроженец Киева в июле 2018-го убедил службу поддержки почтового сервиса bigmir.net, что забыли пароль к почтовому ящику и назвал предварительные известные ему авторизационные данные потерпевшей. Получив новый пароль к электронному почтовому ящику потерпевшей, мужчина незаконно изменил пароль доступа к нему, прочел переписку и собрал с электронного почтового ящика конфиденциальную информацию о девушке – скан-копии загранпаспорта и ИНН. После этого, в этот же день, злоумышленник обратился в службу поддержки Facebook от имени потерпевшей, подтвердив свою «личность» полученными документами, и получил новый код доступа к ее странице и изменил авторизационные данные аккаунта. В дальнейшем мужчина дважды (восьмого и десятого апреля 2019-го) блокировал доступ потерпевшей к её странице, изменяя данные для авторизации.

Действия обвиняемого были классифицированы как несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), компьютерных сетей, что привело к блокированию, потере и утечке информации (уголовное преступление, предусмотренное ч. 1 ст.361 УК Украины), эти же действия совершенные повторно (ч.2 ст.361 УК Украины), нарушение тайны переписки, передаваемой через компьютер (уголовное преступление, предусмотренное ч.1 ст.163 УК Украины) и незаконный сбор, хранение, использование и распространение конфиденциальной информации о лице (ч.1 ст.182 УК Украины).

Обвиняемый в судебном заседании вину в совершении инкриминируемых преступлений признал полностью, искренне раскаялся, дал показания об

обстоятельствах их совершения аналогичные изложенным в предъявленном обвинении и объяснил, что подобного в будущем не повторится.

Потерпевшая подала в суд заявление, в котором указала, что претензий материального и морального характера у нее отсутствуют, просила судебное разбирательство провести без ее участия, наказание обвиняемому назначить на усмотрение суда.

В итоге суд назначил мужчине наказание путем поглощения менее строгого наказания более строгим, в 3 года лишения свободы с лишением права заниматься деятельностью, связанной с использованием электронно-вычислительных машин (компьютеров), систем и компьютерных сетей сроком на 1 год. Также на основании ст.75 УК Украины суд освободил обвиняемого от отбывания наказания в виде 3 лет лишения свободы с установлением испытательного срока продолжительностью 1 год.» ***(Владимир Кондрашов. Украинцу дали три года за взлом почты и страницы в Facebook // Internetua (http://internetua.com/ukraincu-dali-tri-goda-za-vzlom-pocsty-i-stranicy-v-facebook). 19.09.2019).***

***

«Учасники злочинного угрупування, інфікуючи вірусами комп'ютери нотаріусів та державних службовців, незаконно втручалися в роботу державних реєстрів та переоформлювали права власності на нерухомість на користь третіх осіб…

Працівники Департаменту кіберполіції спільно зі слідчими Головного слідчого управління Національної поліції України та Службою безпеки України, за процесуального керівництва Генеральної прокуратури України, припинили діяльність злочинної організації.

Кіберполіція встановила: зловмисники розсилали на електронні адреси посадових осіб, які мали доступ до державних реєстрів, листи, що містили вкладений файл із шкідливим програмним забезпеченням (вірусом). Під час активації файлу вірус інфікував комп'ютер та надавав зловмисникам доступ до електронного цифрового ключа та пароля користувача. При цьому, усі листи маскувалися: їх було надіслано нібито від імені державних установ або використовуючи реальні електронні пошти інфікованих раніше комп'ютерів.

Маючи доступ до Державного реєстру прав власності на нерухоме майно та Державного реєстру обтяжень рухомого майна, зловмисники вносили завідомо підроблені відомості щодо скасування заборон відчуження рухомого та нерухомого майна в інтересах інших осіб. В подальшому власність продавалася. Таким чином їм вдалося реалізувати більше тисячі об'єктів рухомого та нерухомого майна.

Для конспірації своїх дій, зловмисники проводили усі протиправні дії в лісосмузі, неподалік міста Києва. У лісі вони мали схованку, де зберігалися ноутбук і мобільний телефон, який використовували для забезпечення доступу до мережі інтернет. Водночас, щоразу вони використовували різні сім-картки, які знищувалися після одноразового використання.

Правоохоронці встановили, що таку злочинну схему організував колишній працівник Державної виконавчої служби. Група працювала протягом останніх чотирьох років. До її складу входили ще п'ятеро громадян України, віком від 34 до 40 років. При цьому четверо з них також були колишніми співробітниками

територіальних підрозділів Державної виконавчої служби. До діяльності групи вони залучили фахівця у галузі комп’ютерного програмування, який і був розробником шкідливого програмного засобу.

За участі спецпризначенців КОРД, правоохоронці провели одночасно більше 40 санкціонованих обшуків на території декількох областей України. За їх результатами було вилучено автомобілі, комп’ютерну техніку, документи, чорнові записи, зброю, вибухівку та гроші.

Дії учасників злочинної організації кваліфіковано за декількома статтями Кримінального кодексу України: ч. 1 ст. 255 (Створення злочинної організації), ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку), ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут), ст. 209 (Легалізація (відмивання) доходів, одержаних злочинним шляхом) КК України.

Усім учасникам злочинної організації оголошено про підозру. Двох із них затримано в порядку ст. 208 КПК України. До суду направлено клопотання про застосування запобіжних заходів у вигляді тримання під вартою. Учасникам групи загрожує до 12 років ув’язнення.» ***(Кіберполіція затримала організаторів масштабної схеми перереєстрації арештованого майна // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-zatrymala-organizatoriv-masshtabnoyi-sxemy-perereyestracziyi-areshtovanogo-majna-45/). 26.09.2019).***

***

«18-річний мешканець Івано-Франківської області поширював шкідливе програмне забезпечення для віддаленого керування ураженим комп’ютером. Відтак, він отримував повний доступ до комп’ютера, включаючи конфіденційну інформацію користувача, логіни та паролі до усіх його облікових записів, а також онлайн банкінгу. За даним фактом розпочато кримінальне провадження.

Працівники Карпатського управління кіберполіції встановили, що вірус молодик купив у DarkNet. Модифікувавши його, хлопець поширював шкідливе програмне забезпечення серед друзів, знайомих, а також розмістив на відкритих джерелах для завантаження усіма бажаючими. При цьому зловмисник маскував файл як веб-браузер, а також як файл для оновлення комп’ютерних ігор…

Слідчі поліції Івано-Франківської області, за процесуального керівництва прокуратури Івано-Франківської області, розпочали досудове розслідування за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України. Вилучену техніку направлено на експертизу. Поліція встановлює усіх громадян, які стали жертвами молодика. Наразі йому загрожує до шести років ув’язнення…» ***(Кіберполіція викрила хакера у поширенні вірусів, замаскованих під оновлення комп’ютерних ігор // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-xakera-u-poshyrenni-virusiv-zamaskovanyx-pid-onovlennya-kompyuternyx-igor-3157/). 23.09.2019).***

***

«Группа ООН по кибербезопасности соберется в феврале 2020 года для обсуждения доклада по угрозам в этой сфере.

Мир может оказаться на пороге глобальной кибервойны, если правительства стран не найдут способ совместной борьбы с киберугрозами. Об этом заявил спецпредставитель президента РФ по вопросам международного сотрудничества в сфере информационной безопасности Андрей Крутских на пленарном заседании рабочей группы ООН по международной информационной безопасности.

По словам политолога, мир вскоре окажется на пороге глобальной кибервойны, если правительства стран не научатся совместно бороться с киберугрозами. Как сообщил спецпредставитель президента РФ, Россия открыта для диалога со всеми странами и государствами, и необходимо выстраивать совместную работу самым эффективным образом.

«Ситуация в этой сфере стремительно деградирует. Если отбросить пропагандистскую шелуху, то станет очевидным, что киберконфронтация только нарастает и, если мы общими усилиями не найдем действенные способы борьбы с этими угрозами, то, скажу прямо, до глобальной кибервойны будет рукой подать», — приводит информационное агенство ТАСС слова Крутских.

По словам политолога, группа ООН по кибербезопасности соберется в феврале 2020 года для обсуждения доклада по угрозам в этой сфере.» ***(Отсутствие методов совместной борьбы с киберугрозами может привести к глобальной кибервойне // SecurityLab.ru (https://www.securitylab.ru/news/500922.php). 10.08.2019).***

***

«…Microsoft и Hewlett Foundation готовятся к созданию некоммерческой организации, которая будет раскрывать подробности об опасных кибератаках и оказывать помощь пострадавшим. По данным CyberScoop, организация Cyber Peace Institute начнет работу уже в ближайшие несколько недель.

Специалисты Cyber Peace Institute будут проводить расследования и предоставлять аналитическую информацию о масштабных кибератаках на гражданские цели, оценивать расходы и снабжать инструментами безопасности как отдельных лиц, так и целые компании. Об этом сообщается в описании Cyber Peace Institute, обнародованном на конференции B-Sides в Лас-Вегасе в нынешнем году.

Помимо Microsoft и Hewlett Foundation, в организацию также войдут Facebook, Mastercard и Ford Foundation. Однако Cyber Peace Institute не будет зависеть ни от одной компании, занимающейся его финансированием.

По словам источника CyberScoop, Hewlett Foundation выделил институту $5 млн на пять последующих лет, а компания Facebook пообещала $250 тыс. Какую сумму готовы предоставить Microsoft и Mastercard, источнику неизвестно, однако они также намерены участвовать в финансировании организации…» ***(Microsoft и Hewlett Foundation создадут организацию для помощи жертвам кибератак // SecurityLab.ru (https://www.securitylab.ru/news/500911.php). 10.08.2019).***

***

«За последние два года руководители компаний стали больше опасаться кибератак.

В нынешнее время угроза кибератак стала самой большой опасностью для бизнес-компаний. Согласно исследованию, проведенному страховым консалтинговым агентством Marsh и компанией Microsoft, руководители предприятий больше опасаются киберугроз, чем экономической неопределенности, ущерба бренду или правового регулирования.

Опрос более 1,5 тыс. директоров продемонстрировал быстрое изменение предполагаемых рисков для их организаций. По результатам опроса, наличие полиса киберстрахования в текущем году стало более распространенным явлением, чем в 2017 году. В 2017 году 62% респондентов считали кибератаки одной из 5 самых опасных угроз, а в текущем году данный показатель вырос до 79%. Доля респондентов, которые считают кибератаки угрозой номер один, также выросла с 6% до 22% за два года.

По данным страховой компании AIG, самой распространенной и затратной киберугрозой являются BEC–атаки (business email compromise – компрометация деловой почты). Связанные с BEC-атаками страховые иски составляют 23% от всех обращений в регионе EMEA (Europe, the Middle East and Africa). Следующими в списке следует вымогательское ПО.

Согласно исследованию Marsh и Microsoft, за последние два года количество организаций с киберстраховкой выросло с 34% до 47%. 89% респондентов уверены, что их полис киберстрахования способен покрыть ущерб от кибератаки.» ***(22% директоров считают кибератаки угрозой номер один для бизнеса // SecurityLab.ru (https://www.securitylab.ru/news/501281.php). 20.09.2019).***

***

«По оценке специалистов Accenture, рынок сервисов кибербезопасности растет темпами, аналогичными рынкам Digital и ИТ. Компания прогнозирует, что к 2021 г. объем мирового рынка ИБ увеличится на 66% и составит 202 млрд. долл. При этом совокупный мировой ущерб от кибератак может вырасти на 39% до 2,1 млрд. долл.

Основные тренды в области кибербезопасности бизнеса в 2019 г., по данным Accenture, следующие. Первый тренд связан с дезинформацией. Авторы отчета отмечают, что вслед за политической дезинформацией, цель которой – повлиять на общественное мнение, все активнее набирает обороты экономическая дезинформация. Финансовая сфера, и, в частности, высокочастотные торговые алгоритмы, основанные на быстрых текстовых источниках информации, в будущем будут подвергаться широкомасштабным атакам.

Развитие методов машинного обучения, искусственного интеллекта (ИИ) и внедрение сетей связи на базе технологии 5G даст новые возможности для производства и распространения дезинформации.

Одним из примеров применения ИИ является создание высококачественных поддельных изображений или видео, которые можно использовать для дискредитации и шантажа политического оппонента, конкурирующей компании или создания массовой паники.

В свою очередь технология 5G также создает серьезные риски – контроль над оборудованием и ПО инфраструктуры 5G может позволить небольшой группе компаний или злоумышленников проводить информационные операции, подделывая или распространяя дезинформацию для больших групп пользователей 5G.

Второй тренд – объединение киберпреступников в синдикаты и совместное использование продвинутых инструментов, автоматизирующих процесс массового производства и распространения вредоносного ПО, спама и приложений для рассылки вредоносных программ с использованием современных технологий, таких как облака, big data, ИИ. С синдикатами, работающими вместе, границы между группами – источниками угроз становятся еще более размытыми, что дополнительно усложняет идентификацию киберпреступного агента.

Помимо заражения вирусами-шифровальщиками (программы вымогатели) с помощью организации крупномасштабных спам-кампаний, злоумышленники все чаще внедряют их непосредственно в сети организаций, приобретая удаленный доступ к скомпрометированным серверам в подпольных хакерских сообществах и маркетплейсах вредоносного ПО. Это значит, что киберпреступники будут продолжать менять свою тактику, чтобы уменьшить риски обнаружения и неудач.

Применение методов машинного обучения и ИИ в фишинговых атаках позволит киберпреступникам увеличивать их эффективность и приведет к еще более массовому распространению вирусов-шифровальщиков, которые могут стать главным орудием в кибервойнах.

Еще один тренд связан с уязвимостью экосистем. Этот бизнес зависит от взаимосвязанности элементов системы, а связи увеличивают подверженность компаний риску. Появляющиеся в цепочках угрозы превращают друзей, партнеров и клиентов компании в источник опасности.

По мнению авторов исследования, компании должны смотреть на вопрос кибербезопасности комплексно и учитывать слабые стороны и уязвимости партнеров и третьих лиц в своих киберстратегиях. Они должны научиться создавать центры безопасности, адаптируя применяющиеся подходы к последним требованиям.» ***(Киберпреступники также совершенствуют методики за счет машинного обучения и ИИ // Компьютерное Обозрение (https://ko.com.ua/kiberprestupniki_takzhe_sovershenstvuyut_metodiki_za_schet_mashinnogo_obucheniya_i_ii_130242). 23.09.2019).***

***

«Компания Alert Logic опубликовала отчет о киберрисках в сфере малого и среднего бизнеса, основанный на изучении данных о 8,2 млн ИБ-инцидентов, случившихся у более чем 4 тыс. ее клиентов. По мнению аналитиков, ключевой проблемой небольших организаций являются слабое шифрование и использование устаревших версий программного обеспечения. При этом риски, связанные с безопасностью компьютерной инфраструктуры, можно значительно снизить, защитив лишь три порта, на которые приходится две трети всех кибератак.

Причина большинства проблем — слабое шифрование

Как выяснили эксперты, 42% выявленных инцидентов произошли из-за неправильных настроек, связанных с шифрованием. По мнению исследователей, использование облачных сервисов, таких как AWS, требует особого внимания к защите трафика, однако 33% проверенных аккаунтов применяют ненадежные криптографические методы или вовсе не кодируют информацию. Кроме того, 14% небольших организаций имеют проблемы с настройкой корзин S3.

Анализ ошибок конфигурации серверов и рабочих станций показал,что две трети из них связаны с использованием слабых алгоритмов шифрования. Эксперты отметили, что MD5 уже не считается достаточно безопасным методом криптографии, а SHA-0 и SHA-1 легко взламываются с использованием современных вычислительных мощностей. Для надежной защиты данных специалисты рекомендуют применять SHA-256 и AES…

Согласно отчету, 66% проверенных Windows-систем используют устаревшие версии ОС либо те, которые будут сняты с поддержки в январе 2020 года. Ситуация с серверами под управлением Linux не менее тревожная: около 50% из них работают на сборках со старым ядром, для которых не выпускаются обновления безопасности. Кроме того, более 30% почтовых серверов малых организаций уже не поддерживаются производителями.

Исследование также показало, что SMB-компании, использующие актуальные версии системного ПО, зачастую пренебрегают установкой важных патчей. Из 20 уязвимостей, наиболее часто встречающихся на серверах и рабочих станциях в малом бизнесе, 75% исправлены производителем год и более назад…

Как выяснили ИБ-специалисты, 65% нападений на компьютерные системы небольших организаций ведется через TCP-порты 22 (SSH), 443 (HTTPS) и 80 (HTTP). Защитив их файрволом и регулярно проверяя журнал входящих запросов, можно избежать большей части атак, угрожающих предприятиям малого и среднего бизнеса. Дополнительно исследователи рекомендуют обратить внимание на RDP-порт, используемый эксплойтом BlueKeep, а также FTP-порты, с которыми часто работают IP-камеры, принтеры и другие IoT-устройства.» ***(Maxim Zaitsev. Малый бизнес забывает обновлять критически важное ПО // Threatpost (https://threatpost.ru/alert-logic-names-main-cyber-threats-to-smb/34131/). 18.09.2019).***

***

Сполучені Штати Америки

«Лидер меньшинства в Сенате США Чак Шумер призвал правительство усилить борьбу с кибератаками на школьные округа.

Инициатива связана со случаем, когда хакеры вынудили школьный округ Роквилл-центр (штат Мэрилнд, США) в июле заплатить им почти 90 000 долларов в обмен на восстановление работы компьютерной системы учебного заведения.

Шумер собрал в понедельник, 22 сентября, пресс-конференцию, на которой заявил, что такие атаки парализуют деятельность местного самоуправления и что

несмотря на все большее их распространение, школьные власти не имеют ресурсов для борьбы с этим явлением.

Новый законопроект Шумера предусматривает создание внутри Министерства внутренней безопасности США специальных групп, которые будут помогать местным органам власти готовиться к таким атакам и реагировать на них.

Также к рассмотрению аналогичных дел Шумер, имеющий еврейские корни, предложил привлекать ФБР, причем расследование кибератак должно производиться в приоритетном порядке…» ***(Сенатор Шумер представил проект защиты школ от кибератак // Jewishnews (https://jewishnews.com.ua/politics/senator-shumer-predstavil-proekt-zashhityi-shkol-ot-kiberatak). 25.09.2019).***

***

Країни ЄС

«У четвер, 12 вересня, уряд Естонії прийняв рішення про створення в МЗС відділу кібернетичної дипломатії…

"Кібербезпека і безпека стають все більш важливими пріоритетами у зовнішній політиці багатьох країн, і наші союзники бачать Естонію лідером в цій області", - заявив Рейнсалу.

За його словами, новий відділ очолить Хелі Тійрмаа-Клаар - дипломатичний представник, що володіє особливими повноваженнями в галузі кібербезпеки.

Новий відділ почне роботу вже цієї осені.

Кібернетична дипломатія фокусується на поведінці держав у кіберпросторі та дотриманні кіберстандартів.» ***(В МЗС Естонії створять відділ кібердипломатії // Європейська правда (https://www.eurointegration.com.ua/news/2019/09/12/7100662/). 12.09.2019).***

***

«…Федеральное министерство внутренних дел (Bundesministerium des Innern, BMI) Германии в официальном заявлении сообщило о планах сократить зависимость от конкретных IT-поставщиков, особенно Microsoft, в целях укрепления своего «цифрового суверенитета».

«Для обеспечения нашего цифрового суверенитета мы хотим уменьшить зависимость от отдельных IT-поставщиков. Мы также рассматриваем альтернативные программы для замены определенного программного обеспечения. Это будет сделано в тесной координации с другими странами ЕС», — сообщил министр внутренних дел Германии Хорст Зеехофер (Horst Seehofer).

BMI заказало стратегический анализ рынка у транснациональной компании PricewaterhouseCoopers (PwC), и в августе нынешнего года был опубликован документ, в котором рассматриваются риски, присущие IT-зависимости от поставщиков коммерческого программного обеспечения. Особый акцент был поставлен на Microsoft из-за интенсивного использования ее продуктов и их взаимосвязи, особенно Microsoft Office, Windows, Windows Server и Office 365.

В анализе специалисты выделили несколько «болевых точек». Первая касается безопасности данных, поскольку телеметрия передает данные в Microsoft, и пользователь не может контролировать этот процесс. Информация может содержать личные данные и тем самым нарушать генеральный регламент о защите персональных данных (GDPR). Зависимость от облачных сервисов также повышает риск перебоев или удаленной деактивации лицензий на программное обеспечение, полагают специалисты. Использование облачных сервисов может снизить внутреннюю компетентность в области IT, поскольку потребность в поддержке локального программного обеспечения снижается и, следовательно, возникает угроза способности федеральной администрации вводить новшества.

В качестве одного из примеров решения проблем в отчете упоминается министерство юстиции Нидерландов, которое пришло к соглашению с Microsoft в вопросе сбора данных телеметрии. Другой способ заключается в использовании более разнообразного проприетарного программного обеспечения, такого как Google G Suite вместо Microsoft Office или Apple-устройств вместо ПК на базе Windows. Третий подход заключается в создании и использовании открытого программного обеспечения. В отчете упоминается несколько примеров, в том числе неудачная попытка Мюнхена заменить Windows и Office на Linux и OpenOffice, которая впоследствии была отменена, и более успешные усилия французской полиции по использованию Linux, LibreOffice и других приложений с открытым исходным кодом.» ***(МВД Германии хочет сократить зависимость от Microsoft // SecurityLab.ru (https://www.securitylab.ru/news/501282.php). 20.09.2019).***

***

«Уряд Литви відмовився від ідеї введення онлайн-голосування на виборах через зростаючі загрози кібератак і втручання Росії у вибори інших країн…

У середу уряд вирішив відмовитися від ідеї розробки системи онлайн-голосування та внесення поправок до законів про вибори, щоб впровадити електронне голосування.

У 2018 році кабінет міністрів Литви схвалив законопроєкт про створення системи онлайн-голосування та направив його на розгляд до парламенту.

Прихильники законопроєкту вважали, що онлайн-голосування допоможе збільшити явку виборців.

Міністр юстиції Ельвінас Янкявічюс повідомив у вівторок, що, за домовленістю, яка була досягнута, Сейм не ухвалюватиме законопроєкт…» ***(Литва відмовилась від ідеї онлайн-голосування через загрозу Росії // Є новина (https://www.ednist.info/news/93491). 27.09.2019).***

***

Китай

«…Китайскую компанию Huawei, находящуюся под давлением со стороны правительства США в связи с предполагаемыми проблемами информационной безопасности, временно лишили членства в организации

Forum of Incident Response and Security Teams (FIRST), ответственной за обеспечение межотраслевой информационной безопасности. Компании официально заблокируют доступ к общей информации о новых угрозах для платформ и защитных решений, сообщает издание The Wall Street Journal.

FIRST является некоммерческой организацией, которая дает возможность специалистам более эффективно реагировать на инциденты в области безопасности, предоставляя доступ к передовым методикам, инструментам и доверенному общению между членами группы. FIRST также объединяет представителей отрасли с государственными учреждениями, включая экспертов из Министерства внутренней безопасности США и Центра правительственной связи США (GCHQ).

Отстранение Huawei теоретически замедлит способность компании решать или исправлять проблемы безопасности в своих продуктах. Huawei также потеряет доступ к обмену информацией в специальных группах по интересам, данным об уязвимостях и «автоматизированной платформе для обмена информацией о вредоносных программах».

По словам представителя FIRST, данная мера была принята «после обширных консультаций и аудитов», а организация «сожалеет о том, что оказалась в положении, когда пришлось приостановить членство Huawei»…» ***(Huawei закрыли доступ к информации о киберугрозах // SecurityLab.ru (https://www.securitylab.ru/news/501260.php). 19.09.2019).***

***

«Найближчим часом для компаній КНР запровадять систему соціального рейтингу, також як і для громадян. Тепер як локальні, так і іноземні компанії будуть слідувати строгому список з 300 вимог або, в іншому випадку, потрапити в чорний список, повідомляє Wired.

Корпоративний соціальний рейтинг "може стати смертельним вироком" для іноземних компаній у КНР, каже Йорг Ваттке, президент Торгової палати Європейського союзу в Китаї.

За його словами, компаніям доведеться мати справу з 30 різними рейтингами та класифікаціями у відповідності з результатами їх відповідності в таких секторах, як захист навколишнього середовища, податковий контроль і контроль якості, які будуть взяті із звітів, заснованих приблизно на 300 вимогах. Ці рейтинги, будуть охоплювати такі галузі, як податки, митна аутентифікація, захист навколишнього середовища, якість продукції, безпека праці, е-комерція і кібербезпека.

У звіті говориться, що "вимоги та рейтингові механізми значною мірою чітко визначені і можуть бути оцінені за допомогою детального аналізу", погана новина для компаній полягає в тому, що стандарт того, що являє собою "детальний аналіз", є досить високим. База офіційних документів "включає в себе кілька сотень документів, опублікованих тільки на національному рівні, і ще близько 1500 при включенні всіх відповідних документів на рівні провінцій і міст".

Очевидно, що якщо компанія захоче вести бізнес в Китаї, їй доведеться зіткнутися з новими для себе проблемами.

Китайська влада заговорила про введення соціальних рейтингів для населення ще в 2014 році. Згідно з ним, кожна людина в КНР отримає свою

"оцінку" до 2020 року… ***(Не тільки для людей: У Китаї збираються ввести систему соціального рейтингу // Дзеркало тижня. Україна» (https://dt.ua/WORLD/ne-tilki-dlya-lyudey-u-kitayi-zbirayutsya-vvesti-sistemu-socialnogo-reytingu-324445_.html). 24.09.2019).***

***

Російська Федерація та країни ЄАЕС

«Как сообщает CNews, межведомственная комиссия при Совете безопасности приняла решение об увеличении финансирования органов власти регионов по реализации требований закона «О безопасности критической информационной инфраструктуры» (№187-ФЗ). Это следует из материалов федерального проекта «Информационная инфраструктура» национальной программы «Цифровая экономика».

Первоначально сумма затрат по данному мероприятию составляла 250 млн руб. Но Совбез решил увеличить ее в 20 раз до 5 млрд руб. В том числе в 2019 г. должен быть выделен 1 млрд руб., в 2020 и 2021 гг. – по 2 млрд руб. Распоряжаться средствами будет Минцифры.

Федеральный проект «Информационная безопасность» содержит еще ряд мероприятий, связанных с ГосСОПКА. Планируется провести исследование по оценке уязвимости веб-приложений, размещенных в российском сегменте интернета.

Затем следует разработать предложения по функциональности, архитектуре, формату взаимодействия и регламентам обмена данными и функционирования отечественного ресурса и функционирования отечественного ресурса проверки угроз уровня веб-приложений. Соответствующие предложения должны быть согласованы с головным подразделением ГосСОПКА и Базой данных угроз ФСТЭК. После этого будет разработан отечественный ресурс информирования и проверки угроз уровня веб-приложений.

Также запланировано создание корпоративных центров ГосСОПКА, обеспечивающих оказание услуг в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты для физических лиц, индивидуальных предпринимателей и малого бизнеса. В том числе услуги будут оказываться лицам, не относящимся к субъектам КИИ.

Кроме того, запланировано создание стандартизированных, сертифицированных по требованиям информационной безопасности решений для типовых объектов КИИ, а также создание номенклатуры стандартизированных, сертифицированных по требованиям информационной безопасности решений для типовых объектов КИИ.

Кураторами соответствующих мероприятий станут Минцифры, ФСБ, ФСТЭК, ФСО, Минэнерго и Банк России. В число исполнителей войдут «Концерн «Автоматика» («дочка» госкорпорации «Ростех»), Сбербанк и его «дочка», занимающаяся информационной безопасностью – «Бизон».» ***(Система защиты***

от кибератак под кураторством ФСБ подорожает в 20 раз // РосКомСвобода (https://roskomsvoboda.org/49395/). 05.09.2019).

***

«Министерство цифрового развития, связи и массовых коммуникаций РФ совместно с компанией «Ростелеком» создадут специальный киберполигон, где IT-специалисты смогут обучаться современным практикам обеспечения информационной безопасности. Соответствующее соглашение было подписано в четверг, 5 сентября, на Восточном экономическом форуме во Владивостоке.

Главное предназначение киберполигона – моделирование развития киберугроз и тестирование безопасности ПО. Киберполигон будет использоваться для проведения учений и тренировок, в ходе которых IT-специалисты смогут отрабатывать ответные действия на случай кибератак.

На киберполигоне также планируется проведение ежегодных федеральных соревнований по ИБ и создание центра тестирования безопасности ПО для участников научно-технологического центра на острове Русский, организаций Дальневосточного федерального округа и ДВФУ.

«Основная инфраструктура Киберполигона будет создаваться на базе "Ростелекома" с привлечением экспертизы сотрудников его дочерней компании "Ростелеком-Солар", национального провайдера технологий кибербезопасности», - сообщили SecurityLab в компании «Ростелеком». ***(В России появится киберполигон // SecurityLab.ru (https://www.securitylab.ru/news/500837.php). 05.09.2019).***

***

«Россия возглавила рейтинг стран с наибольшим числом вредоносных программ для платформы Android, составленный антивирусной компанией Eset. В десятку также входят Иран, Украина, Индонезия, Индия, Мексика, Чехия, Турция, США и Перу.

Одной из наиболее актуальных угроз является банковское вредоносное ПО для Android. Другая опасность — мобильные вымогатели, такие как Android / Filecoder.C. Наибольший рост за последний год показали майнеры криптовалют, например, Android / Coinminer. Эксперты обнаружили на 72% вирусов больше, чем год назад.

В Eset отметили, что большинство Android-смартфонов используют устаревшие версии ОС: актуальная Android Pie установлена у 10,4% пользователей, а на новейшей Android 10 работают всего 0,1% смартфонов. Это подвергает остальных 89,5% Android-пользователей повышенному риску со стороны мобильных угроз, заключили аналитики.» ***(Eset: Россия на первом месте по числу вредоносного ПО для Android // Открытые системы (https://www.computerworld.ru/news/Eset-Rossiya-na-pervom-meste-po-chislu-vredonosnogo-PO-dlya-Android). 25.09.2019).***

***

«Россия вызывает наибольшие опасения у США в киберпространстве. Об этом на конференции по разведке и национальной безопасности сообщил главный юридический советник Агентства национальной безопасности при Пентагоне Гленн Герстелл…

По его словам, всего есть четыре государства, которым Вашингтон уделяет «особое внимание». Среди них «Россия — однозначно номер один» из-за «больших возможностей создания проблем, особенно в части распространения неверной информации и дезинформации», заявил Герстелл.

На втором месте, по оценке американских властей, стоит Китай, который якобы нацелен на кражу интеллектуальной собственности и информации. На третьем — Северная Корея, «специализирующаяся» на финансовых преступлениях, особенно с использованием уязвимостей криптовалют. Наконец, четвертую позицию занимает Иран, который, по словам сотрудника АНБ, концентрируется на атаках на инфраструктуру, банковскую систему США.

Герстелл считает, что угроза в киберпространстве остается угрозой номер один последние 6-8 лет, и ситуация постоянно ухудшается с развитием технологий и стремительным ростом числа уязвимых устройств и приложений…» ***(Жанна Звягина. В Пентагоне назвали Россию главной угрозой в киберпространстве // Парламентская газета (https://www.pnp.ru/politics/pentagon-nazval-rossiyu-glavnoy-ugrozoy-v-kiberprostranstve.html). 05.09.2019).***

***

«…Австралийской разведке удалось установить, что за кибератаками на парламент страны и три крупнейшие политические партии в преддверии майских выборов стоит Китай…

По словам источников, в марте нынешнего года австралийское разведывательное управление Australian Signals Directorate установило, что вышеупомянутые кибератаки были осуществлены Министерством государственной безопасности КНР. Австралийские власти подготовили соответствующий отчет, включающий сведения, добытые Министерством иностранных дел Австралии, однако они намерены держать его в тайне во избежание ухудшения торгово-экономических отношений между двумя государствами.

Австралийское правительство не выдвигало никаких обвинений в сторону Китая… В свою очередь, Министерство иностранных дел КНР опровергает любые обвинения в киберпреступной деятельности, отмечая, что интернет кишит всевозможными теориями, которые невозможно доказать…» ***(За атаками на парламент Австралии стоит Китай // SecurityLab.ru (https://www.securitylab.ru/news/501110.php). 16.09.2019).***

***

«Путін допоміг нам зрозуміти, чому ми маємо модернізуватися - начальник штабу оборони Британії…

Як зауважив начальник штабу оборони Великобританії генерал Нік Картер, різниці між миром та війною більше не існує.

Генерал Картер зазначив, що традиційна концепція війни тільки на суші, на морі та в повітрі застаріла.

«Майбутня війна в основному орієнтована на інформацію. Вона буде більш складнішою і буде захоплювати нові області, зокрема, космосу та кібер», - підкреслив голова військового відомства Британії…

«Росія сьогодні становить більшу загрозу, ніж п'ять років тому», - наголосив він.

Генерал також окреслив складність надійного військового стримування, такого як наразі в Прибалтиці, і водночас перетворення збройних сил в майбутнє поле битви, де, ймовірно, буде домінувати кібервійна…» ***(У Британії заявили, що країна «перебуває у стані холодної війни» через російські кібератаки // Українські медійні системи (https://glavcom.ua/world/observe/u-britaniji-zayavili-shcho-krajina-perebuvaje-u-stani-holodnoji-viyni-cherez-rosiyski-kiberataki-628877.html). 30.09.2019).***

***

«Кибератаки США против ядерных объектов Ирана могли привести к миллионным жертвам. Об этом в интервью NBC заявил глава МИД Ирана Джавад Зариф…

При этом Зариф упомянул вирус StuxNet, примененный против Ирана.

По его словам, Иран втянут в "кибервойну", однако "любую войну, которую развязали США, они же не смогут закончить"…» ***(Глава МИД Ирана обвинил США в развязывании кибервойны // Информационное Агентство 112.ua (https://112.ua/mir/glava-mid-irana-obvinil-ssha-v-razvyazyvanii-kibervoyny-509207.html). 20.09.2019).***

***

Створення та функціонування кібервійськ

«Приоритетными направлениями, по которым Токио собирается укреплять свою обороноспособность, будут космос, киберпространство и защита от электромагнитного излучения, говорится в Белой книге обороны за 2019 год.

В пятницу документ представили правительству страны…

…отмечается необходимость создания механизмов предупреждения кибератак на системы командования и коммуникаций сил самообороны и их сетей, а также минимизации ущерба в случае подобных инцидентов…

Белая книга сообщает, что Япония намерена сформировать «специальное подразделение по космическому пространству» к 2022 году и переформатировать существующие в трех родах войск отделы кибербезопасности в единое «подразделение кибероборонь» к 2023 году…» ***(Наталья Ануфриева. Япония расставила приоритеты в укреплении обороны // Деловая газета «Взгляд» (https://vz.ru/news/2019/9/27/999993.html). 27.09.2019).***

***

«Хакерская атака, осуществленная весной текущего года на одну из американских электростанций, оказалась не так разрушительна, как предполагалось ранее, утверждается в отчете Североамериканской корпорации по надежности энергоснабжения (North American Electric Reliability Corporation, NERC).

Инцидент произошел 5 марта. В ходе атаки злоумышленники в течение примерно 10 часов постоянно вызывали сбой в работе межсетевых экранов. Согласно отчету, данный инцидент не оказал существенного влияния на функционирование сети энергоснабжения США. Атака затронула лишь межсетевые экраны на границе сетевого периметра, которые в течение всего дня 5 марта, постоянно выходили из строя на пять минут.

Как показало расследование, перезагрузки были вызваны «вмешательством стороннего лица, эксплуатирующего известные уязвимости в межсетевых экранах». Позже выяснилось, что оператор не установил обновления прошивки для затронутых решений. После обновления систем атаки прекратились.

Причину данной ситуации оператор пояснил отсутствием механизма проверки обновлений безопасности перед их развертыванием. Хотя инцидент не вызвал масштабных последствий, NERC акцентировала на нем внимание, чтобы подчеркнуть тот факт, что многие компании не устанавливают обновления вовремя и это может привести появлению уязвимостей в сетях.

Организация привела ряд рекомендаций по работе с межсетевыми экранами и патчами, в их числе: следование практикам отрасли по устранению уязвимостей; уменьшение поверхности атаки; использование VPN и списков контроля доступа; сегментация и мониторинг сети и пр. Полный набор рекомендаций представлен в отчете NERC…» ***(В атаке на электростанцию в США эксплуатировались уязвимости в межсетевых экранах // SecurityLab.ru (https://www.securitylab.ru/news/500890.php). 09.08.2019).***

***

«МАГАТЕ розробляє єдиний стандарт для всіх АЕС світу з набором інструментів. Документ стане інструкцією для тренувань з кібербезпеки в атомній енергетиці.

Зустріч провідних програмістів-атомників, що розробляють проект документа, відбулась у Відні (Австрія). Від України участь в роботі брав провідний інженер-програміст цеху теплової автоматики та вимірювань ВП ЗАЕС Станіслав Стеблюк.

На енергоблоках йде заміна обладнання з використанням сучасних комп’ютерно-інтегрованих систем управління. І якщо тренування і навчання з ядерної, пожежної, радіаційної безпеки в атомній енергетиці України проходять постійно, то з кібербезпеки їх наразі немає.

Поки що тільки США, Канада, Словенія і Аргентина проводять національні міжгалузеві навчання з кібербезпеки.

«Країни-учасниці пропонують різні підходи для організації тренувань з комп'ютерної безпеки. Зараз модернізується велика кількість комп'ютерних систем і кібербезпеці приділяється все більша увага. Нам потрібно розуміти, які існують ризики, і бути до них готовими», — розповів Станіслав Стеблюк.

Це вже друга зустріч фахівців з кібербезпеки. Кожен з них презентував проведення тренувань з різними підходами та сценаріями.

На створення документу МАГАТЕ відведено рік. Стандарт дозволить грамотно проводити тренування та навчання з комп'ютерної безпеки і включатиме позитивні практики в системах захисту, а також рекомендації для оперативного реагування на атаки, що можуть виникнути.» ***(МАГАТЕ розробляє документ стосовно кібербезпеки на АЕС // МОЙ НИКОПОЛЬ.ОНЛАЙН (https://moi-nikopol.online/news/nikopol/16311-magate-rozrobljaie-dokument-stosovno-kiberbezpeki-na-aes/). 11.09.2019).***

***

Захист персональних даних

«Разработчики Chromium-браузера Brave заявили об имеющихся у них новых доказательствах нарушения компанией Google европейского законодательства в области защиты данных. Старший директор по политике и отраслевым отношениям Brave Джонни Райан (Johnny Ryan) представил имеющиеся в его распоряжении факты Комиссии по защите данных (Data Protection Commission, DPC) в Ирландии.

В мае нынешнего года DPC начала расследование в отношении Google RTB, протокола обмена рекламой, используемого для связи рекламодателей с web-сайтами, продающими их продукцию.

В прошлом году Райан подал жалобу на Google в Ирландии и Великобритании, обвинив компанию в нарушении «Общего регламента по защите данных» (GDPR). Согласно жалобе, Google и рекламные компании раскрывали персональные данные в ходе запросов RTB на сайтах, использующих поведенческую рекламу от Google. По словам Райана, техногигант «транслировал» данные сотням своих партнеров, и дальнейшая судьба этих данных была неизвестна.

Теперь Райан заявляет, что компания обходит GDPR с помощью файлов cookie под названием google_push (Push Page). По его словам, google_push позволяет рекламщикам обмениваться идентификационными данными профиля пользователя во время загрузки им web-страниц.

Каждый Push Page является уникальным, поскольку к URL-адресу страницы добавляется уникальный идентификатор, который в совокупности с остальными файлами cookie позволяет компаниям идентифицировать пользователя.

Поведенческая реклама – контекстная реклама, созданная с привязкой к конкретным интересам пользователя.» ***(Google обвиняется в обмене данными***

пользователей с сотнями своих партнеров // SecurityLab.ru (https://www.securitylab.ru/news/500856.php). 06.08.2019).

***

«Исследователи из компании Avast обнаружили более 600 тыс. GPS-трекеров, используемых для отслеживания пожилых людей и детей, в которых по умолчанию установлен пароль «123456». Данные устройства популярно в США, Европе и других регионах.

По словам специалистов, злоумышленники могут использовать этот пароль для взлома учетных записей пользователей, а затем подслушивать разговоры рядом с GPS-трекером, подделывать его реальное местоположение или получить номер телефона на прилагаемой SIM-карте для отслеживания по каналам GSM.

Проблема была обнаружена в более 30 моделях GPS-трекеров, изготовленных китайским производителем IoT-устройств Shenzhen i365-Tech. Все модели имеют одинаковую серверную инфраструктуру, которая состоит из облачного сервера, web-панели для входа в браузер с целью проверить местоположение трекера и мобильного приложения, которое также подключается к облачному серверу.

Идентификаторы пользователей основываются на номере международного идентификатора мобильного оборудования (International Mobile Equipment Identity, IMEI) GPS-трекера и являются последовательными, в то время как пароль одинаков для всех устройств — «123456». Злоумышленник может запускать автоматические атаки на облачный сервер Shenzhen i365-Tech, просматривать все идентификаторы пользователя один за другим, использовать один и тот же пароль «123456» и перехватывать учетные записи пользователей.

Хотя пользователи могут изменить дефолтный пароль после первого входа в учетную запись, во время сканирования около 4 млн идентификаторов пользователей специалисты обнаружили свыше 600 тыс. учетных записей с паролем «123456».

Компания Shenzhen i365-Tech не ответила на электронные письма исследователей об обнаруженной проблеме. Пользователям рекомендуется сменить пароли в учетных записей как можно скорее.» ***(В более 600 тыс. китайских GPS-трекерах по умолчанию установлен пароль «123456» // SecurityLab.ru (https://www.securitylab.ru/news/500855.php). 06.08.2019).***

***

«В рамках масштабного проекта по картированию Сети исследовательская команда vpnMentor обнаружила утечку электронных писем южнокорейской компании DK-LOK.

DK-LOK является крупным производителем промышленных труб, клапанов и трубопроводных фитингов с клиентами по всему миру. Исследователи обнаружили уязвимость в базе данных используемой компанией почтовой платформы, позволившую им получить доступ к внутренней и внешней электронной переписке. Многие письма были помечены как конфиденциальные и содержали информацию о проводимых DK-LOK операциях в разных странах (в том числе в России), продуктах и связях с клиентами. По словам исследователей, утечка затрагивает подразделения компании в нескольких странах.

Уязвимость в платформе позволила не только просматривать содержимое электронных писем, но также получить доступ к персональным данным сотрудников и клиентов компании. В частности, исследователи смогли узнать полные имена и фамилии, идентификационные номера, внутренние электронные адреса сотрудников международных отделений DK-LOK, внешние электронные адреса клиентов, номера телефонов и пр.

Команда vpnMentor попыталась связаться с компанией и сообщить о проблеме, но не получила никакого ответа. Поскольку исследователям видна вся переписка, они увидели, что их электронное письмо было не просто благополучно доставлено, но и удалено.» ***(Обнаружена утечка данных крупного производителя промышленных труб // SecurityLab.ru (https://www.securitylab.ru/news/500851.php). 06.08.2019).***

***

«**Эксперты компании Wizcase нашли в свободном доступе более 15 тыс. IP-камер, которые транслируют в Интернет видео из частных домов, организаций и религиозных учреждений.** По словам исследователей, во многих случаях сторонние пользователи могут удаленно менять настройки устройств, что открывает злоумышленникам дополнительные возможности для вмешательства в частную жизнь.

Уязвимые камеры расположены в разных странах, в том числе в России, Австралии, Германии, Великобритании, Франции и США. Список поставщиков небезопасных устройств также оказался немалым — в отчете перечислены около 10 изделий различного производства; в этот список включена продукция AXIS, Cisco и Yawcam…

Как отмечают эксперты, по техническим данным веб-камер не получится определить владельца какого-либо устройства. В то же время длительная слежка позволит злоумышленнику собрать дополнительную информацию из подслушанных разговоров и прочих деталей контекста. Таким образом, он сможет получить конфиденциальные данные своих жертв, определить их адрес и подгадать момент, когда дом или офис будет пустовать. В тех случаях, когда уязвимое устройство открывает доступ к панели администратора, взломщик сможет даже удалить видео со следами вторжения.

Кража со взломом — далеко не единственная угроза, о которой предупреждают исследователи. Камеры передают онлайн интимные сцены пользователей, позволяют следить за их детьми. Экстремисты могут таким образом планировать атаки на групповые меньшинства, а если устройство установлено в какой-либо организации, оно становится удобным средством корпоративного шпионажа…

«Производители веб-камер стремятся использовать технологии, облегчающие установку устройства, — поясняют исследователи. — Однако иногда это приводит к открытым портам и отсутствию каких-либо аутентификационных механизмов. Во многих случаях устройство не защищено брандмауэром или VPN, не использует белые списки IP-адресов, хотя все эти меры блокируют возможность сканирования и произвольных подключений».

Именно частные виртуальные сети (Virtual Private Network) эксперты называют самым надежным способом защиты. Они создают барьер между уязвимой камерой и внешним Интернетом, запрещая прямой доступ к открытым портам через внешний IP-адрес. В качестве дополнительного средства безопасности рекомендуется также установить уникальный пароль для каждого сетевого устройства.

Пользователям также стоит проверить, каким способом обеспечивается удаленный доступ к их камере. Производители используют для этого две технологии: UPnP (Universal Plug and Play) открывает порт на домашнем роутере, P2P (Peer To Peer) устанавливает соединение через сервер производителя. Второй способ считается безопаснее, поэтому эксперты рекомендуют покупать устройства с поддержкой этой функции и проверять при установке, отключен ли протокол UPnP…» ***(Maxim Zaitsev. В открытом доступе обнаружено 15 тысяч IP-камер // Threatpost (https://threatpost.ru/researches-discover-15-thousand-ip-cameras-in-public-access/34115/). 17.09.2019).***

***

«В 2019 г. с утечками данных столкнулись 34% крупных и 27% небольших компаний в России, сообщила пресс-служба «Лаборатории Касперского». Эти показатели значительно выше аналогичных за прошлый год.

К небольшим компаниям эксперты отнесли те, в которых работают не более 50 человек. Число утечек в таких компаниях выросло по сравнению с результатами исследования 2018 г. на 12 процентных пунктов.

Похожая тенденция наблюдается и в крупном бизнесе. Согласно опросу 2018 г., с утечкой сталкивалась каждая четвертая корпорация, а по итогам исследования 2019 г. – уже каждая третья.

Эксперты связали рост числа утечек с недостаточными мерами в области кибербезопасности. «Небольшие компании часто сфокусированы на росте своего бизнеса, кибербезопасность не входит в число их приоритетов», – пояснил Андрей Данкевич, руководитель направления маркетинга для малого и среднего бизнеса «Лаборатории Касперского». ***(Треть крупных российских компаний столкнулась с утечкой данных в 2019 году // АО Бизнес Ньюс Меди (https://www.vedomosti.ru/technology/news/2019/09/16/811341-2019). 16.09.2019).***

***

«Появление единой системы, позволяющей банкам проверять сведения о владельцах SIM-карт, чревато масштабными утечками данных. Об этом сообщается в письме, адресованном «большой тройкой» операторов связи руководителю комитета Госдумы по финансовому рынку Анатолию Аксакову (копия есть у РБК, свое участие в работе над письмом подтвердили представители МТС, «МегаФона» и «ВымпелКома»).

Создание такой системы предусмотрено поправками в закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», которые в июле 2018 года были внесены в Госдуму, а в марте 2019-го приняты в первом чтении. Второе чтение документа запланировано на октябрь, сообщил Анатолий Аксаков. Письмо «тройки» он пока

не видел. В то же время Аксаков отметил, что «если аргументы операторов будут достаточными, то их учтут».

Операторы связи в своем письме указали, что поддерживают идею борьбы с мошенничеством на финансовом рынке, но предлагаемый депутатами механизм несет «ряд существенных рисков».

Поправки не содержат требований к информационной безопасности данных, передаваемых через единую систему, что «может повлечь утечку данных о нескольких десятках миллионов абонентов». Инициатива заставит операторов нарушать закон «О персональных данных», который не допускает обработку данных, если это не соответствует изначально заявленным целям. Оператор обрабатывает сведения об абонентах для оказания услуг связи, а не для обмена информацией с кредитными организациями…». ***(Операторы: при передаче банкам данных об абонентах могут произойти утечки // (https://roskomsvoboda.org/49711/). 18.09.2019).***

***

«Исследователи из Северо-Восточного университета США и Имперского колледжа Лондона обнаружили, что умные телевизоры от Samsung, LG и Amazon отправляют данные о местоположении и IP-адреса пользователей сторонним компаниям, даже находясь в режиме ожидания, пишет Financial Times. Помимо Samsung и LG, в отчете исследователей фигурируют такие марки как Roku и Amazon Fire TV. Отправляются данные чаще всего в Google, Facebook, Amazon и Netflix.

Причём данные отправляются независимо от того, есть ли у пользователя учетная запись Netflix. Исследователи также выяснили, что другие «умные» устройства, например, динамики и камеры, тоже отправляют пользовательские данные десяткам сторонних разработчиков, включая Spotify и Microsoft. Кроме того, в исследовании говорится, что Smart TV используют технологию распознавания контента, которая отслеживает все, что смотрят пользователи и получает огромный массив данных для статистической обработки.

В большинстве случаев дело касается трёх вещей: умные телевизоры отправляют данные о местоположении, IP-адреса и время, в которое устройство было использовано. Последний факт недвусмысленно намекает на то, что рекламодатели получили возможность видеть, когда пользователь дома, а когда нет.

Однако большая часть данных оказалась зашифрована и ученые не смогли выяснить, что ещё отправляют Smart TV о своих владельцах.

В ответ на запрос СМИ, Netflix и Facebook сказали, что отправляемые данные нужны им исключительно для корректировки отображения данных сервисов на экранах умных телевизоров и прочих технических нюансов. В Google заявили, что с помощью получаемых данных измеряют эффективность рекламы, что помогает таргетировать рекламу создателям приложений на Smart TV.

Эксперты говорят, что надзор за тем, как умные девайсы распоряжаются данными пользователей, слишком слабый и стоит его усилить. Мы уже привыкли к сбору данных со смартфонов, но то, что это делают телевизоры прямо из дома, и правда настораживает.» ***(Умные телевизоры отправляют данные пользователей***

Google и Facebook // РосКомСвобода (https://roskomsvoboda.org/49718/). 18.09.2019).

***

«…Специалисты компании UpGuard обнаружили в открытом доступе конфиденциальные документы, раскрывающие подробности об использовании на сетях российских операторов связи системы технических средств для обеспечения функций оперативно-разыскных мероприятий (СОРМ).

1,7 ТБ чувствительных данных, в том числе схемы, учетные данные администраторов, архивы электронных писем и другие материалы, проливающие свет на инфраструктуру телекоммуникационных компаний, хранились на незащищенном сервере rsync, доступ к которому мог получить любой желающий.

Хотя на сервере хранилась информация, касающаяся крупнейших в России операторов связи, утечка затронула в основном компании Nokia и Mobile TeleSystems (МТС). Согласно письму, полученному специалистами UpGuard от представителей Nokia, набор данных представляет собой «папку», переданную сотрудником Nokia неназванной третьей стороне. Именно эта третья сторона, говорится в письме, и не позаботилась об обеспечении надлежащей защиты сервера, не принадлежащего Nokia.

Помимо прочего, на сервере хранились фотографии (578 тыс. файлов jpeg) и инструкции по развертыванию СОРМ – оборудования, устанавливаемого на сетях операторов связи и использующегося ФСБ РФ для перехвата телекоммуникаций в рамках исполнения требований «закона Яровой». В частности СОРМ позволяет перехватывать идентификаторы абонентов, их номера телефонов, текстовые сообщения, электронные письма и IP-адреса. С 1995 года установка СОРМ является обязательной для всех операторов связи в РФ…

11 сентября UpGuard обратилась за помощью к правительству США, и в результате компании удалось связаться с нью-йоркским юридическим офисом Nokia. Позднее в этот же день Викери позвонил директор по информационной безопасности Nokia. Еще 12 сентября сервер оставался доступным, но уже на следующий день был защищен.» ***(Масштабная утечка данных пролила свет на участие Nokia в установке СОРМ на сетях МТС // SecurityLab.ru (https://www.securitylab.ru/news/501193.php). 19.09.2019).***

***

«…В Эквадоре арестован исполнительный директор аналитической компании, оставившей персональные данные практически всех жителей страны в открытом доступе на незащищенном сервере. Арест был произведен в рамках расследования, инициированного после сообщений в СМИ о масштабной утечке данных эквадорцев.

В понедельник, 16 сентября, специалисты команды vpnMentor сообщили об обнаружении в открытом доступе базы данных, содержащей персональную информацию более 20 млн человек. Незащищенный сервер Elasticsearch располагался в Майами (штат Флорида) и принадлежал эквадорской консалтинговой компании Novaestrat, оказывающей услуги в сфере аналитики, стратегического маркетинга и разработки программного обеспечения.

Размер базы данных составлял 18 ГБ. В ней содержалась высоко персонализированная информация, которая могла быть собрана из внешних источников, таких как государственные реестры, автомобильная ассоциация Aeade и Национальный банк Эквадора. В частности, на сервере хранились полные имена и фамилии граждан, сведения о половой принадлежности, дате и месте рождения, домашние и электронные адреса, домашние и рабочие номера телефонов, сведения о семейном статусе и дате вступления в брак, а в некоторых случаях еще и даты смерти.

Более того, в БД содержались сведения о клиентах эквадорского нацбанка, в том числе информация о балансе счета, типе кредитования и пр., а также подробные сведения о каждом члене семьи, включая их идентификационные номера.

Исследователи также обнаружили в БД персональные данные Джулиана Ассанжа, которому власти Эквадора предоставляли политическое убежище с 2012-го по апрель 2019-го года.

Сообщение об утечке всколыхнуло общественность, и руководство страны незамедлительно предприняло соответствующие меры. По горячим следам было инициировано расследование, в ходе которого выяснилось, что Novaestrat не имела права владеть вышеперечисленными данными. Против руководства компании было выдвинуто обвинение в нарушении приватности и несанкционированном распространении персональных данных.

В рамках расследования был произведен арест главы Novaestrat Уильяма Роберто Г. (William Roberto G.). В ходе обыска из его дома была изъята компьютерная техника.» ***(Эквадор бурно отреагировал на утечку данных всех жителей страны // SecurityLab.ru (https://www.securitylab.ru/news/501173.php). 19.09.2019).***

***

«…Исследователь Авишай Эфрат (Avishai Efrat) из компании Wizcase обнаружил более 15 тыс. потенциально доступных для взлома web-камер, многие из которых расположены в домах людей по всему миру, включая Аргентину, Австралию, Австрию, Бразилию, Канаду, Францию, Германию, Италию, Японию, Пакистан, Россию, Испанию, Швейцарию, Великобританию, США и Вьетнам.

По словам исследователя, практически любой злоумышленник с подключением к Интернету может получить к ним доступ и изменить настройки устройства. Большинство камер также имеют очень простые учетные данные, которые можно обойти для получения прав администратора.

Данная проблема затрагивает web-камеры от AXIS, Cisco Linksys, IP Camera Logo Server, IP WebCam, IQ Invision web camera, Mega-Pixel IP Camera, Mobotix, WebCamXP 5 и Yawcam. Среди доступных устройств также были камеры в магазинах, на кухнях/в гостиных/офисах частных семейных домов, теннисных кортах, складских помещениях, отелях, церквях, мечетях, автостоянках, спортивных залах и пр.

Благодаря доступу к web-камерам злоумышленники могут собирать компрометирующую информацию, изменять настройки и учетные данные

администратора, получить информацию для доступа к банковским счетам и кражи личных данных, проводить межгосударственный шпионаж, следить за конкурирующими предприятиями и пр.

Специалисты рекомендуют в целях безопасности ограничить список адресов, которые могут подключаться к web-камере, изменить установленные по умолчанию учетные данные и использовать только защищенные камеры.» ***(Около 15 тыс. web-камер оказались доступны для удаленного взлома // SecurityLab.ru (https://www.securitylab.ru/news/501138.php). 17.09.2019).***

***

«Користувачі застосовують різні паролі, серед них є комбінації, що викликають занепокоєння. Фахівці компанії Avira, що спеціалізується на кібербезпеці, назвали саме небажане поєднання цифр і букв…

Експерти відзначають, що мова не йде про паролі, що складаються з набору цифр типу «123456» або букв («qwerty» або «admin»). Є велика кількість людей, що користуються простими комбінаціями. У цьому випадку ризик злому залишається дуже високим. Вкрай небезпечним способом вважають відсутність цифр і букв. Його користувачі не заповнюють необхідні поля для логіна і пароля, вони просто ставлять прогалини. Системи авторизації не завжди допускають створення облікового запису на основі таких параметрів. Поряд з цим, багато хто з них ще не вимагають при вході на інтернет-ресурси числові або інші комбінації. Для забезпечення повної безпеки свого облікового запису і збереження особистої інформації необхідно використовувати складні варіанти.

При цьому не можна допускати, щоб один і той же набір даних застосовувався для e-mail і для роботи в соцмережах. Порядку 10% користувачів придумують правильні поєднання для облікових записів, тоді як понад 55% використовують однакові паролі для різних акаунтів, що є небезпечним.» ***(Експерти назвали найбільш поширений і небезпечний пароль // ВСВІТІ (http://vsviti.com.ua/news/104370). 22.09.2019).***

***

«Владельцы YouTube-каналов с многомиллионной аудиторией жалуются на массовый угон аккаунтов… в конце прошлой недели злоумышленники сумели завладеть доступом к десяткам видеоблогов, преимущественно автомобильной тематики. Владельцы взломанных профилей пытаются получить помощь у администрации сервиса, однако его представители пока отказываются комментировать ситуацию.

По словам пострадавших, киберпреступники сумели украсть действующие логины и пароли YouTube-аккаунтов, заманив их создателей на фишинговый сайт. Как удалось узнать ZDNet, злоумышленники использовали методы социальной инженерии, рассылая жертвам письма с упоминанием других каналов из этой же ниши. Послание, замаскированное под сообщение о выигрыше в конкурсе, содержало ссылку на ресурс, контролируемый преступниками.

После того как владелец профиля вводил свои учетные данные на поддельной странице авторизации, мошенники заходили в скомпрометированный аккаунт, меняли логин, пароль и электронную почту владельца, а также адрес канала. Если пострадавший пользователь YouTube пытался открыть свою

страницу, используя прежний URL, он видел сообщение, что такого канала не существует.

Злоумышленники попытаются продать угнанные YouTube-каналы в даркнете

В ряде случаев киберпреступники сумели обойти двухфакторную аутентификацию и перехватить код подтверждения из SMS. По мнению ИБ-специалистов, авторы кампании могли использовать один из фишинговых тулкитов на базе обратного прокси-сервера для доступа к мобильным сообщениям сервиса. Как утверждают владельцы взломанных каналов, YouTube пока не торопится возвращать украденные аккаунты.

Журналистом удалось получить комментарий одного из участников хакерского сообщества OGUsers под псевдонимом Askamani. По его словам, в ближайшее время следует ожидать массовой продажи угнанных профилей на специализированных форумах в даркнете, поскольку злоумышленникам необходимо сбыть свою добычу до того, как видеохостинг отреагирует на инцидент. Askamani также отметил, что в атаках, скорее всего, используются сведения из базы данных с электронными адресами популярных блогеров, сгруппированными по тематике каналов…» ***(Maxim Zaitsev. Автомобильные блогеры лишились своих YouTube-каналов // Threatpost (https://threatpost.ru/new-account-hijack-campaign-targeting-youtube-car-community/34222/). 24.09.2019).***

***

«Операторы ботнета Gootkit оставили в открытом доступе две базы MongoDB с информацией, которую они собрали на компьютерах частных лиц, компаний и государственных организаций. Обнаружившие хранилище эксперты смогли подробно изучить материалы и сформировать представление о деятельности группировки.

Как и почему эти серверы оказались в открытом доступе, неизвестно. Причиной могла стать ошибка преступников, забывших установить пароль, или сбой брандмауэра, за которым находились хранилища. Через неделю после обнаружения базы из открытого доступа пропали, однако эксперты успели скопировать содержащиеся в них данные.

Стоящие за GootKit злоумышленники редко попадают в поле зрения СМИ — преступники проводят точечные атаки, не сравнимые по масштабам с операциями ботоводов Emotet или Trickbot. Несмотря на это, зловред, за которым аналитики наблюдают с 2014 года, довольно опасен…

В незащищенных базах MongoDB эксперты нашли коллекцию разнообразных данных, собранных зловредом. Как выяснилось, два сервера аккумулировали информацию с трех ботнетов Gootkit, которые охватывали в общей сложности около 39 тыс. зараженных компьютеров. В хранилищах был обнаружен набор «коллекций», в частности:

Luhnforms — около 15 тыс. записей с данными платежных карт, подробностями о том, на каком сайте они были похищены, какой компьютер и какой браузер использует жертва.

Windowscredentials — около 2,4 млн записей с логинами и паролями от различных онлайн-сервисов: интернет-магазинов, сайтов государственных организаций, криптобирж; эксперты полагают, что в данном случае реальное число

пострадавших пользователей не совпадает с количеством записей, т. к. среди данных могут встречаться дубликаты.

Screenshots — снимки с экрана.

Еще более десятка коллекций содержало технические данные зараженных компьютеров — от IP-адресов и доменных имен до версии ОС и результатов проверки на виртуальное окружение. В дополнение к этой информации на серверах обнаружились конфигурационные файлы Gootkit со ссылками для загрузки функциональных модулей зловреда…» ***(Julia Glazova. Эксперты нашли в Интернете базы данных группировки Gootkit // Threatpost (https://threatpost.ru/gootkit-mongodb-databases-found-in-internet/34144/). 19.09.2019).***

***

«Специалист по безопасности Авинаш Джайн (Avinash Jain) обнаружил в свободном доступе тысячи календарей Google. Таким образом, любой пользователь может отслеживать частные и корпоративные мероприятия, читать конфиденциальные материалы из вложений к планируемым событиям.

Джайн сделал свое открытие, используя специальные поисковые запросы Google (так называемые Google Dorks). В частности, команда inurl:https://calendar.google.com/calendar?cid= открывает все общедоступные календари. На момент публикации их количество составляет около восьми тысяч…

Виновниками такой ситуации оказались владельцы календарей, которые сами предоставляют свою информацию поисковику. Настройки Google позволяют им делиться расписанием с определенными пользователями, сделать его доступным по ссылке или же открыть для всех желающих.

При открытии публичного доступа на экране появляется уведомление о том, что данные появятся в результатах поиска Google и будут доступны всем желающим. Однако, по мнению Джайна, многие пользователи игнорируют это предупреждение или забывают о нем…

Исследователь допускает, что многие календари могут быть открыты специально — например, чтобы встраивать их в сайты или предлагать интернет-пользователям для подписки. Однако во многих случаях они явно содержали конфиденциальную информацию. Среди таких материалов были ссылки на корпоративные мероприятия, внутренние презентации, данные о посещении врача и приватные встречи…

Разработчики Google заявили, что пользователи осознанно принимают решение о предоставлении общего доступа к своим календарям. Таким образом, возможность прочитать и подписаться на чужое расписание нельзя считать уязвимостью сервиса. Тем не менее, многие комментаторы указывают, что владельцы публичных календарей могут со временем забыть об открытом доступе.

Эксперты рекомендуют всем администраторам проверить установленный уровень приватности Google-календарей. Инструкции для этого процесса опубликованы на сайте поддержки. При необходимости пользователи могут скрыть детали мероприятий и оставить видимой лишь информацию о том, заняты они или свободны в определенный период времени…» ***(Dmitry Nazarov. Данные тысяч пользователей доступны через Google Календарь // Threatpost***

(https://threatpost.ru/users-data-exposed-via-public-google-calendars/34132/). 18.09.2019).

***

«По мере роста числа подключенных устройств киберпреступники все чаще обращают внимание на «Интернет вещей» (IoT). Сейчас самыми популярными у хакеров IoT-устройствами являются маршрутизаторы. Тем не менее, как отмечают специалисты, в последнее время киберпреступники стали проявлять интерес к «умным» газовым насосам.

В ходе исследования эксперты компании Trend Micro изучили торговые площадки даркнета на русском, арабском, португальском, испанском и английском языках. Наиболее передовыми оказались русскоязычные киберпреступные форумы. На них продаются не только эксплоиты и методы осуществления атак, но также модифицированные «умные» электросчетчики.

Согласно принятому Госдумой РФ закону, с 1 июля 2020 года по мере выхода из строя старых электросчетчиков россияне будут обязаны устанавливать новые смарт-счетчики, автоматически фиксирующие расход электроэнергии и передающие эти данные обслуживающим энергосбытовым компаниям.

В ожидании вступления закона в силу киберпреступники уже сейчас продают смарт-счетчики с модифицированной прошивкой, способной регистрировать меньшее энергопотребление и позволяющей, по сути, воровать электричество.

Участники русскоязычных киберпреступных форумов также активно интересуются методами взлома газовых насосов и обмениваются пособиями по их внутреннему устройству, в том числе насосов, оснащенных программируемыми логическими контроллерами.

Касающиеся газовых насосов темы также стали появляться на бразильских форумах. Более того, участники этих форумов обмениваются еще более подробными техническими инструкциями по взлому.

Скорее всего, способы взлома газовых насосов интересуют киберпреступников с той же целью, что и взлом электросчетчиков – для похищения ресурсов. Однако компрометация газовых насосов может также использоваться и в более деструктивных целях, например, для причинения физического ущерба оборудованию, включения его в ботнет для осуществления DDoS-атак, блокировки с целью вымогательства и пр.» ***(Киберпреступники обратили внимание на «умные» газовые насосы // SecurityLab.ru (https://www.securitylab.ru/news/501027.php). 11.08.2019).***

***

«Производитель автомобильных компонентов Toyota Boshoku Corporation (входит в Toyota Group) сообщил о мошенничестве, в результате которого одна из ее европейских дочерних компаний потеряла более $37 млн. Инцидент произошел 14 августа текущего года.

BEC-атаки (business email compromise – компрометация деловой почты) — мошеннические операции, в рамках которых преступники пытаются путем обмана убедить одного или нескольких сотрудников целевых организаций перевести деньги на банковские счета, контролируемые злоумышленниками. Данный тип атак довольно успешен, поскольку мошенники выбирают людей, которым доверяют сотрудники, например, надежный деловой партнер или генеральный директор компании.

Подробности об инциденте пока отсутствуют. Компания сообщила о происшествии властям и вместе с правоохранительными органами начала расследование…» ***(Дочерняя компания Toyota Boshoku потеряла $37 млн в результате BEC-атаки // SecurityLab.ru (https://www.securitylab.ru/news/500893.php). 09.08.2019).***

***

«Китайские киберпреступники нацелились на корпоративные VPN-серверы от Fortinet и Pulse Secure. Причиной тому стала публикация в свободном доступе информации об уязвимостях, обнаруженных в продуктах в августе нынешнего год…

Атаки осуществляются киберпреступной группировкой APT5 (Manganese), предположительно спонсируемой китайским правительством. Преступники атакуют и взламывают организации в разных отраслях, однако в первую очередь они уделяют внимание телекоммуникационным и технологическим компаниям и проявляют особый интерес к компаниям, занимающимся спутниковой связью. По словам исследователей из ИБ-компании FireEye, APT5 действует с 2007 года и «представляет собой большую группу преступников, состоящую из нескольких подгрупп с определенной тактикой и инфраструктурой».

Начиная с конца августа, одна из подгрупп APT5 создала инфраструктуру, посредством которой она проводила интернет-сканирование для поиска VPN-серверов Fortinet и Pulse Secure, предполагают исследователи. Затем преступники попытались проэксплуатировать уязвимости в VPN-серверах. Обе уязвимости (CVE-2018-13379 в Fortinet и CVE-2019-11510 в Pulse Secure) связаны с «предварительным считыванием файлов». Их эксплуатация позволяет неавторизованному злоумышленнику извлекать файлы с VPN-сервера…» ***(Китайская группировка Manganese нацелилась на VPN-серверы Pulse Secure и Fortinet // SecurityLab.ru (https://www.securitylab.ru/news/500860.php). 06.08.2019).***

***

«Гугл» платитиме фахівцям з кібербезпеки, які виявлять ознаки зловживання даними в продуктах, що розміщені на платформах компанії.

Як повідомляє TechCrunch, йдеться про Android-додатки і розширення для Chrome. У компанії підкреслили, що додатки, які продають або несанкціоновано використовують призначені для користувача дані, будуть негайно видалені з Google Play і Google Chrome Web Store. А якщо розробника зловлять на зловживанні доступом до обмежених областей в Gmail — для нього закриють API.

Поки «Гугл» не встановила точних розмірів винагород в рамках програми виявлення багів, проте в компанії говорять, що вони можуть досягати $ 50 000 за один репорт…» ***(«Гугл» заплатить до $ 50 000 за виявлені зловживання даними***

в Chrome і Android // MediaSapiens (https://ms.detector.media/web/IT_companies/gugl_zaplatit_do_50_000_za_viyavleni_zlovzhivannya_danimi_v_chrome_i_android/). 02.09.2019).

***

«Злочин був скоєний ще у березні 2019 року, але відомо про це стало тільки тепер. Шахраї використали штучний інтелект і зімітувавши голос керівника британської компанії, змусили підлеглого переказати їм $ 243 тис. Генеральний директор британської енергетичної фірми думав, що розмовляв по телефону зі своїм начальником, виконавчим директором німецької головної компанії. Бос попросив його терміново, протягом години, переказати $ 243 тис. угорському постачальнику.

Директор британської фірми впізнав німецький акцент і тембр начальника голосу, тому виконав прохання. Але шахраї подзвонили ще двічі. Після переказу грошей хакери сказали, що німецька компанія відправила британській суму на відшкодування збитків. Втретє вони запросили другий платіж. Однак обіцяний переказ ще не прийшов, а дзвінок надійшов з австрійського номера. Тоді британець запідозрив недобре і не став платити ще раз.

Гроші пішли на рахунок угорського банку, потім були переведені в Мексику і далі розійшлися по різних місцях. Детективам не вдалося виявити жодного підозрюваного. Невідомо, чи використовували злочинці роботів, щоб згенерований голос міг самостійно реагувати на питання жертви…

Поліція та експерти з кібербезпеки ще в 2018 році передбачали, що злочинці почнуть використовувати штучний інтелект для автоматизації кібератак. Рюдігер Кірш, експерт з шахрайства в Euler Hermes, зазначив, що ніколи не стикався з шахраями, які використовували б штучний інтелект. Інцидент став першим подібним зареєстрованим злочином у Європі. Філіп Аманн, глава безпеки в Європейському центрі кіберзлочинності, зазначив, що хакери, швидше за все, почнуть частіше використовувати технологію, якщо вона дозволяє успішно скоювати злочини. Кірш вважає, що шахраї використовували комерційну програму для генерації голосу. За допомогою подібного сервісу він записав власний голос і зазначив, що імітація звучала як справжня. Існує кілька компаній, які продають програми, що дозволяють швидко імітувати голос…» ***(Іраклі Берідзе. Штучний інтелект допоміг шахраям викрасти велику суму грошей // Pingvin.pro (https://pingvin.pro/gadgets/news-gadgets/shtuchnyj-intelekt-dopomig-shahrayam-vykrasty-velyku-sumu-groshej.html). 06.09.2019).***

***

«З учорашнього вечора тривають потужні атаки на сервери Вікіпедії, тож сайт може бути недоступним», — таке повідомлення з'явилося на Фейсбук-сторінці «Вікімедіа Україна» 7 вересня.

Там уточнили, що атаки періодично зупиняються, але поновлюються. Спершу вони були зосереджені тільки на Європі та Близькому Сході, тепер — і на США.

Також у «Вікімедіа Україна» дали посилання на офіційне повідомлення від «Фонду Вікімедіа» про те, що це — таки атаки, а не технічні несправності.

«Сьогодні на Вікіпедію здійснено зловмисну атаку, яка перервала її роботу в декількох країнах. Атака триває, і наша команда інженерів наполегливо працює над тим, щоб зупинити її та відновити доступ до сайту», — йдеться у заяві.

Через сучасні виклики регіональні об'єднання та «Фонд Вікімедіа» створили спеціальні системи та найняли персонал для регулярного контролю таких ситуацій та подолання ризиків, пишуть автори…» ***(У Вікіпедії заявили про масштабну атаку на сайт енциклопедії // MediaSapiens (https://ms.detector.media/web/cybersecurity/u_vikipedii_zayavili_pro_masshtabnu_ataku_na_sayt_entsiklopedii/). 09.09.2019).***

***

«Исследователи обнаружили шпионскую кампанию, эксплуатирующую прошивку SIM-карт. Злоумышленники используют скрытые системные приложения, чтобы отслеживать перемещения своих целей во множестве стран по всему миру.

Вредоносная технология получила название Simjacker; аналитики полагают, что за ней стоит профессиональная кибергруппировка, которая начала кампанию как минимум два года назад. Этот метод гораздо сложнее известных ранее способов слежки за сотовыми абонентами, но при этом требует практически нулевых инвестиций в инфраструктуру — все операции идут через простой GSM-модем стоимостью $10…

Метод использует возможности служебной программы S@T Browser, которая поддерживает рабочие сервисы SIM-карт (например, запрос баланса или трансляцию сообщений от сотового провайдера). Это приложение считается устаревшим — в последний раз его обновляли в 2009 году. Тем не менее, оно все еще установлено на значительной части устройств.

Чтобы наладить слежку за абонентом, преступники отправляют на его аппарат специальное SMS-сообщение, адресованное напрямую S@T Browser. В нем закодированы команды, которые позволяют скрытно выполнять различные операции с пользовательским устройством. Обмен данными происходит без ведома владельца — полученные и отправленные сообщения не появляются в меню телефона.

В ходе выявленных атак злоумышленников интересовало географическое расположение и IMEI-номера целевых устройств. Исследователи определили, что таким образом можно заставить телефон совершить звонок, отправить SMS или открыть канал для передачи данных. В результате Simjacker предоставляет набор вредоносных возможностей, включая подписку на платные услуги, отправку SMS и MMS от лица жертвы, загрузку вредоносного ПО через браузер телефона…

По словам экспертов, уязвимую технологию применяют сотовые операторы в 30 странах, которые суммарно обслуживают миллиард абонентов. Обнаруженные атаки были направлены на владельцев телефонов Apple, Motorola, Samsung, Google и других крупных производителей. Simjacker можно также использовать для атак на IoT-устройства с SIM-картами…

Провайдеры могут защитить своих абонентов, блокируя сообщения с командами для S@T Browser. Кроме того, они могут удаленно перепрограммировать SIM-карты или вовсе удалить с них уязвимое приложение. В

то же время эксперты называют эти меры временными, а реальную безопасность обеспечит только новый подход к защите…» ***(Egor Nashilov. Устаревшая технология SIM-карт угрожает миллиарду абонентов // Threatpost (https://threatpost.ru/simjcker-targets-1b-cell-users/34080/). 13.09.2019).***

***

«…Исследователи из компании ReversingLabs обнаружили новую тактику, которую преступники используют для мошеннических операций. Теперь злоумышленники притворяются легальными руководителями предприятия для покупки сертификатов безопасности в интернете и дальнейшей их продажи на подпольных форумах.

В рамках данной схемы преступник сначала ищет подходящую жертву. В одном случае преступник удалил информацию со страницы руководителя британской компании в социальной сети LinkedIn, а затем зарегистрировал доменное имя, связанное с данным предприятием. Потом преступник заказал Code Signing сертификат, для которого он уже имел все необходимые данные. Для подтверждения личности юридическая информация о фирме проверяется в правительственных или доверенных сторонних базах данных, домен web-сайта проверяется по электронной почте, а затем происходит автоматический процесс обратного вызова. Теперь злоумышленник успешно выдал себя за директора компании и у него есть Code Signing сертификат, который можно продать. Данный сертификат, полученный нелегальным способом в описанном случае, теперь используется в рекламном ПО OpenSUpdater для подписи 22 исполняемых файлов, многие из которых являются вредоносными.

«Обман удостоверяющего центра — еще одна тактика, применяемая данным преступником. Используя одну и ту же личность, субъект пытается купить как можно больше сертификатов у как можно большего количества удостоверяющих центров», — поясняет сооснователь ReversingLabs Томислав Перицин (Tomislav Pericin).

Исследователи полагают, что преступник использовал ту же тактику по крайней мере против десятка компаний. С одной личностью были связаны мошеннические сертификаты расширенной проверки (EV-сертификаты). Предположительно, размер прибыли оправдывает мониторинг и настройку инфраструктуры, необходимых для прохождения многочисленных проверок личности.

Сертификаты безопасности предназначены для того, чтобы вызвать доверие пользователей к развертыванию программного обеспечения. Традиционное антивирусное программное обеспечение обычно использует базы сигнатур для определения того, содержит ли ПО, загруженное или запущенное на компьютере, вредонос. Тем не менее, если вредоносный программный продукт будет иметь законную подпись, он сможет обойти проверку.» ***(Преступники покупают сертификаты безопасности, притворяясь директорами компаний // SecurityLab.ru (https://www.securitylab.ru/news/501272.php). 20.09.2019).***

***

«…Разработчик компьютерных игр французская компания Ubisoft разослала владельцам сервисов по осуществлению заказных DDoS-атак

письменные предупреждения с требованием прекратить противоправные действия. Данный шаг является частью масштабной стратегии , направленной на борьбу с DDoS-атаками на серверы многопользовательской игры Rainbow Six Siege.

С момента выхода обновления Operation Ember Rise для Rainbow Six Siege на прошлой неделе Ubisoft находится под постоянными DDoS-атаками. С выпуском обновления компания также обнулила многопользовательские рейтинги, после чего на нее обрушился шквал атак.

С помощью DDoS-атак недобросовестные игроки вызывают задержки в работе сервера и тем самым замедляют игру. Раздосадованные постоянными задержками противники в итоге бросают игру, за что получают штрафы. В результате рейтинг запустившего DDoS-атаку игрока незаслуженно поднимается вверх. Вероятно, после обнуления рейтингов геймеры решили как можно скорее его «накрутить» и обрушили на серверы шквал DDoS-атак.

Зачастую недобросовестные игроки не осуществляют атаки сами за неимением ресурсов и обращаются за помощью к сервисам, которые готовы DDoS'ить что угодно, лишь бы заказчик платил деньги.

В связи с обрушившейся на нее волной атак компания Ubisoft разослала вышеупомянутым сервисам так называемые письма «cease & desist». Эти письма представляют собой предупреждения с требованием прекратить незаконную деятельность. Как правило, авторы таких писем устанавливают срок, до которого адресат должен выполнить требования. Если по истечении срока адресат не прекратил противоправные действия, авторы письма обращаются в суд.

В случае с Ubisoft целесообразность писем «cease & desist» находится под большим вопросом. Сервисы по осуществлению заказных DDoS-атак сами по себе являются незаконными, и «пугать» их судебным разбирательством не имеет смысла.» ***(Разработчик компьютерных игр Ubisoft пригрозил DDoS'ерам судом // SecurityLab.ru (https://www.securitylab.ru/news/501261.php). 19.09.2019).***

***

«В субботу власти Ирана заявили о том, что нефтяная инфраструктура исламского государства подверглась кибер-атаке, в результате которой возникли перебои в работе нефтяной отрасли.

"Вопреки утверждениям западных СМИ, проведенные сегодня расследования показали, что нефтяные объекты страны и другая важная инфраструктура не была подвергнута кибератакам", - заявили в государственном органе Ирана, отвечающем за кибербезопасность.

Между тем "NetBlocks", организация, которая отслеживает перебои с интернетом, в субботу ночью написала в "Twitter", что "сетевые данные показывают прерывистые нарушения интернет-соединения в Иране". Отмечается, что причина перебоев, затронувших "онлайн платформы промышленных предприятий и правительственных органов" не была установлена.» ***(Иран отрицает успешную кибератаку на нефтяные промыслы // ISRAland Online Ltd (http://www.isra.com/news/235310). 22.09.2019).***

***

«Аналитики «Лаборатории Касперского» рассказали о кибератаках на умные здания, которые были зафиксированы в первой половине 2019 года у клиентов компании. По данным экспертов, за этот период под удар попали около 40% систем автоматизации, а чаще всего инциденты были связаны с активностью шпионских зловредов…

Как пояснили специалисты, сегодня умные датчики и контроллеры используются во многих офисах и жилых зданиях, больницах, торговых центрах, на транспортных объектах и в прочих общественных заведениях. Атаки на системы управления этими модулями чаще всего грозят перебоями в работе лифтов и электронных замков. Если же в здании не обеспечена автономная подача электричества, воды и отопления, последствия могут быть серьезнее.

Несмотря на значительный объем угроз, аналитики уточняют, что основная часть атак имеет не направленный, а случайный характер — инциденты провоцируют обычные зловреды, которые пытаются попасть в корпоративные сети. Их функции не позволяют нанести серьезный урон, хотя в принципе любое вмешательство в работу умного здания может привести к проблемам. Наибольшую угрозу представляют шифровальщики, ботнет-агенты, открывающие бэкдор и перегружающие сеть вредоносным трафиком, и шпионские программы, которые охотятся за учетными данными.

Исследователи также отметили, что многие кибератаки — как случайные, так и таргетированные — направлены на сети разработчиков, интеграторов и диспетчеров систем автоматизации. Таким образом преступники пытаются расширить площадь атаки, получив доступ сразу ко всем инфраструктурам, с которыми работает их жертва. Этот вектор набирает популярность в последнее время — например, в июне таким способом воспользовались операторы шифровальщика Sodinokibi.

Больше всего от атак на системы автоматизации зданий страдают Италия и Испания. В этих странах инциденты зафиксированы почти в половине релевантных инфраструктур. В первую пятерку также вошли Великобритания (44%), Чехия (42%) и Румыния (42%). Россия осталась за пределами списка ТОП-10…

Аналитики «Лаборатории Касперского» сравнили данные о вредоносных атаках на умные здания и такую же статистику по промышленным инфраструктурам. В разделении по источникам угроз (веб-атаки, съемные носители, почтовые клиенты, сетевые папки) показатели первой группы оказались заметно выше.

В то же время по доле систем автоматизации, на которых в первом полугодии было заблокировано вредоносное ПО, сфера промышленного производства обогнала умные здания (41% против 38%). Такое положение вещей может быть связано с тем, что системы управления умными зданиями имеют большую площадь атаки — они чаще подключены к Интернету, используют email и съемные носители, поэтому один компьютер может быть атакован из разных источников…» ***(Maxim Zaitsev. Шпионы и черви возглавили список угроз умным зданиям // Threatpost (https://threatpost.ru/kaspersky-reports-on-smart-building-threats-in-1h2019/34172/). 21.09.2019).***

***

«Компания McAfee представила очередной ежеквартальный отчет по киберугрозам, в котором рассказывает об основных и актуальных на сегодня трендах в сфере киберпреступности.

Отмечается, что в I квартале специалистами McAfee был отмечен значительный рост кибератак с использованием вирусов-вымогателей – сразу на 118%. Также, в январе команда экспертов McAfee Advanced Threat Research выявила новое семейство вирусов-шифровальщиков под названием Anatova, которые могут быстро адаптироваться, используя тактики уклонения и механизмы защиты против статического анализа.

Из ключевых тем отчета можно выделить:

Основные атаки, которые используют уязвимости SMB и HTTP протоколов;

Использование уязвимости нулевого дня на различных операционных системах;

Последовательные атаки, использующие backdoor для доступа;

Схемы работы различных уязвимостей. Диаграммы активности вредоносного ПО за последние пару лет.

Более детально с этими и другими темами можно ознакомиться в отчете McAfee Labs Threats Report, August 2019 (PDF, EN).» ***(Число кибератак с использованием вирусов-вымогателей выросло на 118% // Компьютерное Обозрение (https://ko.com.ua/chislo_kiberatak_s_ispolzovaniem_virusov-vymogatelej_vyroslo_na_118_130296). 26.09.2019).***

***

«…Предположительно поддерживаемые правительством киберпреступники из Ирана атаковали американских ветеранов вредоносным ПО с помощью поддельного web-сайта. По словам исследователей из команды Cisco Talos, вредоносную кампанию организовала группировка Tortoiseshell.

Киберпреступная группировка, которую компания Symantec ранее назвала Tortoiseshell, создала web-сайт (hxxp://hiremilitaryheroes[.]com), предоставляющий помощь военным ветеранам США в поисках работы. Сайт предлагает загрузить поддельное приложение для получения доступа к предложениям о работе. Вместо этого приложение только устанавливает вредоносные программы на пользовательских системах и показывает сообщение о неудачной установке.

Вредоносная программа собирает и отправляет злоумышленникам данные, которые включают в себя информацию о системе, аппаратном обеспечении, версиях обновлений, конфигурациях сети, версиях прошивки, контроллере домена, имени администратора, списках учетных записей, дате, времени, драйверах и пр.

Помимо сбора данных, вредоносное ПО также устанавливает инструмент для удаленного доступа (RAT), который может предоставить злоумышленникам доступ к зараженной системе. Компонент RAT может запускать файлы, загруженные из интернета, выполнять shell-команды и, при необходимости, удалять себя с компьютера хоста.» ***(Американские ветераны стали жертвами киберпреступников // SecurityLab.ru (https://www.securitylab.ru/news/501389.php). 26.09.2019).***

***

«…Исследователи из компании Cylance обнаружили вредоносную кампанию, в рамках которой предположительно китайская киберпреступная группировка использовала поддельную версию утилиты «экранный диктор» (Narator) в компоненте Ease of Access для Windows. Целями атак стали технологические компании, использующие данную легитимную функцию NVIDIA.

Narrator («экранный диктор») представляет собой утилиту для Windows, которая вслух читает текст на экране для слабовидящих. Его можно вызвать на экране входа с помощью сочетания клавиш, который обеспечивает постоянный доступ на уровне системы.

Злоумышленники также используют образец вредоносного ПО с открытым исходным кодом, известный как бэкдор PcShare, для первоначального закрепления в системах жертв. Используя данные инструменты, злоумышленники могут без учетных данных тайно управлять компьютерами на базе Windows через экраны удаленной авторизации рабочего стола.

Атаки начинаются с доставки бэкдора PcShare жертвам посредством целенаправленных фишинговых атак (spear-phishing). По словам исследователей, инструмент был модифицирован и предназначен для работы при фоновой загрузке легитимным приложением NVIDIA. Как только злоумышленники получают права администратора в системе жертвы, они заменяют Narrator.exe вредоносной версией, которая дает им возможность запускать любую программу с системными привилегиями. Стоит пользователю включить поддельного «экранного диктора» на экране авторизации в систему с помощью Ease of Access, winlogon.exe запустит вредонос и предоставит привилегии SYSTEM.

После выполнения вредонос запустит легитимную утилиту, затем зарегистрирует класс окна («NARRATOR») и создаст окно («Narrator»). Данная процедура создает диалог с элементом управления редактирования и кнопкой «r», в то время как отдельный поток постоянно отслеживает нажатия клавиш. Если вредоносная программа обнаружит, что был введен определенный пароль (встроенный в файл в виде строки «showmememe»), он отобразит ранее созданный диалог, позволяя злоумышленнику указать команду или путь к файлу для выполнения с помощью элемента управления для редактирования.

Ввод заданного злоумышленником пароля позволяет создавать любой исполняемый файл с привилегиями SYSTEM на экране авторизации в систему. Данный метод в конечном итоге обеспечивает оболочке преступника персистентность в системе, не требуя настоящих учетных данных.» ***(Взлом утилиты «экранный диктор» для Windows дает полный контроль над системой // SecurityLab.ru (https://www.securitylab.ru/news/501398.php). 26.09.2019).***

***

«Злоумышленники продолжают находить всё новые способы взлома устройств обычных пользователей, под час используя для этого весьма неожиданные лазейки. Сотрудники из компании Ginno Security Lab, специализирующейся на кибербезопасности, подготовили доклад, в котором сообщили, что Simjacker — далеко не единственный эксплойт, способный работать с SIM-картами. Также они указали на WIBattack, новую уязвимость SIM-карт,

связанную с приложением WIB (Wireless Internet Browser). Согласно заявлению экспертов, WIB получает доступ к браузеру, а затем заражает телефон при помощи тщательно отформатированного SMS-сообщения, содержащего инструкции, которые могут быть приведены в исполнение на картах, не имеющих ключевых средств по обеспечению безопасности.

В случае успешного заражения чужого мобильного телефона или смартфона, контроль за устройством полностью переходит в руки злоумышленников. При помощи инструментов удалённого доступа они подключаются к заражённому аппарату, а потом начинают использовать его по своему усмотрению: звонить на платные номера, посещать фишинговые сайты, рассылать сообщения, отображать на экране определённый текст и сообщать злоумышленникам и не только информацию о местоположении заражённого гаджета.

В своём докладе эксперты Ginno Security Lab уже переслали необходимую информацию в Ассоциацию GSM, но ответа о том, начали ли в организации принимать какие-то меры — неясно. По словам обнаруживших уязвимость сотрудников Ginno Security Lab, точное количество заражённых смартфонов определить довольно сложно, однако, по предварительным данным компании, речь может идти о «сотнях миллионах» устройств. При этом их коллеги с цифрами не согласны. Они провели собственное расследование, изучив 800 SIM-карт, но только 10,7 процентов были атакованы. Так же сообщается, что три процента из этих карт заражены или уязвимы для Simjacker. И речь не обязательно идёт о картах из перехода! Все они абсолютно легальны.

На вопрос о том, насколько эффективен новый эксплойт, специалисты ответить пока затрудняются, при этом сообщают, что есть гораздо менее затратная по времени и усилиям процедура. SIM-карту можно заразить, например, вредоносным исполнительным файлом SS7.

Основная проблема SIM-карт заключается в том, что в большинстве из них применяются устаревшие криптографические шифры, созданные более 30 лет назад. Именно по этой причине хакеры могут получить доступ к карточке, а потом и устройству пользователя. Производителям SIM-карт уже давно следовало обновить не только шифры, но и содержащееся на карте ПО, приведя его в соответствие с современными стандартами безопасности. К сожалению этого до сих пор не происходит. Видимо, для разработки и перевыпуска новых карточек требуется много средств и ресурсов, раз не все могут себе это позволить…» ***(Вячеслав Ларионов. Новая уязвимость SIM-карт передаёт хакерам контроль за смартфоном // AndroidInsider.ru (https://androidinsider.ru/smartfony/novaya-uyazvimost-sim-kart-peredayot-hakeram-kontrol-za-smartfonom.html). 29.09.2019).***

***

Діяльність хакерів та хакерські угруповування

«Кибернетическое командование США загрузило в сервис VirusTotal 11 образцов вредоносного ПО, предположительно связанного с северокорейской группировкой Lazarus.

Несколько образцов относятся к трояну HOPLIGHT, предназначенному для сбора информации об операционных системах жертвы. Для связи со злоумышленниками троян использует общедоступный SSL-сертификат.

В апреле текущего года ФБР и Агентство по кибербезопасности и безопасности инфраструктуры Министерства внутренней безопасности США выпустили совместное предупреждение о трояне HOPLIGHT, чтобы компании и ведомства могли обеспечить защиту сетей и снизить риск вредоносной киберактивности со стороны правительства Северной Кореи.

Напомним, с 2018 году Министерство обороны США размещает на VirusTotal незасекреченные образцы вредоносного ПО, используемого в атаках различных APT-группировок. Данные доступны в учетной записи CNMF в сервисе VirusTotal, а также через аккаунт USCYBERCOM в Twitter, где ведомство публикует ссылки на все свежие загрузки…» ***(На VirusTotal загружено 11 вредоносов, связанных с группировкой Lazarus // SecurityLab.ru (https://www.securitylab.ru/news/500889.php). 09.08.2019).***

***

«Австрійська народна партія, яка є одним з фаворитів виборчих перегонів у країні, повідомила про хакерську атаку і викрадення даних…

Партія повідомила про викрадення 1300 гігабайтів даних з серверів партії. Частина інформації, зокрема, все, що стосувалося пожертв і фінансування виборчої кампанії, була злита у медіа.

За даними експерта з кібербезпеки Аві Кравіца, залученого партією, атака на сервери проводилася з 27 липня по 3 вересня.

В Австрійській народній партії назвали кібератаки нападом не тільки на її інфраструктуру, а й на австрійську демократичну систему. В даний час сайт партії працює з перебоями.

Австрійська влада повідомила ЄС через систему раннього оповіщення Rapid Alert System (RAS) про кібератаку. Названу спробою втручання у вибори.

За запитом кількох партії будуть проведені збори Ради з нацбезпеки, на яких обговорять спроби протидії кібератакам…» ***(Вибори в Австрії: хакери зламали базу даних однієї з двох найбільших партій // Європейська правда (https://www.eurointegration.com.ua/news/2019/09/6/7100461/). 06.09.2019).***

***

«…За последние 14 месяцев киберпреступная группировка Tortoiseshell атаковала по меньшей мере 11 IT-компаний, большинство из которых расположены в Саудовской Аравии. По словам исследователей из компании Symantec, целью злоумышленников, предположительно, является компрометация клиентов компаний.

В некоторых случаях злоумышленникам удалось получить привилегии администратора, а также заразить несколько сотен компьютеров в попытках найти нужные им данные, такие как IP-адреса и информацию о сетевых подключениях.

Группировка взяла на вооружение вредоносное ПО под названием Backdoor.Syskit, разработанный в версиях на языках Delphi и .NET. С помощью данного бэкдора преступники могут загружать и выполнять дополнительные инструменты и команды. Для установки Backdoor.Syskit запускается с помощью

параметра «-install». Вредоносная программа собирает и отправляет IP-адреса, данные о названии и версии используемой ОС, а также Mac-адреса на C&C-сервер, используя URL-адрес в разделе реестра Sendvmd. Данные, отправляемые на C&C-сервер, шифруются в Base64.

По словам исследователей, данные операции могут быть частью атак по цепочке поставок, а конечной целью является получение доступа к сетям некоторых клиентов IT-провайдеров…» ***(Киберпреступная группировка Tortoiseshell атаковала саудовские IT-компании // SecurityLab.ru (https://www.securitylab.ru/news/501198.php). 18.09.2019).***

***

«Создавшая вирусы-вымогатели хакерская группа GandCrab осуществила кибератаки по всему миру, хотя ранее считалось, что она распалась. Эксперты компании Secureworks нашли след группы в новом вирусе-вымогателе под названием REvil и Sondinokibi.

Код этого вируса похож на предыдущий, также он содержит схожиие ошибки.

По словам директора отдела по противодействию кибератакам компании Дона Смита, возвращение хакеров их не удивило. Он пояснил, что хакерская деятельность приносила злоумышленникам хороший доход. Он предположил, что хакеры хотели отвлечь внимание от бренда GandCrab, чтобы продолжить работу с новым продуктом.

Группу GandCrab связывают с Россией. Предположительно, они продавали вирусы-вымогатели криминальным группировкам. У пострадавших зашифрововались файлы и с них требовали деньги за их расшифровку.» ***(Российская хакерская группа GandCrab возобновила кібератаки // Каспаров.Ru (http://www.kasparov.ru/material.php?id=5D8B3A0E01105). 25.09.2019).***

***

«Лаборатория Касперского» предупреждает о том, что кибергруппировка Lazarus начала применять ранее неизвестный шпионский инструмент, получивший название Dtrack.

Lazarus — это довольно необычная группа сетевых злоумышленников. Основным видом её деятельности является кибершпионаж, но она также замечена в проведении атак, нацеленных непосредственно на кражу денег, что обычно не свойственно подобным группировкам.

Новый инструмент Dtrack представляет собой ПО для удалённого администрирования. Этот зловред позволяет злоумышленникам выполнять на компьютере жертвы самые разнообразные операции.

К примеру, киберпреступники могут загружать и выгружать файлы, записывать нажатия клавиш клавиатуры, читать историю браузера и пр. В целом, Dtrack предоставляет возможность полностью контролировать заражённое устройство…» ***(Кибергруппировка Lazarus взяла на вооружение новый шпионский інструмент // Goodnews.ua (http://goodnews.ua/technologies/kibergruppirovka-lazarus-vzyala-na-vooruzhenie-novyj-shpionskij-instrument/). 26.09.2019).***

***

«…Исследователи безопасности из фирмы ESET обнаружили новое вредоносное ПО, которое использует службу фоновой интеллектуальной передачи данных Windows Background Intelligent Transfer Service (BITS) для кражи данных. По словам специалистов, вредонос может быть делом рук киберпреступной группировки Stealth Falcon.

Группировка Stealth Falcon, специализирующаяся на кибершпионаже, действует с 2012 года и нацелена на политических активистов и журналистов на Ближнем Востоке. В 2016 году некоммерческая организация Citizen Lab, занимающаяся вопросами безопасности и прав человека, опубликовала отчет о деятельности кибергруппировки. В январе 2019 года информагентство Reuters опубликовало отчет о расследовании в отношении подразделение под названием Project Raven, состоящего из сотрудников спецслужб ОАЭ и бывших агентов разведки США, у которого были схожие цели с Stealth Falcon.

В предыдущих атаках группировка Stealth Falcon использовала бэкдор, написанный на языке PowerShell, однако затем переключилась на новый инструмент, получивший название Win32/StealthFalcon (по классификации ESET). Вредоносная программа использует систему Windows BITS для связи и взаимодействия с C&C-сервером. Бэкдор позволяет преступникам загружать и запускать дополнительный код на зараженных системах, извлекать данные и отправлять на подконтрольные злоумышленникам удаленные серверы.

Для связи с удаленным сервером бэкдор использует не классические HTTP- или HTTPS-запросы, а трафик BITS. По мнению специалистов, таким образом злоумышленники обходят межсетевые экраны, поскольку, как правило, защитные средства не запрещают трафик BITS…» ***(Группировка Stealth Falcon эксплуатирует службу Windows BITS для кражи данных // SecurityLab.ru (https://www.securitylab.ru/news/500924.php). 10.08.2019).***

***

«Дослідники в області кібербезпеки виявили новий небезпечний троян, названий Joker. Як повідомляє BleepingComputer, він переховувався в 24 додатках, доступних в магазині Google Play. Загальна кількість завантажень заражених програм досягло 472 тисяч.

Троян призначений для довантаження шкідливого програмного забезпечення на заражені гаджети. Воно збирає інформацію про пристрій жертви, копіює її список контактів і текстові повідомлення. Отримані дані відправляються в зашифрованому вигляді на сервери зловмисників.

Також механізм виконує функцію клікера (імітує роботу користувача з рекламними сайтами) і «підписує» юзера на преміум-сервіси, використовуючи коди з SMS.

Небезпечна програма націлена на користувачів з певних країн: для цього вона автоматично звіряє мобільний код жертви зі вшитим «списком». Атака звернена на користувачів із США, Австралії, Великобританії, Франції, Німеччини, Індії.

Google вже видалив всі заражені програми з офіційного магазину додатків.» ***(Небезпечний вірус вкрав переписку сотень тисяч користувачів Android // "Коректно" (https://korektno.com.ua/nebezpechnyj-virus-vkrav-perepysku-soten-tysyach-korystuvachiv-android/56492/). 08.09.2019).***

***

«Согласно сообщению Bleeping Computer, активность шифровальщика TFlower, ориентированного на корпоративные сети, начала набирать обороты. Зловред объявился в конце июля и устанавливается в систему после хакерской атаки, нацеленной на получение доступа к службе удаленного рабочего стола.

В настоящее время TFlower раздается жертвам в виде файла chilli.exe и шифрует данные, используя алгоритм AES в режиме CBC. Он также умеет удалять теневые копии Windows, отключать средства восстановления Windows 10 и принудительно завершать процесс Outlook.exe, чтобы добраться до его файлов.

Процесс шифрования зловред отображает в консоли; а приступив к выполнению этой задачи, он соединяется с центром управления и обновляет свой статус. Отыскивая и преобразуя файлы жертвы, TFlower обходит стороной папки Windows и «Образцы музыки» (расположение — C:\Users\Public\Public Music\Sample Music).

Своего расширения для зашифрованных файлов у новобранца нет, он лишь добавляет в них маркер *tflower и ключ шифрования. Закончив свою работу, зловред рапортует об этом на C&C-сервер, а на зараженной машине появляются сообщения с требованием выкупа !_Notice_!.txt — во всех папках с измененными файлами и на рабочем столе. Для получения инструкций по восстановлению файлов вымогатели предлагают связаться с ними по электронной почте, используя адрес @protonmail.com или @tutanota.com.

Когда TFlower дебютировал, его повелители взимали 15 биткойнов за ключ расшифровки. С конца августа они перестали указывать размер выкупа в своих сообщениях. Вернуть файлы без уплаты выкупа в настоящее время невозможно: аналитики изучают вредоносный код, но уязвимостей в системе шифрования пока не обнаружили.

Доступные из Интернета RDP-службы как вектор атаки весьма популярны у распространителей программ-шифровальщиков, нацеленных на корпоративное окружение. Подобный способ заражения использовали SamSam, Scarabey, Matrix, Dharma, а в этом году — Nemty.» ***(Maxim Zaitsev. TFlower — еще один вымогатель, использующий RDP // Threatpost (https://threatpost.ru/tflower-ransomware-sneaks-into-networks-through-exposed-rdp-services/34129/). 18.09.2019).***

***

«После долгого отсутствия ботнет, построенный на основе троянской программы Emotet, вернулся на интернет-арену и начал генерировать спам, нацеленный на дальнейшее распространение зловреда. Вредоносные рассылки замечены в Германии, Польше, Великобритании, Италии и США.

Согласно наблюдениям, C&C-серверы Emotet три месяца никак не проявляли себя — по данным некоммерческой организации Spamhaus, их активность упала до нуля в начале июня. По всей видимости, операторы бот-сети решили вычистить

подставные боты ИБ-исследователей, проверить надежность инфраструктуры и пополнить запас взломанных сайтов для раздачи трояна, прежде чем идти в новое наступление. Командные серверы Emotet ожили лишь в конце августа; первые сообщения о новой спам-кампании появились в Twitter в понедельник, 16 сентября.

Комментируя новый всплеск активности ботнета для Bleeping Computer, эксперты Cofense Labs отметили, что они уже насчитали порядка 66 тыс. уникальных писем с привязкой к 30 тыс. вредоносных доменов в 385 TLD-зонах, а также 3362 различных отправителя. Злоумышленники используют в основном финансовые темы, маскируют свои сообщения под продолжение переписки и просят ознакомиться с информацией во вложении.

Как показал анализ, прикрепленный документ Microsoft Word содержит вредоносный макрос. Для его запуска получателю предлагают активировать соответствующую опцию, поясняя, что это якобы необходимо для подтверждения лицензионного соглашения с Microsoft — в противном случае 20 сентября текстовый редактор перестанет функционировать. Для пущей убедительности в ложное сообщение вставлен логотип Microsoft.

Если пользователь последует инструкциям злоумышленников, на его машину загрузится Emotet. На настоящий момент вредоносное вложение распознают около половины антивирусов из коллекции VirusTotal.

Однако расширение владений Emotet — не единственная цель новой спам-кампании. Обосновавшись на компьютере жертвы, зловред приводит еще одного трояна — Trickbot…» ***(Maxim Zaitsev. Emotet вновь пошел в наступление // Threatpost (https://threatpost.ru/emotet-botnet-is-back-with-new-spam-campaign/34107/). 17.09.2019).***

***

«Разработчики вымогателя Nemty продолжают активно работать над своим вредоносным ПО, стремясь повысить к нему интерес на подпольных форумах. Злоумышленники внесли изменения в характер его действий в системе жертвы. Теперь программа может не только шифровать файлы, но и завершать процессы и службы, мешающие выполнению этой задачи.

Впервые в поле зрения ИБ-специалистов Nemty попал в середине августа. За прошедший месяц вирусописатели успели выпустить новую версию зловреда под номером 1.4, в которой исправили найденные ошибки и добавили стоп-лист. Программа стала сворачивать свою деятельность, если целевая система находилась в России, Белоруссии, Казахстане, Таджикистане или Украине.

На днях ИБ-исследователь Виталий Кремез (Vitali Kremez) выяснил, что авторы шифровальщика, не меняя номер версии, внесли очередные коррективы. Пополнилось число географических регионов из стоп-листа: к ним добавились Азербайджан, Армения, Молдавия и Киргизия.

Однако основным нововведением стала функция, которая делает поведение Nemty гораздо более агрессивным. Добавленный разработчиками код может принудительно завершать запущенные в системе процессы, чтобы в числе прочих можно было шифровать и файлы, открытые жертвой. Основными целями зловреда являются девять программ и служб Windows, в том числе текстовые редакторы WordPad и Microsoft Word, приложение Microsoft Excel, почтовые клиенты

Microsoft Outlook и Mozilla Thunderbird, служба SQL и ПО виртуализации VirtualBox.

Как отмечает издание Bleeping Computer, два последних пункта в этом списке дают повод думать, что в качестве потенциальных жертв преступников больше всего интересуют крупные компании и корпорации.

Кроме того, по мнению автора Bleeping Computer Ионута Иласку (Ionut Ilascu), есть основания полагать, что злоумышленники не остановятся и в поиске наиболее эффективных путей доставки вредоноса в целевые системы. На текущий момент они уже протестировали заражение через уязвимые RDP-подключения, а также при помощи фальшивой страницы PayPal. Так как преступники уже пользовались одним из эксплойт-паков — RIG, использующим уязвимости в Internet Explorer, Java, Adobe Flash и Silverlight, — возможно, они прибегнут и к другим наборам эксплойтов.» ***(Maxim Zaitsev. Шифровальщик Nemty продолжает активно развиваться // Threatpost (https://threatpost.ru/shifrovalshhik-nemty-prodolzhaet-aktivno-razvivatsya/34097/). 16.09.2019).***

***

«Крупный американский поставщик полупроводников пострадал от вторжения шпионского трояна LokiBot. Злоумышленники доставили зловреда в инфраструктуру предприятия с помощью вредоносного письма с email-адреса одного из контрагентов предприятия.

Впервые LokiBot попал на радары ИБ-специалистов в 2015 году. Создатели трояна, которого не следует путать с одноименным Android-зловредом, обеспечили ему возможность красть информацию о зараженной системе, учетные данные электронных кошельков, идентификаторы из браузеров, почтовых клиентов и т. д. Программа также умеет отслеживать нажатия клавиш.

По мнению специалистов, в 2017 году троян украли у разработчиков. Нынешние операторы LokiBot нередко прибегают к оригинальным методам доставки, например встраивают зловред в PNG-файлы или ISO-образы…

Текущую кампанию обнаружили в конце августа. Она была построена на более традиционных методах — сотрудник организации получил вредоносное электронное письмо. Отправитель сообщения ссылался на отсутствие своего коллеги и просил срочно просмотреть файл во вложении. Там находился вредоносный дистрибутив, замаскированный под архив с документом.

Исследователи отмечают, что при внимательном изучении адресат письма мог заподозрить неладное. В частности, в тексте письма злоумышленники упоминали один документ, тогда как во вложении находился другой. Файл зловреда, скрывавшийся в архиве, назывался Dora Explorer Games. Это название отсылает к героине детского мультфильма Dora the Explorer и не очень подходит для целевой атаки на промышленную организацию. Тем не менее, получивший письмо сотрудник не обратил внимания на эти нестыковки и запустил зловреда. Последствия инцидента компания оставила в секрете…

По словам аналитиков, замеченный в атаке IP-адрес в июне уже использовался в похожей кампании. Предыдущие атаки были направлены на компанию German Bakery. Как и в новом случае, злоумышленники пытались

заставить корпоративных пользователей открыть вредоносное вложение, только тогда это был RTF-файл. Кроме того, письма, полученные сотрудниками German Bakery, были составлены на китайском.

Исследователи предполагают, что обе кампании организовала одна и та же группа, хотя говорить об этом с уверенностью не могут: выборка слишком мала. По их мнению, преступники могут использовать эту инфраструктуру для направленных атак.

«Злоумышленники используют социальную инженерию, — заключают эксперты. — Крайне важно, чтобы сотрудники организации знали о таком типе угроз, проходили регулярные тренинги и внезапные проверки безопасности»…» ***(Julia Glazova. LokiBot атаковал американскую промышленную компанию // Threatpost (https://threatpost.ru/lokibot-attacked-american-industrial-company/34065/). 12.09.2019).***

***

«…Предназначенный для добычи криптовалюты и кражи учетных данных ботнет Smominru (также известен как Ismo) начал распространяться с невероятной скоростью. По словам исследователей из команды Guardicore Labs, ботнет каждый месяц заражает более 90 тыс. компьютеров по всему миру.

Только в августе нынешнего года более 4,9 тыс. сетей были заражены вредоносом. Кампания затронула расположенные в США высшие учебные заведения, медицинские фирмы и даже компании, занимающиеся кибербезопасностью, а также системы в Китае, Тайване, России и Бразилии. Большинство зараженных машин работают под управлением Windows 7 и Windows Server 2008 и представляют собой небольшие серверы с 1-4 ядрами ЦП, в результате чего многие из них оказались непригодным для использования из-за чрезмерной нагрузки на ЦП в процессе майнинга.

Ботнет Smominru с 2017 года компрометирует системы на базе Windows с помощью эксплоита EternalBlue, созданного Агентством национальной безопасности США, но позже обнародованного киберпреступной группировкой Shadow Brokers. Червь был разработан для получения доступа к уязвимым системам методом брутфорса различных служб Windows, включая MS-SQL, RDP и Telnet.

Оказавшись на системе, Smominru устанавливает троянское вредоносное ПО и майнер криптовалюты, распространяется внутри сети, и использует возможности ЦП компьютеров жертв для майнинга Monero и отправки его на кошелек злоумышленников.

Злоумышленники создают множество бэкдоров на компьютере на разных этапах атаки. К ним относятся новые созданные пользователи, запланированные задачи, объекты WMI и службы, настроенные для запуска во время загрузки. Исследователям удалось получить доступ к одному из основных серверов злоумышленников, на котором хранится информация о жертвах и их украденные учетные данные.

«Логи злоумышленников описывают каждую зараженную систему, включая информацию внешних и внутренних IP-адресах, операционной системе и нагрузке на центральный процессор. Более того, злоумышленники пытаются собрать

информацию о запущенных процессах и украсть учетные данные, используя иструмент Mimikatz», — сообщают специалисты.

В отличие от предыдущих версий Smominru, новый вариант также удаляет следы заражения других киберпреступных группировок со скомпрометированных систем, а также блокирует TCP-порты (SMB, RPC), предотвращая проникновение конкурентов.» ***(Ботнет Smominru взламывает более 90 тыс. компьютеров каждый месяц // SecurityLab.ru (https://www.securitylab.ru/news/501196.php). 19.09.2019).***

***

«Вредоносное приложение Stockfoli маскируется под легитимную биржевую программу для macOS и похищает данные пользователей. Об этом сообщили ИБ-специалисты, изучившие два варианта зловреда GMERA, задействованные в кибератаках.

Исследователи обратили внимание на подозрительный shell-скрипт, выявленный антивирусным сканером. Программа не детектировалась как вредоносная, поскольку обращалась к внешним файлам с легитимными расширениями.

Повергнутый анализу образец представлял собой ZIP-архив, содержавший приложение Stockfoli.app и скрытый зашифрованный файл .app. Установочный комплект, идентифицированный как Trojan.MacOS.GMERA.A, включал в себя измененную копию легитимного приложения для биржевой торговли Stockfolio, подписанную сертификатом безопасности автора зловреда. После запуска программы пользователь видел интерфейс биржевого клиента, в то время как троян в фоновом режиме выполнял два скрипта.

Сценарий plugin собирал с компьютера жертвы имя пользователя, IP-адрес, сохраненные снимки экрана и файлы в ряде папок, а также системную информацию. Эти данные кодировались по стандарту Base64 и отправлялись на сервер злоумышленников…

Скрипт stock создавал копию папки appcode из дистрибутива зловреда и пытался расшифровать файл .app, содержавшийся в первоначальном архиве. Исследователям не удалось восстановить этот объект, поскольку веб-ресурс, на котором хранится AES-ключ, был недоступен. ИБ-специалисты предполагают, что файл предназначен для доставки дополнительной полезной нагрузки или реализации иных вредоносных функций.

Выполнив поиск по сертификату, использованному для подписи вредоносной программы, аналитики обнаружили еще один ее штамм — Trojan.MacOS.GMERA.B. Образец, способный создавать обратный шелл и подключаться к C&C каждые 10 000 секунд, загрузили на портал VirusTotal в июне этого года.

По мнению экспертов, в данный момент GMERA находится в стадии разработки, и авторы зловреда тестируют различные функции, позволяющие оставаться на инфицированном компьютере в течение длительного времени.

Представители Apple сообщили, что сертификат разработчика, которым пользовались злоумышленники, отозвали в июле этого года…» ***(Egor Nashilov.***

Инфостилер для macOS маскируется под трейдерскую программу // Threatpost (https://threatpost.ru/gmera-stockfoli-infostealer/34194/). 23.09.2019).

***

«Самым активным вымогательским ПО в настоящее время являются представители семейства STOP. К такому выводу пришел эксперт Bleeping Computer Лоуренс Абрамс (Lawrence Abrams), проанализировав жалобы пострадавших на форуме компании и на ИБ-сайте ID Ransomware.

В прошлом году на долю STOP и его вариаций приходилась половина детектов среди образцов, артефакты которых пользователи загружают на ID Ransomware в надежде получить помощь. В этом году вклад активно распространяемого зловреда заметно возрос. По словам Абрамса, идентификационный сервис ID Ransomware ежедневно собирает порядка 2,5 тыс. загрузок и в 60–70% случаев возвращает вердикт STOP.

Этот Windows-вымогатель проникает на компьютеры жертв в основном вместе с пиратским ПО или adware-пакетом, по ошибке скачанным с теневого сайта. По своему поведению STOP мало отличается от своих собратьев: он шифрует файлы, добавляет к результату расширение и оставляет на машине записку с требованием выкупа. Семейство выделяет лишь огромное количество модификаций, которые не перестают плодиться, — эксперты иногда регистрируют по 3-4 варианта в сутки, и тут же появляются тысячи новых жертв.

За два года своего присутствия в Сети авторы STOP обновляли его не менее 160 раз. При этом они обычно меняют используемое расширение и контактные email-адреса, иногда — имя файла с требованием выкупа. Злоумышленники также экспериментируют с разными криптоалгоритмами: вначале это был AES-256 в режиме CFB, в конце прошлого года появились варианты, оперирующие XOR, а затем STOP перешел на Salsa20 (с выходом модификации Djvu).

Универсального бесплатного декриптора для STOP до сих пор нет, однако крупнейшему специалисту по вымогательскому ПО Майклу Гиллеспи (Michael Gillespie) иногда удается оказать помощь жертвам. Созданная им утилита STOPDecryptor содержит ряд ключей расшифровки, которыми STOP пользуется в автономном режиме — когда C&C-сервер недоступен. К сожалению, в конце августа авторы зловреда опять сменили шифр, и исследователи пока не в состоянии помогать жертвам в прежнем объеме.

Новейший вариант шифровальщика использует расширение .karl и оставляет записку в файле _readme.txt, в которой требует 980 долларов за расшифровку, со скидкой 50% в течение первых трех суток после заражения. Идти на поводу у вымогателей эксперты не советуют: успех воодушевляет, и подобные зловреды будут множиться и впредь.» ***(Maxim Zaitsev. Шифровальщик STOP разгулялся // Threatpost (https://threatpost.ru/stop-family-outstrips-other-ransomware-actively-distributed-itw/34182/). 23.09.2019).***

***

«…Тысячи компьютеров на базе Windows по всему миру за последние несколько недель были заражены новым видом вредоносного ПО. Вредонос под названием Nodersok загружает и устанавливает копию инфраструктуры Node.js

для преобразования зараженных систем в прокси-серверы и проведения мошеннических операций.

Вредоносная программа, названная Nodersok (в отчете Microsoft) и Divergent (в отчете Cisco Talos), впервые была обнаружена летом нынешнего года и распространялась с помощью вредоносной рекламы, которая принудительно загружала файлы HTA (HTML Application) на компьютеры пользователей. Запуск HTA-файлов начинал многоэтапный процесс заражения с использованием скриптов Excel, JavaScript и PowerShell, которые в конечном итоге загружали и устанавливали вредоносное ПО Nodersok.

Сама вредоносная программа имеет несколько компонентов, включая PowerShell-модуль, который пытается отключить Защитника Windows и Центр обновления Windows, а также компонент для повышения привилегий вредоносного ПО до уровня SYSTEM. Но есть также два компонента, которые являются легитимными приложениями, а именно: WinDivert и Node.js. Первое представляет собой приложение для захвата и взаимодействия с сетевыми пакетами, а второе — известный инструмент для запуска JavaScript на web-серверах.

Легитимные приложения используются для запуска прокси-сервера SOCKS на зараженных хостах. Исследователи из компании Microsoft утверждают, что вредоносная программа превращает зараженные хосты в прокси-серверы для передачи вредоносного трафика. По словам специалистов из Cisco Talos, с другой стороны, прокси используются для мошеннических операций.

Так или иначе, создатели Nodersok могут в любой момент развернуть другие модули для выполнения дополнительных задач или даже запустить вымогательское ПО или банковские трояны.» ***(Новый вредонос Nodersok заразил тысячи компьютеров на базе Windows // SecurityLab.ru (https://www.securitylab.ru/news/501410.php). 27.09.2019).***

***

«…Исследователь Трой Марш (Troy Mursch) из компании Bad Packets Report обнаружил ботнет, который эксплуатирует уязвимость в одной из популярных программ для интернет-форумов vBulletin для защиты уязвимых серверов. Таким образом ботнет блокирует другим вредоносным программам доступ к серверам и наращивает собственную армию скомпрометированных серверов, не опасаясь конкуренции. Напомним, что ранее на этой неделе в Сети была опубликована информация и PoC-код для критической уязвимости в vBulletin.

Ботнет, взламывая уязвимый сервер с помощью эксплоита, использует его для изменения уязвимого файла исходного кода таким образом, чтобы требовался пароль для выполнения команд. Поскольку только злоумышленники знают пароль, они будут единственными, кто сможет выполнять команды на сервере.

Исследователь зафиксировал атаки из разных стран, причем Бразилия, Вьетнам и Индия являются тремя крупнейшими их источниками…

Пользователям версий vBulletin 5.5.2, 5.5.3 или 5.5.4 настоятельно рекомендуется установить официальные патчи vBulletin.» ***(Ботнет использует эксплоит для vBulletin для защиты от конкурентов // SecurityLab.ru (https://www.securitylab.ru/news/501406.php). 27.09.2019).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«…Управление по контролю за иностранными активами Министерства финансов США объявило о санкциях против трех киберпреступных группировок, предположительно спонсируемых государством Северной Кореи, которые совершали кибератаки на правительственные и частные организации по всему миру. В санкционный список попали три группировки, а именно Lazarus Group, Bluenoroff и Andariel.

«Министерство принимает меры против киберпреступных группировок, которые совершают атаки для финансовой поддержки программ незаконного вооружения», — заявил заместитель министра финансов по вопросам терроризма и финансовой разведки Сигал Манделькер (Sigal Mandelker).

Жертвами атак Lazarus Group в основном становились правительственные, военные, финансовые, промышленные, медийные, развлекательные и международные судоходные компании, а также критически важные инфраструктуры. Преступники прибегали к таким тактикам, как кибершпионаж, кража данных и финансовых средств и распространение вредоносного ПО. Группировку обвиняют в атаке с использованием вымогательского ПО WannaCry 2.0, которую США, Австралия, Канада, Новая Зеландия и Великобритания публично приписали Северной Корее в декабре 2017 года. Атака затронула по меньшей мере 150 стран по всему миру и привела к блокированию около 300 тыс. компьютеров.

В заявлении также упоминаются две подгруппы Lazarus Group — Bluenoroff и Andariel. Преступники из Bluenoroff осуществляли кибератаки на иностранные финансовые организации, похищая деньги, предположительно, для финансирования ракетных и ядерных программ Северной Кореи. Именно Bluenoroff эксперты приписывают нашумевший взлом серверов Sony Pictures Entertainment в 2014 году и похищение $81 млн у Центробанка Бангладеш.

Andariel – еще одна подгруппа Lazarus Group, которая организовывала атаки на иностранные компании, правительственные ведомства, частные корпорации и оборонную индустрию Южной Кореи с целью сбора информации и создания беспорядков. Andariel также несет ответственность за разработку и создание вредоносных программ для взлома сайтов online-покера и других азартных игр с целью кражи денег.

Преступная деятельность группировок также затронула и владельцев виртуальных активов. В период с января 2017-го по сентябрь 2018 года группировкам удалось украсть около $571 млн в криптовалюте у пяти бирж в Азии.» ***(США ввели санкции против группировок Lazarus, Bluenoroff, Andariel // SecurityLab.ru (https://www.securitylab.ru/news/501109.php). 16.09.2019).***

***

«Українець Федір Гладир у федеральному суді в американському Сіетлі визнав себе винним за обвинуваченнями в здійсненні кібератак та шахрайстві в обмін на зняття решти обвинувачень…

Тепер йому загрожує термін ув'язнення терміном до 25 років… В іншому разі час позбавлення волі міг би вимірюватися багатьма десятиліттями і навіть століттями, що фактично означало б довічне ув'язнення.

За словами адвоката українця Аркадія Буха, оголошення вироку Гладирю очікується у наступному 2020 році. Хакера разом із двома іншими українцями заарештували за звинуваченнями в участі в діяльності хакерської групи FIN7.

За даними влади США, організованою групою було викрадено близько 15 мільйонів кредитних і дебетових карт компаній Chipotle і Arby. Як заявили у ФБР, викрадені карти часто продавали на підпільних ринках.

Українця екстрадували з Німеччини до США у 2018 році, післячого він постав перед судом восени того ж року.

Другий обвинувачений був екстрадований з Іспанії громадянин України Андрій Колпаков постав 3 червня перед федеральним судом в американському Сіетлі, пише «Радіо Свобода».

Третій підозрюваний, Дмитро Федоров, зараз очікує на екстрадицію до Сполучених Штатів у Польщі…» ***(Звинувачений у кібератаках українець визнав себе винним — США // MediaSapiens (https://ms.detector.media/web/cybersecurity/zvinuvacheniy_u_kiberatakakh_ukrainets_viznav_sebe_vinnim_ssha/). 13.09.2019).***

***

«…Генеральная прокуратура Португалии обвинила основателя web-сайта Football Leaks (действующий по типу WikiLeaks) Руи Пинто (Rui Pinto) в 147 преступлениях. Согласно официальному заявлению, 75 преступлений были связаны с несанкционированным доступом к чужим данным, а 70 — с вымогательствами при отягчающих обстоятельствах и нарушениями приватности переписки…

Португальская полиция задержала Руи Пинто в Венгрии в январе нынешнего года по подозрению во взломе баз данных европейских футбольных клубов и дальнейшей публикации секретных документов на протяжении последних четырех лет на портале Football Leaks. Согласно обвинительному заключению, с начала 2015 года Руи Пинто получал «несанкционированный доступ к компьютерным системам и почтовым ящикам» с помощью «компьютерных программ и цифровых инструментов».

Пинту обвиняют в незаконном доступе к серверам Генеральной прокуратуры и документам по делам Tancos, BES, и операции Marques, а также данным лиссабонской юридической фирмы PLMJ, инвестиционного фонда Doyen Sports и португальской футбольная федерации.

По словам Руи Пинту, он создал Football Leaks с целью раскрыть коррупцию в спорте путем публикации конфиденциальных документов, включая «информацию о трансферах игроков и тренеров, соглашениях между спортивными организациями, спортивных контрактах и агентствах игроков». Благодаря опубликованным Football Leaks данным были зафиксированы серьезные нарушения

финансового фэйр-плей (свод этических и моральных законов) со стороны многих клубов, в частности, «ПСЖ» и «Манчестер Сити», что грозило им исключением их из Лиги чемпионов. Также обнародованные данные вызвали проблемы с налоговыми органами Испании у нападающего «Ювентуса» Криштиану Роналду.» ***(Основателя Football Leaks обвинили в 147 преступлениях // SecurityLab.ru (https://www.securitylab.ru/news/501301.php). 22.09.2019).***

***

«…В США двум молодым людям предъявлены обвинения в незаконном получении $10 млн от владельцев компьютеров. По данным прокуратуры южного округа Нью-Йорка, Романа Лейва (Romana Leyva) и Арифул Хакве (Ariful Haque) использовали классическую схему мошенничества с техподдержкой. Жертвам отображались поддельные уведомления о заражении их компьютеров несуществующим «вирусом» и предлагалась «помощь» в решении проблемы, естественно, за деньги.

Как правило, подобный вид мошенничества заключается в том, что в браузере появляется всплывающая реклама, замаскированная под системные уведомления. Согласно судебным документам , как минимум в одном случае жертвам отображалось уведомление с предупреждением, будто, перезагрузив компьютер или выключив компьютер, они причинят ему серьезный вред, в том числе вызовут полное удаление данных. В некоторых случаях для придания большей убедительности в уведомлениях незаконно использовался логотип известной технологической компании.

Хотя вышеупомянутая мошенническая схема хорошо известна пользователям, она по-прежнему очень эффективна. Вероятно, это связано с выбором жертв. По данным прокуратуры, жертвами Лейвы и Хакве становились пожилые люди, не разбирающиеся в компьютерах.

Помимо ненужной «починки», мошенники также подписывали пользователей на несуществующие платные сервисы. Иногда они даже выуживали у жертв банковские данные, мотивируя это тем, что компания закрывается и хочет вернуть клиентам деньги. Безусловно, никакие деньги не возвращались, а полученные данные использовались для кражи средств.

Мошенники были арестованы и в настоящее время дожидаются суда.» ***(Мошенничество с техподдержкой принесло двум американцам $10 млн // SecurityLab.ru (https://www.securitylab.ru/news/501270.php). 20.09.2019).***

***

«36-річний росіянин Андрій Тюрін зізнався в крадіжці даних у більш ніж 80 млн клієнтів JPMorgan Chase та інших фінансових компаній. Йому загрожує до 92 років тюремного ув'язнення за «привласнення сотень мільйонів доларів»

Росіянин Андрій Тюрін, який в минулому році був екстрадований з Грузії в США, визнав провину за пред'явленими йому звинуваченнями в кібератаках, спрямованих, зокрема, проти банку JPMorgan Chase, повідомляє РБК.

«Я визнав себе винним за цими пунктами, тому що я дійсно винен», – сказав він на засіданні суду в Нью-Йорку.

36-річному Тюріну інкримінуються зломи комп'ютерних систем фінансових структур, брокерських контор і ЗМІ, що спеціалізуються на публікації економічної інформації.

Росіянину пред'явили звинувачення за шістьма пунктами, в сукупності йому може загрожувати до 92 років тюремного ув'язнення.

Раніше повідомлялося, що хакерська група APT41 атакує підприємства у сферах охорони здоров'я, телекомунікацій, фінтех технологій, медіа, а також криптовалютні біржі.» Цю діяльність фінансує китайський уряд. ***(Екстрадований в США росіянин зізнався у кібератаках на банк JPMorgan // Західна інформаційна корпорація (https://zik.ua/news/2019/09/24/ekstradovanyy_v_ssha_rosiyanyn_ziznavsya_u_kiberatakah_na_bank_jpmorgan_1652801). 24.09.2019).***

***

Технічні аспекти кібербезпеки

Виявлені вразливості технічних засобів та програмного забезпечення

«Компанія Apple поставила під сумнів ступінь серйозності проблем із захистом смартфонів iPhone, виявлених компанією Google…

У Apple жорстко відреагували на звіт Google, в якому стверджувалось в кінці серпня, що її служба кібербезпеки викрила групу хакерів, які протягом двох років зламували iPhone. Жертвами щотижня ставали тисячі власників смартфонів виробництва Apple. Для зараження використовувалося кілька сайтів, при вході в які на iPhone користувача приховано встановлювалося шкідливе програмне забезпечення (ПЗ).

"По-перше, витончені атаки були зосереджені на дуже вузькому полі, а не широко розгорнуті на масованому використанні (вразливих місць в захисті) iPhone", — зазначила Apple. "Атака торкнулася менше дюжини веб-сайтів, які спеціалізуються на контенті, що стосується уйгурів", — додала компанія, маючи на увазі населення Синьцзян-Уйгурського автономного району (СУАР) в Китаї.

"По-друге, все свідчить на користь того, що ця атака на сайти тривала недовго — близько двох місяців, а не два роки, як стверджує Google", — зауважила Apple. Google в поширеній в п'ятницю заяві висловила впевненість у правильності висновків своїх експертів…» ***(Ілля Нежигай. У Apple поставили під сумнів висновки експертів Google про вразливість iPhone // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1823033-u-apple-postavili-pid-sumniv-visnovki-ekspertiv-google-pro-vrazlivist-iphone). 07.09.2019).***

***

«Исследователи кибербезопасности из команды SpiderLabs компании TrustWave обнаружили многочисленные уязвимости в некоторых моделях маршрутизаторов от производителей D-Link и Comba Telecom, которые связаны с небезопасным хранением учетных данных.

В общей сложности было обнаружено пять уязвимостей — две в модеме D-Link DSL, обычно устанавливаемом для подключения домашней сети к провайдеру, и три в нескольких устройствах от Comba Telecom. Эксплуатация данных уязвимостей позволяет злоумышленникам изменять настройки устройства, извлекать конфиденциальную информацию, выполнять атаки посредника (MitM), перенаправлять пользователя на фишинговые или вредоносные сайты и запускать множество других типов атак.

Первая уязвимость затрагивает двухдиапазонный беспроводной маршрутизатор D-Link DSL-2875AL и связана с хранением пароля для входа в систему устройства в виде открытого текста. Его может заполучить любой неавторизованный пользователь с доступом к IP-адресу для входа в панель управления. Вторая уязвимость затрагивает модели D-Link DSL-2875AL и DSL-2877AL и приводит к утечке учетных данных провайдера, которые используются маршрутизатором для аутентификации. Эти данные содержатся в исходном коде (HTML) страницы авторизации маршрутизатора.

Исследователи уведомили D-Link об уязвимостях в начале января нынешнего года, но компания выпустила исправленную версию прошивки только 6 сентября — за три дня до публикации PoC-кода.

Из трех уязвимостей в маршрутизаторах от Comba первая затрагивает контроллер доступа Wi-Fi Comba AC2400 и позволяет неавторизованному злоумышленнику получить доступ к MD5 хэшу пароля устройства через URL-адрес. Две другие уязвимости затрагивают точку доступа Wi-Fi Comba AP2600-I (версия A02,0202N00PD2). Одна из них также позволяет получить доступ к MD5 хэшу логина и пароля устройства через исходный код страницы авторизации. Вторая проблема связана с хранением учетных данных в открытом виде в базе данных SQLite.

Исследователи трижды пытались связаться с представителями Comba Telecom, однако компания не отреагировала на сообщения об обнаруженных уязвимостях. В итоге все уязвимости пока остаются не исправленными…» ***(Уязвимости в маршрутизаторах D-Link и Comba раскрывают пароли пользователей // SecurityLab.ru (https://www.securitylab.ru/news/500983.php). 11.08.2019).***

***

«Компания Facebook исправила две опасные уязвимости в серверном приложении HHVM. Их эксплуатация позволяет злоумышленникам удаленно получать конфиденциальную информацию или вызывать отказ в обслуживании системы путем загрузки вредоносного файла в формате JPEG.

HHVM (HipHop Virtual Machine) — высокопроизводительная виртуальная машина с открытым исходным кодом, разработанная Facebook для выполнения программ, написанных на языках PHP и Hack. HHVM использует подход компиляции «на лету» (just-in-time) для достижения превосходной

производительности кода Hack и PHP при сохранении гибкости разработки, которую обеспечивает язык PHP.

Поскольку серверное приложение HHVM является открытым, обе уязвимости затрагивают все web-сайты, использующие его, включая Wikipedia, Box и особенно те, которые позволяют пользователям загружать изображения на сервер.

Уязвимости (CVE-2019-11925 и CVE-2019-11926) связаны с возможным переполнения памяти в расширении GD при передаче специально сформированного недействительного JPEG-файла. При обработке маркеров блока JPEG APP12 и маркеров M_SOFx из заголовков JPEG в расширении GD возникают проблемы с проверкой границ, что позволяет злоумышленнику получить доступ к памяти за границами поля (out-of-bound).

Обе уязвимости затрагивают версии HHVM до 3.30.9, с 4.0.0 по 4.8.3, с 4.9.0 по 4.15.2, с 4.16.0 по 4.16.3, с 4.17.0 по 4.17.2, с 4.18.0 по 4.18.1, 4.19.0 и с 4.20.0 по 4.20.1. Разработчики HHVM исправили уязвимости, выпустив версии 4.21.0, 4.20.2, 4.19.1, 4.18.2, 4.17.3, 4.16.4, 4.15.3, 4.8.4 и 3.30.10.» ***(Facebook исправила две опасные уязвимости в серверах HHVM // SecurityLab.ru (https://www.securitylab.ru/news/500891.php). 09.08.2019).***

***

«Исследователь Уилл Дорманн (Will Dormann) из Координационного центра CERT обнаружил «слепую зону» системы Windows и антивирусных программ — образы диска в форматах VHD и VHDX. Как выяснил Дорманн, находящиеся внутри образов файлы не будут проверяться антивирусными программами, пока пользователь не смонтирует образ и не запустит их.

Формат файла VHD (виртуальный жесткий диск) может хранить содержимое жесткого диска. После подключения образ VHD-диска отображается в Windows как обычный жесткий диск, физически подключенный к системе. Образы VHDX (Virtual Hard Disk v2) функционально эквивалентны VHD, но включают более современные функции, такие как поддержка больших размеров и изменение размера диска.

Исследователь смог найти несколько способов аварийного завершения работы Windows в результате подключения поврежденного диска. Файлы VHD и VHDX устраняют необходимость физического доступа к системе. Пользователю достаточно дважды кликнуть на файл VHD или VHDX со специально сформированной файловой системой, что может привести к завершению работы системы.

Операционная система Windows умеет отличать степень опасности данных на основе их источника. Для этого система обозначает файлы ярлыком Mark of the Web (MOTW), выдавая им лишь ограниченный доступ к ресурсам компьютера. Пользователи в данной ситуации видят специальное предупреждение о потенциальном риске запуска файлов, скачанных из интернета. Ярлык MOTW присваивается всем загруженным из интернета файлам, включая архивы.

Однако данный принцип не распространяется на файлы образов VHD и VHDX, несмотря на их сходство с ZIP-архивами. Любой находящийся внутри VHD

и VHDX файл не будет расцениваться Windows в качестве потенциальной угрозы, как это происходит с другими типами файлов, загруженных из Сети.

Дорманн не нашел ни одного антивирусного ПО, способного сканировать файлы, содержащиеся в VHD или VHDX. Если содержимое файлов VHD и VHDX не сканируется решениями безопасности электронной почты и web-шлюзов, у системы нет шансов обнаружить вредоносные программы, содержащихся в файлах VHD или VHDX.

В целях безопасности исследователь рекомендует блокировать файлы VHD и VHDX на почтовых шлюзах и отменить регистрацию расширений данных файлов в «Проводнике» Windows…» ***(Образы VHD и VHDX можно использовать для обхода антивирусов // SecurityLab.ru (https://www.securitylab.ru/news/500886.php). 09.08.2019).***

***

«В популярном ПО для почтовых серверов Exim обнаружена критическая уязвимость (CVE-2019-15846), позволяющая удаленно выполнить код и получить доступ к системе с правами суперпользователя. Исправление для уязвимости, а также подробное ее описание будет опубликовано в пятницу, 6 сентября. С целью предотвращения атак с использованием CVE-2019-15846 рекомендуется обновить Exim до версии 4.92.2 или более поздней.

Проэксплуатировать уязвимость может авторизованный пользователь или злоумышленник, находящийся в одной сети с уязвимым устройством. Также ее можно проэксплуатировать удаленно, если сервер подключен к интернету.

Как сообщает один из разработчиков Exim Хайко Шлиттерман (Heiko Schlitterman), ему и его коллегам стало известно об уязвимости 3 сентября. На следующий день подписчики рассылки получили уведомление о готовящемся патче, который будет выпущен 6 сентября.

По словам Шлиттермана, пока что полноценного рабочего эксплоита для уязвимости не существует. Однако уже есть примитивный PoC-эксплоит, в связи с чем администраторам настоятельно рекомендуется установить обновление как можно скорее.

Патч является самым крупным обновлением с момента выхода версии Exim 4.92.1, выпущенной в июле нынешнего года. Обновление также исправляло критическую уязвимость (CVE-2019-13917), позволявшую удаленно выполнять код с правами суперпользователя при нестандартных настройках конфигурации.» ***(В Exim обнаружена вторая за два месяца критическая уязвимость // SecurityLab.ru (https://www.securitylab.ru/news/500863.php). 06.08.2019).***

***

«Исследователи из 9sg Security обнаружили критические уязвимости в двух компонентах программного обеспечения, разработанного поставщиком решений для промышленной автоматизации EZAutomation. Их эксплуатация позволяет злоумышленнику выполнить удаленный код.

Одна из уязвимостей (CVE-2019-13518) связана с переполнением буфера в стеке. Она затрагивает редактор человеко-машинного интерфейса EZTouch Editor версии 2.1.0 и ниже. Эксплуатация уязвимости позволяет злоумышленнику

выполнить произвольный код в контексте текущего процесса, если пользователь откроет специально сформированный файл проекта EZP.

Вторая уязвимость (CVE-2019-13522) связана с повреждением памяти и затрагивает решение EZ PLC Editor (версии 1.8.41 и более ранние) — инструмент программирования для программируемых логических контроллеров. Эксплуатация уязвимости также позволяет злоумышленнику выполнить произвольный код. Для этого он должен убедить пользователя открыть вредоносный файл проекта EZC.

Уязвимости были исправлены в EZPLC Editor версии 1.9.0 и EZTouch Editor версии 2.2.0.» ***(В программном обеспечении от EZAutomation обнаружены критические уязвимости // SecurityLab.ru (https://www.securitylab.ru/news/500852.php). 06.09.2019).***

***

«Представник компанії «Гугл» підтвердив наявність вразливостей в сервісах Gmail і «Гугл Календарі», які ще у 2017 році були виявлені дослідниками з Black Hills Information Security.

У повідомленні, опублікованому на форум користувачів, говориться, що співробітники «Гугла» «посилено працюють над вирішенням проблеми». Про це повідомляє Forbes. Видання пише, що компанія фактично визнала, що ці сервіси справді можна зламати.

Зловмисники користуються тим, що хто завгодно може призначити зустріч у «Календарі» з іншим користувачем. При цьому на пошту прийде лист, в якому потрібно підтвердити участь або відмовитися. У повідомлення може бути зашита шкідлива посилання.

Ще у червні 2019 року представники компанії заперечували проблему, яка зачіпає мінімум 1 млрд користувачів цих сервісів.

Проте недавно автору статті прес-секретар «Гугла» відповів:

«Загальні положення та умови «Гугла» та політика щодо продуктів забороняють поширювати шкідливий вміст на наших сервісах, і ми старанно працюємо над запобіганням та попередженням протидії зловживанням».

У цій заяві говорилося, що у компанії пропонують «заходи безпеки для користувачів, попереджаючи їх про відомі шкідливі URL-адреси через фільтри безпечного перегляду Google Chrome»…

Як зловмисники можуть використати «Гугл-календар»? Наприклад, коли запрошення календаря надсилається користувачеві, на його смартфоні з'являється спливаюче повідомлення. Автори злочинних схем створюють власні повідомлення, у які включають шкідливе посилання, спекулюючи на довірі, яку користувач має до сервісу.

Ці посилання можуть містити фейкові онлайн-опитування чи анкетування, які збирають дані користувача або стимулюють його вказати дані банківського рахунку чи кредитної картки…» ***(«Гугл» визнала вразливість Gmail і «Гугл Календаря» до шахрайських дій // MediaSapiens (https://ms.detector.media/web/cybersecurity/gugl_viznala_vrazlivist_gmail_i_gugl_kalendarya_do_shakhrayskikh_diy/). 10.09.2019).***

***

«Независимый ИБ-специалист под ником ZHacker13 обнаружил уязвимость соцсети Instagram, которая позволяла автоматически собирать данные ее пользователей. Представители сервиса несколько недель не могли устранить угрозу и начали активно работать над решением только после обращения журналиста Forbes.

Как рассказал исследователь, его схема атаки построена на багах служб авторизации и импорта контактов в Instagram. С ее помощью можно собрать из разрозненных источников в единую базу настоящие имена пользователей, данные их аккаунтов, полные телефонные номера…

На первом этапе злоумышленнику необходимо найти телефонные номера, к которым привязаны реальные учетные записи. Их можно выявить, проставляя разные комбинации цифр в форму авторизации Instagram — по результатам запроса на этой странице сразу станет понятно, есть ли тот или иной номер в базах сервиса.

Процесс можно легко автоматизировать, собирая ежедневно более 1000 актуальных номеров телефонов. ZHacker13 также уточнил, что при использовании параллельно работающих ботов эта цифра увеличивается практически до бесконечности.

Имея на руках списки номеров, злоумышленник связывает их с соответствующими учетными записями через систему импорта контактов. Как пояснил исследователь, Instagram предлагает каждому новому пользователю синхронизировать контакты, чтобы найти знакомых, которые уже зарегистрированы в соцсети. Если сервис обращается к настоящему списку контактов, по предлагаемому списку невозможно установить, какой номер привязан к той или иной учетной записи. Однако в сценарии ZHacker13 предлагаемая записная книжка содержала всего один телефон, поэтому злоумышленник мог установить параллель и собрать данные в базу.

Разработчики Instagram разрешают каждому пользователю ежедневно отправлять не более трех запросов на синхронизацию аккаунтов. Использование множества ботов позволяет обойти и этот лимит, после чего единственное, что ограничивает аппетит злоумышленников — это доступные вычислительные мощности. По расчетам ZHacker13, его метод позволял в приемлемые сроки и без значительных затрат собрать информацию миллионов пользователей…

В начале августа эксперт сообщил о своей находке компании Facebook, которая владеет Instagram. Те заявили, что не считают серьезной угрозой возможность уточнить, привязан ли к какой-либо учетной записи конкретный телефон или электронный адрес. В то же время разработчики признали, что если уязвимость позволяет узнать контакты конкретного пользователя, то она может представлять опасность.

Тем не менее, Facebook отказала ZHacker13 в вознаграждении в рамках программы по поиску багов. В компании сказали, что ее собственные специалисты ранее обнаружили проблему и уже работают над ее решением. Когда спустя несколько недель эксперт обнаружил, что уязвимость все еще не закрыта, он продемонстрировал работоспособность PoC-атаки колумнисту Forbes.

Получив запрос журналиста, сотрудники Facebook пересмотрели свою позицию о выплате вознаграждения и попросили повременить с публикацией до тех пор, пока разработчики не исправят ошибку.

Репортер Forbes отметил, что находка указывает на более серьезные риски, нежели уязвимость отдельного веб-сервиса. По его мнению, в будущем можно ждать новых кибератак с использованием пользовательских телефонных номеров, поскольку они все чаще используются для авторизации в приложениях и сервисах…» ***(Dmitry Nazarov. Instagram устранил угрозу приватности пользователей // Threatpost (https://threatpost.ru/instagram-fixed-privacy-flaw-in-its-services/34101/). 16.09.2019).***

***

«Длинный список проблем, устраняемых сентябрьским набором патчей для продуктов Microsoft, содержит две уязвимости нулевого дня, уже взятые на вооружение злоумышленниками. Им присвоены идентификаторы CVE-2019-1214 и CVE-2019-1215; первая найдена в Windows-драйвере Common Log File System (clfs.sys), вторая — в драйвере режима ядра Winsock IFS (ws2ifsl.sys). Оба бага позволяют атакующему повысить привилегии в системе.

«В обоих случаях причиной уязвимости является некорректная обработка драйвером объектов в памяти, — пишет старший разработчик-исследователь в Tenable Сатнам Наранг (Satnam Narang), отвечая на запрос Threatpost. — Авторы атак используют баги повышения привилегий после получения доступа к системе, чтобы выполнить в ней код с расширенными правами».

Дастин Чайлдс (Dustin Childs) из проекта Zero-Day Initiative компании Trend Micro рекомендует назначить заплатке для CVE-2019-1215 высший приоритет. «Эксплуатация этой уязвимости позволит злоумышленнику поднять уровень доступа с пользовательского до административного, — поясняет эксперт, разбирая сентябрьский «вторник патчей». — Microsoft признала, что злоумышленники уже активно опробуют эксплойт как на новейших, так и на более старых поддерживаемых ОС. Примечательно, что вредоносное ПО прежде уже пыталось атаковать этот файл. Подобные случаи упоминались еще в 2007 году, что неудивительно: зловреды зачастую бывают нацелены на Windows-службы низкого уровня».

Уязвимости CVE-2019-1214, со слов Microsoft, новейшие ОС не подвержены. «Хороший повод напомнить, что меньше чем через полгода Windows 7 будет снята с поддержки, а значит, в феврале уже не будет патчей для подобных багов, — комментирует Чайлдс. — Латайте системы, а после этого займитесь подготовкой апгрейда».

Суммарно Microsoft устранила в своих продуктах 79 уязвимостей, в том числе 17 критических. Из последних эксперты советуют обратить внимание на четыре бага в клиенте удаленного рабочего стола (CVE-2019-1290, CVE-2019-1291, CVE-2019-0787, CVE-2019-0788). Они дополняют коллекцию, в которую уже входят пропатченный в мае BlueKeep и августовские уязвимости, получившие известность как DejaBlue.

«В отличие от BlueKeep и DejaBlue, где атака нацелена на уязвимый сервер удаленного рабочего стола, эти уязвимости требуют, чтобы атакующий убедил

пользователя подключиться к вредоносному серверу удаленного рабочего стола, — поясняет Наранг. — Автор атаки может также взломать уязвимый сервер, разместить на нем вредоносный код и ждать, когда пользователи начнут устанавливать соединение».

Девять критических багов предполагают атаки через браузер. В равной мере опасна уязвимость в Azure DevOps (ADO) и Team Foundation Server (TFS) (CVE-2019-1306), позволяющая выполнить на сервере код на правах законного пользователя ADO или TFS. «Автору атаки понадобится разрешение на загрузку файла в целевое хранилище, — пишет Чайлдс. — В случае успеха ему удастся выполнить код, как только уязвимый сервер проиндексирует этот файл».

Три критические уязвимости в службе подключения к бизнес-данным Microsoft SharePoint связаны с ошибками десериализации. В своей блог-записи Чайлдс уделил внимание лишь одной из них, CVE-2019-1257. «В этом случае автор атаки сможет исполнить свой код в контексте пользователя пула приложений, загрузив на уязвимый сервер специально созданный пакет приложения SharePoint, — отметил исследователь. — Обычно для загрузки такого пакета требуется авторизация, но можно попытаться включить анонимный доступ».

Уязвимость CVE-2019-1280 в Windows связана с обработкой lnk-файлов. «Злоумышленник может предложить пользователю съемный носитель или удаленный совместно используемый ресурс, содержащий вредоносный файл .LNK и ассоциированный с ним вредоносный бинарный код, — сказано в бюллетене Microsoft. — Когда пользователь откроет носитель (или удаленную общую папку) в Проводнике Windows или любом другом приложении, выполняющем парсинг lnk-файлов, вредоносный бинарник выполнит код в целевой системе по выбору атакующего».

Разработчик также обновил служебный стек для всех операционных систем (ADV990001). «Обычно такие обновления выходят для одного или двух выпусков Windows, но на этот раз затронуты все ОС Windows, — заявил директор по управлению продукцией Ivanti Крис Гётль (Chris Goettl) в комментарии для Threatpost. — Подобные обновления оцениваются как критические, однако уязвимостей они не устраняют и никогда не входят в состав накопительных обновлений. В то же время они критически важны для системы обновления, встроенной в ОС Microsoft, а значит, для всей линейки грядут изменения, и в какой-то момент обновление Windows станет невозможным без обновления пакета Servicing Stack». ***(Tara Seals. Microsoft закрыла две уязвимости, используемые в атаках // Threatpost (https://threatpost.ru/microsoft-addresses-two-zero-days-under-active-attack/34061/). 12.09.2019).***

***

«Компания выпустила экстренные патчи для уязвимостей в Internet Explorer и Microsoft Defender.

Компания Microsoft выпустила экстренные внеплановые обновления, исправляющие две уязвимости, в том числе уязвимость нулевого дня.

Уязвимость нулевого дня в Internet Explorer (CVE-2019-1367) позволяет атакующему удаленно выполнить на системе произвольный код и повысить свои привилегии до уровня текущего пользователя. Как сообщается в уведомлении

Microsoft, причиной проблемы является то, как скриптовый движок (инструмент для реализации скриптов в различных скриптовых языках) обрабатывает объекты в памяти браузера.

Уязвимость приводит к повреждению памяти, чем может воспользоваться злоумышленник и выполнить произвольный код в контексте текущего пользователя. Если текущий пользователь обладает правами администратора, то атакующий может получить полный контроль над системой. В таком случае у него появится возможность устанавливать программы, просматривать, модифицировать и удалять данные, а также создавать новые учетные записи.

Уязвимость можно проэксплуатировать удаленно через интернет. Для этого злоумышленнику нужно создать особым образом настроенный сайт, способный проэксплуатировать уязвимость через браузер, и заманить на него жертву. Проблема затрагивает версии Internet Explorer 9, 10 и 11.

Уязвимость уже эксплуатируется во вредоносных кампаниях, однако Microsoft пока не раскрывает никакой информации о них.

Вторая проблема представляет собой уязвимость отказа в обслуживании (CVE-2019-1255) в Microsoft Defender. Она затрагивает версии Microsoft Malware Protection Engine до 1.1.16300.1 включительно и была исправлена в версии 1.1.16300.2.

Уязвимость позволяет блокировать выполнение действительными учетными записями легитимных системных кодов. Для ее эксплуатации злоумышленник сначала должен выполнить код на атакуемой системе. Исправление для проблемы будет установлено автоматически в течение 48 часов с момента выхода.» ***(Microsoft в срочном порядке исправила уязвимость нулевого дня в IE // SecurityLab.ru (https://www.securitylab.ru/news/501329.php). 24.09.2019).***

***

«…Компания Atlassian выпустила обновления для программного обеспечения Jira Service Desk и Jira Service Desk Data Center, исправляющее опасные уязвимости. Они могут быть проэксплуатированы для раскрытия информации или удаленного выполнения кода.

Одна из проблем (CVE-2019-14994) затрагивает ПО Jira Service Desk и Jira Service Desk Data Center и представляет собой опасную уязвимость типа path traversal (некорректные ограничения путей для каталогов, подмена пути). По словам исследователя безопасности Сэма Карри (Sam Curry), ограничения способен обойти любой пользователь с доступом к порталу, как клиент, так и сотрудник. Эксплуатация позволяет злоумышленнику просматривать все запросы во всех проектах Jira, содержащихся в уязвимых установках, включая Jira Service Desk, Jira Core и Jira Software.

Поисковые запросы выявили 25 тыс. организаций по всему миру в сфере здравоохранения, государственного управления, образования и промышленности, которые используют данный web-портал.

Уязвимости затрагивают версии продуктов Jira Service Desk и Jira Service Desk Data Center 3.9.16 и младше, с 3.10.0 по 3.16.8, с 4.0.0 по 4.1.3, с 4.2.0 по 4.2.5, с 4.3.0 по 4.3. 4, и 4.4.0. Проблема CVE-2019-14994 была исправлена в версиях 3.9.16, 3.16.8, 4.1.3, 4.2.5, 4.3.4 и 4.4.1.

В отдельном предупреждении Atlassian сообщила об уязвимости (CVE-2019-15001) типа template injection (внедрение шаблона) в плагине Importer. Она может быть проэксплуатирована злоумышленником с доступом к группе JIRA Administrators и позволяет удаленно выполнять код на системах с уязвимой версией Jira Server или Data Center.

Уязвимость затрагивает версии Jira Server и Jira Data Center с 7.0.10 до 7.6.16 (исправлено в 7.6.16), с 7.7.0 до 7.13.8 (исправлено в 7.13.8), от 8.0.0 до 8.1.3 (исправлено в 8.1.3), с 8.2.0 до 8.2.5 (исправлено в 8.2.5), с 8.3.0 до 8.3.4 (исправлено в 8.3.4), с 8.4.0 до 8.4.1 (исправлено в 8.4.1)…» ***(В ПО Jira Server и Service Desk исправлены опасные уязвимости // SecurityLab.ru (https://www.securitylab.ru/news/501318.php). 23.09.2019).***

***

«…Разработчики менеджера паролей LastPass на прошлой неделе исправили уязвимость, раскрывающую пароли от ранее посещенных сайтов. Проблему обнаружил исследователь безопасности Тэвис Орманди (Tavis Ormandy), подробно описавший ее после того, как разработчики LastPass выпустили исправление.

Поскольку атака основывается на выполнении JavaScript-кода и не требует участия пользователя, уязвимость считается опасной и потенциально эксплуатируемой. Злоумышленник может заманить жертву на вредоносную web-страницу и через уязвимость получить пароли, введенные на предыдущих сайтах.

Проблема затрагивает только расширения LastPass для Chrome и Opera и уже исправлена в версии 4.33.0. Пользователям, отключившим механизм автоматического обновления менеджера паролей, рекомендуется как можно скорее установить патч вручную, поскольку публикация Орманди содержит все сведения, необходимые для эксплуатации уязвимости.

Никаких свидетельств использования уязвимости в реальных атаках не обнаружено. Поскольку проблема была успешно исправлена, нет никаких причин отказываться от LastPass. Хранить учетные данные в менеджерах паролей намного надежнее, чем в браузерах, откуда злоумышленники могут с легкостью их изъять с помощью специальных инструментов и вредоносного ПО.» ***(Уязвимость в LastPass раскрывает пароли от ранее посещенных сайтов // SecurityLab.ru (https://www.securitylab.ru/news/501141.php). 17.09.2019).***

***

«Корпорація Microsoft відреагувала на знайдену експертом Threat Analysis Group з кібербезпеки Клеманом Лецинем з Google уразливість в Internet Explorer і офіційно підтвердила, що браузер становить загрозу для користувачів Windows 7, Windows 8.1 і Windows 10. Втім, ніхто і не сумнівався, так як цей браузер був спочатку провальною ідеєю з-за конкуренції. Приміром, Google Chrome і Mozilla Firefox у всьому краще браузера від Microsoft.

Якщо комп'ютером користується людина з правами адміністратора, хакер може забезпечити собі повний доступ до встановлення програм, перегляду і видалення даних, а також створенню нових користувачів у тому числі і з правами адміністратора. Звичайно ж, робиться це без відома користувача, так що хакери можуть зламувати ПК непомітно.

Втім, компанія поки нічого не може зробити, і рекомендує переходити на Microsoft Edge, який нітрохи не краще застарілого браузера…» ***(Microsoft визнала наявність вразливостей в браузері Windows 10: мільйони користувачів під загрозою // Знай.ua (https://techno.znaj.ua/264849-microsoft-viznala-nayavnist-vrazlivostey-v-brauzeri-windows-10-milyoni-koristuvachiv-pid-zagrozoyu). 25.09.2019).***

***

«Разработчики Microsoft выпустили экстренные обновления для Internet Explorer и Microsoft Defender (ранее Windows Defender — Защитник Windows). Браузер содержит критическую уязвимость, уже используемую в атаках, поэтому его рекомендуется залатать как можно скорее.

Новая проблема в IE (CVE-2019-1367) открывает возможность для выполнения вредоносного кода в системе с правами текущего пользователя. Баг CVE-2019-1255 в Microsoft Defender менее опасен — он позволяет вызвать состояние отказа в обслуживании…

Согласно бюллетеню Microsoft, уязвимость нулевого дня в IE вызвана неправильной обработкой объектов в памяти скриптовым движком браузера. В результате может возникнуть ошибка нарушения целостности памяти, используя которую, автор атаки сможет выполнить произвольный код в контексте текущего пользователя.

«Если пользователь вошел в систему с привилегиями администратора, успешный эксплойт позволит атакующему захватить контроль над уязвимой системой, — поясняют разработчики. — В итоге он сможет устанавливать программы, просматривать, изменять и удалять данные или создавать новые аккаунты с полным набором прав».

Эксплуатация в данном случае осуществляется удаленно, в том числе через вредоносный сайт, на который пользователя можно заманить, например, с помощью поддельного письма. Наличие уязвимости подтверждено для Internet Explorer версий 9, 10 и 11. Заплатка для всех Windows 10 вышла в виде целевых обновлений, для Windows 7 и 8.1 — в составе накопительного обновления браузера; устанавливать ее придется вручную — или ждать октябрьского «вторника патчей», рискуя попасть под атаку.

Об использовании нового бага 0-day злоумышленниками Microsoft сообщил аналитик из Google Клеман Лесинь (Clément Lecigne). Национальная Группа быстрого реагирования на киберинциденты в США (US-CERT) призывает всех пользователей применить патч в кратчайшие сроки.

Уязвимость в утилите Microsoft Defender привязана к движку Microsoft Malware Protection Engine, который также используется в других антивирусных решениях компании. Согласно бюллетеню, проблема проявляется при обработке файлов и позволяет «воспрепятствовать исполнению легитимных системных бинарных кодов под легитимным аккаунтом». Воспользоваться недочетом можно лишь при наличии доступа к системе и возможности выполнить код.

Уязвимости CVE-2019-1255 подвержены все версии Microsoft Malware Protection Engine до 1.1.16300.1 включительно; ошибка исправлена в релизе 1.1.16400.2. При дефолтных настройках обновление антивирусного ПО будет произведено автоматически…» ***(Lindsey O'Donnell. Внеочередной патч для IE***

устраняет уязвимость 0-day // Threatpost (https://threatpost.ru/microsoft-internet-explorer-zero-day-flaw-addressed-in-out-of-band-security-update/34206/). 24.09.2019).

***

«Специалисты по кибербезопасности обнаружили новый способ взломать страницу в Instagram.

Сначала мошенники присылают на почту письмо, в котором говорится, что страница в соцсети будет заблокирована спустя 24 часа из-за нарушения юзером права интеллектуальной собственности.

Чтобы этого не произошло, можно якобы оспаривать нарушение с помощью активной ссылки под названием Copyright Objection Form, размещенной в письме.

При нажатии на нее открывается ненастоящее окно соцсети, где пользователь сам вводит все свои данные, которые получают злоумышленники.» ***(Эксперты нашли новый способ взломать аккаунт в Instagram // Goodnews.ua (http://goodnews.ua/technologies/eksperty-nashli-novyj-sposob-vzlomat-akkaunt-v-instagram/). 27.09.2019).***

***

«Есть много способов того, как оставаться в курсе самых последних событий на интересующие вас темы… у Google есть свой метод — система Google Alerts (или, если угодно, Google Оповещения), предоставляющая доступ к массе свежего информационного контента. И хакеры недавно научились пользоваться ей в своих корыстных целях.

Google Alerts, в отличие от обычных каналов или служб подписки, позволяет отслеживать интересующие вас темы на основе выбранных ключевых слов. Это упрощает взаимодействие с источниками информации и делает выборку не по профильным ресурсам, а именно по темам, которые вам интересны…

В то время как пользователи уже долгое время пользуются системой Google Alerts, похоже, что хакеры и мошенники нашли в ней неприятную лазейку. Используя тактику подмены ключевых слов, ассоциированных с ресурсом, они научились выводить эти самые ресурсы в топ выдачи Google Alerts, тем самым заставляя ничего не подозревающих пользователей переходить по ссылкам и получать в ответ не полезную информацию, а вредоносное ПО.

Как это работает? Говоря простыми словами, вас интересуют, скажем, смартфоны. Хакеры создают ресурсы, которые алгоритмами поисковой системы определяются как те, где есть самая свежая информация о смартфонах. Хотя на самом деле там ее может и не быть…

…аналитики, занимающиеся вопросами кибербезопасности, из компании BleepingComputer, которые и обнаружили уязвимость, решили проверить, какие опасности несет недавно найденная «дыра»… Специалисты просто настроили работу таким образом, чтобы она производила более глубокий поиск на сайтах, содержащих, так называемые, «ransomware» (вирусы-вымогатели). Это разновидность вирусов, которые за свое удаление просят у пользователей денег.

Каково же было удивление сотрудников BleepingComputer, когда они обнаружили посредством простого поиска сотни сайтов, содержащих вирусы-вымогатели, и при этом маскирующиеся под «обычные». При этом поток проходящего через них трафика был довольно высок. По понятным причинам, эти

самые ресурсы не раскрываются. Но и это еще не все. Google Alerts выдал также массу ссылок на сайты с «дешифровщиками», предлагающими за бесплатно избавиться от ransomware. Но эти дешифровщики, как вы наверно уже догадались, тоже оказались ни чем иным, как вирусами. По сообщению BleepingComputer, информация уже передана в Google и специалисты поискового гиганта должны будут разобраться в ситуации «в самое ближайшее время». ***(Хакеры начали использовать популярный сервис Google для рассылки вредоносного кода // Goodnews.ua (http://goodnews.ua/technologies/xakery-nachali-ispolzovat-populyarnyj-servis-google-dlya-rassylki-vredonosnogo-koda/). 27.09.2019).***

***

«…Cisco обнаружила в своем ПО Cisco IOS и IOS XE более десятка опасных уязвимостей, в том числе уязвимость, затрагивающую маршрутизаторы промышленного класса. Компания также рекомендовала пользователям отключить в IOS функцию трассировки маршрутов L2, для уязвимости в которой уже опубликован эксплоит.

Cisco раскрыла подробности об уязвимостях в рамках планового исправления проблем безопасности в Cisco IOS и IOS XE, проходящего два раза в год (в каждую четвертую среду марта и сентября). Нынешнее обновление включает 12 уведомлений безопасности для 13 отдельных уязвимостей высокой опасности. Проблемы позволяют злоумышленникам получать неавторизованный доступ к устройству, внедрять команды, истощать ресурсы устройства и вызывать отказ в обслуживании.

Ни одна уязвимость не отмечена в бюллетенях как критическая. Тем не менее, обнаруженная в среде приложения IOx для IOS проблема с идентификатором CVE-2019-12648 получила по системе оценивания опасности уязвимостей CVSS 3.0 оценку 9,9 из максимальных 10. Она затрагивает маршрутизаторы Cisco промышленного класса серий 800 и 1000.

Как правило, уязвимости, получившие столь высокую оценку по системе CVSS, считаются критическими. Однако в данном случае CVE-2019-12648 не является таковой, поскольку затрагивает лишь гостевую ОС на виртуальной машине, запущенной на IOS-устройстве, и ни при каких условиях не предоставляет атакующему прав администратора на самой IOS.

Проблема существует из-за некорректной оценки технологией RBAC управления доступом гостевой ОС на IOS. Для эксплуатации уязвимости злоумышленник сначала должен авторизоваться. С ее помощью атакующий с низкими привилегиями может запросить доступ к гостевой ОС, который должен быть разрешен только для администратора. Уязвимость позволяет злоумышленнику получить права суперпользователя на ОС.

Единственный способ обезопасить уязвимое устройство от эксплуатации CVE-2019-12648 – установить обновление. Если по каким-либо причинам это невозможно сделать как можно скорее, Cisco рекомендует отключить гостевую ОС, что позволит «устранить вектор атаки».

Управление доступом на основе ролей (Role Based Access Control, RBAC) – развитие политики избирательного управления доступом, при котором права доступа субъектов системы на объекты группируются с учетом специфики их

применения, образуя роли.» ***(Маршрутизаторы Cisco промышленного класса уязвимы к кібератакам // SecurityLab.ru (https://www.securitylab.ru/news/501405.php). 27.09.2019).***

***

«Дослідник з кібербезпеки під псевдонімом axi0mX виявив критичну уразливість у iOS-пристроях, що працюють на процесорах від A5 (iPhone 4S) до A11 (iPhone 8 і iPhone X).

Цей код має назву checkm8. Він є вразливістю типу bootrom, яка може дати хакерам доступ до iPhone, який Apple не зможе блокувати.

Він використовує уразливість в вихідному коді, яка потрапляє на пристрої iOS при завантаженні.

Сотні мільйонів пристроїв iPhone схильні до цієї уразливості: будь-який пристрій, починаючи з iPhone 4S (чіп A5) через iPhone 8 і iPhone X (чіп A11).

За інформацією дослідника, Apple вже виправила недолік в торішніх процесорах A12. Тож нові смартфони iPhone XS / XR і 11/11 Pro Не будуть порушені.

Як вона може нашкодити? Хакери можуть використовувати цю вразливість для обходу блокування облікових записів Apple iCloud, які використовуються для того, щоб знайти загублені пристрої, або для установки програм, які крадуть призначену для користувача інформацію.» ***(У більшості моделей iPhone виявили критичну уразливість // BCBITI (http://vsviti.com.ua/news/104729). 29.09.2019).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Компания FireEye выпустила SharPersist — бесплатный набор инструментов с открытым исходным кодом для тестирования эффективности средств защиты от хакерских атак. С его помощью организации могут тестировать эффективность своих систем защиты против кибератак и улучшать их.

SharPersist представляет собой инструмент командной строки, написанный на языке C#, совместимый с любым фреймворком, поддерживающим технику отражающей загрузки сборок .NET.

Модульная структура инструмента позволяет добавлять новые методы сохранения персистентности. Текущая версия SharPersist поддерживает методы, включающие KeePass, новые или существующие запланированные задачи, новые службы Windows, новые или измененные записи реестра, папку автозагрузки и бесплатный клиент Tortoise SVN для системы контроля версий Subversion.

Компания опубликовала подробные инструкции по использованию SharPersist на GitHub.» ***(Опубликован инструмент для проверки эффективности защиты от кибератак // SecurityLab.ru (https://www.securitylab.ru/news/500839.php). 05.09.2019).***

***

«Компания Siemens расширила продуктовую линейку коммуникационных устройств мультисервисной платформы Ruggedcom (Ruggedcom Multi-Service Platform), представив новую, более мощную версию модуля обработки приложений Ruggedcom APE.

Модуль Ruggedcom APE представляет собой платформу для размещения приложений и работы со сторонними программными приложениями в тяжелых условиях эксплуатации.

Модуль Ruggedcom APE1808 является представителем семейства продуктов Ruggedcom RX15xx – экономичных коммутаторов и маршрутизаторов 2-го и 3-го уровней. Эта модульная, заменяемая в полевых условиях платформа позволяет клиентам выбрать одну из следующих трех опций связи: WAN, последовательный порт и Ethernet. Она идеально подходит для электроэнергетических компаний, железнодорожного транспорта и систем управления движением. Встроенные функции коммутации и маршрутизации мультисервисной платформы Ruggedcom RX1500, которыми обладает модуль Ruggedcom APE1808, позволяют использовать его для непосредственного подключения к любому изделию, входящему в это семейство. Модуль Ruggedcom APE1808 предоставляет один канал Gigabit Ethernet на передней панели шасси RX1500, а также другой – равнозначный, но полностью отдельный канал – на объединительную плату корпуса RX1500.

Ruggedcom APE поставляется с покрытием для дополнительной защиты и может работать при температуре окружающей среды от -40 до +75 градусов Цельсия. Он соответствует всем электрическим характеристикам платформы Ruggedcom RX15xx, а именно МЭК 61850-3 и IEEE 1613, и может использоваться для работы в самых тяжелых промышленных условиях.

Модуль Ruggedcom APE1808 на базе четырехъядерного процессора Intel с поддержкой операционных систем Linux и Windows 10 представляет собой стандартизированную платформу для доступного коммерческого программного обеспечения. Это позволяет установить партнерские отношения с лидерами отрасли в области обнаружения и предотвращения киберугроз.

Отмечается, что новый Ruggedcom APE1808 превосходит такие решения, как межсетевые экраны, процессоры сетевых журналов и нагрузки, а также датчики охранной сигнализации. Он может анализировать данные на уровне источника без дополнительных сложностей, связанных с установкой внешнего промышленного ПК. Ruggedcom APE1808 и решения в области кибербезопасности разработаны для электроэнергетики, транспорта и нефтегазовой промышленности, но также могут использоваться в любых других условиях с целью защиты сетей от растущего числа кибератак.

Портфель решений для информационной безопасности Ruggedcom обеспечивает доступ к множеству передовых приложений кибербезопасности, разработанных лидерами отрасли в рамках недавно заявленного партнерства с такими компаниями, как Fortinet, Nozomi Networks, Secure-NOK и Claroty. Клиенты «Сименс» извлекут пользу из опыта этих компаний в области защиты промышленных сетей от постоянно эволюционирующих угроз. На мультисервисной платформе Ruggedcom с помощью сертифицированных партнерских приложений от Fortinet, Nozomi Networks, Secure-NOK или Claroty

будут предоставляться следующие решения: система обнаружения вторжений (IDS), система предотвращения вторжений (IPS), глубокая проверка пакетов (DPI), межсетевой экран нового поколения (NGFW).

Ruggedcom APE1808 является ключевым продуктом в расширяющемся портфолио решений и услуг компании Siemens в области кибербезопасности, которое включает в себя комплексный сетевой консалтинг, оценку защищенности, интеграцию, внедрение, обучение и обслуживание на месте.» ***(Siemens выпускает промышленную платформу для приложений кибербезопасности // Компьютерное Обозрение (https://ko.com.ua/siemens_vypuskaet_promyshlennuyu_platformu_dlya_prilozhenij_kiberbezopasnosti_130215). 20.09.2019).***

***

«Посейдон» ищет куберуязвивимости при помощи нейросетей и искусственного интеллекта…

Как рассказал технический директор «Инжиниринговых технологий» Артём Долгих, применение программы позволит сократить расходы судовладельцев. В настоящее время идут тесты альфа-версии прототипа комплекса, программную его часть планируется разрабатывать в России, а аппаратная часть может быть произведена как на территории РФ, так и за её пределами. Помимо непосредственно защиты кораблей, «Посейдон» может использоваться для всей морской инфраструктуры — портов, верфей, буровых платформ. Сейчас 90% грузоперевозок идёт по морю и многие объекты этой сферы подвергаются атакам. Например, в России в начале 2018 года хакеры пытались нарушить работу администрации морских портов Азовского моря...» ***(Российские программисты создали защиту кораблей и портов от кибератак // Новости Великобритании на русском (https://theuk.one/rossijskie-programmisty-sozdali-zashhitu-korablej-i-portov-ot-kiberatak/). 30.09.2019).***

***

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

Актуальні дослідження правових та економічних процесів в контексті євроінтеграції = Actual studies of legal and economic processes in the context of european integration : матеріали Всеукр. наук.-практ. конф. здобувачів вищ. освіти, (28 трав. 2019 р., Дніпропетр. держ. ун-т внутр. справ). - Дніпро, 2019. - 186 с.

Зі змісту:

- Кошевець Е.Р. Соціальний вплив кіберзлочинності.

Шифр зберігання НБУВ: ВА834467

***

Актуальні питання судової експертизи і криміналістики : зб. матеріалів Міжнар. наук.-практ. конф., присвяч. 150-річчю з дня народж. Заслуж. проф. М. С. Бокаріуса, Харків, 18-19 квіт. 2019 р. - Харків : ХНДІСЕ, 2019. - 507 с.

Зі змісту:

- Філіппова Т.О. Інформаційне суспільство і кіберзлочинність: філософсько-антропологічний аспект.

Шифр зберігання НБУВ: СО36650

***

Безпека соціально-економічних процесів в кіберпросторі : матеріали Всеукр. наук.-практ. конф. (Київ, 27 берез. 2019 р.). - Київ, 2019. - 243 с.

Зі змісту:

- Деменюк С.В., Чубаєвський В.І., Макоєдова В.О. Міжнародне співробітництво як напрям забезпечення кібербезпеки України;
- Браіловський М.М., Хорошко В.О. Особливості кібербезпеки на підприємствах України в сучасних умовах;
- Пашорін В.І. Термінологічні та освітні аспекти кібербезпеки;
- Звєрєв В.П., Козаченко І.М. Актуальні проблеми кіберзахисту елементів критичної інфраструктури в період виборчої кампанії 2014 року;
- Швецова Г.Л. Корупція як загроза кібербезпеці об’єктів критичної інфраструктури;
- Білецький А.Л. Цифрова безпека розумного міста;
- Козік О.І., Гаврилюк Я.М. Актуальність кібертероризму;
- Жирова Т.О., Гамалій Б.С. Шляхи злому баз даних;
- Жирова Т.О., Маркевич Б.С. Огляд сучасних тенденцій боротьби у кіберпросторі;
- Олексюк Л.В. Кібергігієна особи – основа кібербезпеки України;
- Котенко Н.О., Гамалій Л.С. Загальна структура системи програмного захисту мережевих ресурсів;
- Половенко Л.П. Кіберзагрози у контексті інтерактивної освіти;
- Фомічова Н.В. Специфіка захисту інформації в закладах вищої освіти;
- Добровольська Н.В. Проблеми забезпечення боротьби з кіберзлочинністю.

Шифр зберігання НБУВ: СО36728

***

Гаращенко Ю.В. Державна політика у сфері кібербезпеки / Гаращенко Ю.В. // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Державне управління. - 2019. - Т. 30(69), № 3. - С. 140-145.

Проаналізовано історію становлення й основні поняття та категорії державної політики у сфері кібербезпеки, законодавчу та нормативно-правову базу для розуміння проблем, які наявні на цьому етапі розвитку української держави.

Шифр зберігання НБУВ: Ж70795/держ. упр.

***

Дудикевич В. Б. Безпровідні сенсорні мережі Zigbee, Wi-Fi та Bluetooth в кіберфізичних системах: концепція «об'єкт – загроза – захист» на основі моделі OSI / В. Б. Дудикевич, Г. В. Микитин, А. І. Ребець, М. В. Мельник // Системи обробки інформації. - 2019. - Вип. 2. - С. 114-120.

Розглянуто інформаційну безпеку сенсорних мереж Zigbee, Wi-Fi та Bluetooth згідно моделі OSI у просторі «рівень OSI – функції – протоколи» на основі концепції «об’єкт – загроза – захист» та нормативного забезпечення, які системно створюють підхід до побудови комплексних систем безпеки сенсорного безпровідного комунікаційного середовища (КС) кіберфізичних систем (КФС) за профілями конфіденційність – цілісність – доступність, що забезпечує безпечні процеси автоматизації об’єктів промислової інфраструктури України та інтеграції в міжнародний інтелектуальний простір.

Шифр зберігання НБУВ: Ж70474

***

Звоздецька О. Я. Нові підходи Північноатлантичного Альянсу (НАТО) у сфері кібербезпеки в умовах загострення інформаційного протистояння / О. Я. Звоздецька // Медіафорум: аналітика, прогнози, інформаційний менеджмент. - 2018. - Вип. 6. - С. 71-93.

Проаналізовано сучасну політику НАТО в сфері кібербезпеки в умовах загострення інформаційного протистояння. Констатовано, що гарантування міжнародної інформаційної безпеки та її складової – кібербезпеки залишаються одним із стратегічних завдань діяльності НАТО.

Шифр зберігання НБУВ: Ж74132

***

Информационное противоборство в современных условиях : монография. - Киев : Компринт, 2019. - 225 с.

Зі змісту:

- Гл. 6. Кибернетическая война – основная форма современного противоборства.

Шифр зберігання НБУВ: ВА834512

***

Кибіч Я. В. Особливості формування кібернетичної безпеки в умовах гібридної війни / Я. В. Кибіч // Медіафорум: аналітика, прогнози, інформаційний менеджмент. - 2018. - Вип. 6. - С. 94-111.

Проаналізовано проблему інформаційної безпеки України на сучасному етапі розвитку в умовах розгортання інформаційного суспільства. Розглянуто теоретичні підходи до визначення сутності поняття «кіберебезпека», «кіберпростір» вітчизняними та зарубіжними науковцями. Охарактеризовано нормативно-правову базу України, що регулює сферу інформаційної безпеки, зокрема нормативно-правові акти, які були прийняті, починаючи із 2014 року. Доведено, що кібернетичні атаки на інформаційні ресурси держави стали невід’ємним компонентом гібридної війни, розв’язаною Росією. Досліджено пріоритетні напрями державної політики у сфері забезпечення кібернетичної безпеки України в умовах гібридної війни.

Шифр зберігання НБУВ: Ж74132

***

Ланде Д. В. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки : навч. посіб. / Д. В. Ланде, І. Ю. Субач, Ю. Є. Бояринова. - Київ, 2018. - 300 с.

Розглянуто базові питання теорії і практики інтелектуального аналізу даних: алгоритми, моделі, задачі класифікації, кластерного аналізу, пошуку, глибинного аналізу даних (Data Mining), теорії складних мереж (Complex Networks), а також наведено відомості, необхідні для математичного і комп'ютерного моделювання та аналізу складних систем і мереж в сфері кібербезпеки.

Шифр зберігання НБУВ: ВА834626

***

Майбутнє науки в обріях права : зб. наук. пр. : матеріали IX міжнар. наук.-практ. конф. молодих учених (Київ, 5 груд. 2018 р.). - Київ, 2018. - 203 с.

Зі змісту:

- Дрогомирецький Б. Державні та правові заходи України в контексті захисту кіберпростору від російської агресії;
- Демченко П. Захист та гарантії конституційних прав і свобод людини та громадянина в рамках забезпечення кібернетичної безпеки України.

Шифр зберігання НБУВ: ВА834937

***

Матеріали IX міжнародної науково-практичної конференції «Комплексне забезпечення якості технологічних процесів та систем» (14-16 травня 2019 р., м.Чернігів). - Чернігів : ЧНТУ, 2019 . - Т. 2. - 283 с.

Зі змісту:

- Лахно В.А., Плиска Л.Д. Модель для опису процесу інвестування у кібербезпеку.

Шифр зберігання НБУВ: В357840/2

***

Матеріали Міжнародної науково-практичної конференції «Міжнародне та національне законодавство: способи удосконалення», 29-30 березня 2019 р. - Дніпро, 2019. - 196 с.

Зі змісту:

- Довженко О.Ю. Методика особистості злочинця при розслідуванні кіберзлочинів.

Шифр зберігання НБУВ: ВА834939

***

Матеріали міжнародної науково-практичної конференції «Тенденції розвитку юридичної науки в інформаційному суспільстві», 28 грудня 2018 року. - Одеса, 2018. - 215 с.

Зі змісту:

- Невара Л.М. Вплив кіберзагрози на освіту.

Шифр зберігання НБУВ: ВА835142

***

Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали III Міжнар. наук.-практ. конф. (м. Дніпро, 15 берез. 2019 р.) = International and national security: theoretical and applied aspects : theses of the III International scientific-practical conf. (Dnipro, March 15, 2019). - Дніпро, 2019. - 359 с.

Зі змісту:

- Кудінов В.А. Методика створення надійних паролів користувачів інформаційними ресурсами баз (банків) даних Національної поліції України;
- Орлова О.О., Циб І.С. Кібербезпека – складова сталого розвитку інформаційного суспільства та національної безпеки України у кіберпросторі;
- Ігнатов С.О. Кібертероризм як нова загроза національної безпеки України;
- Махницький О.В., Гавриш О.С. Аналіз кіберзагроз: найближчі перспективи.

Шифр зберігання НБУВ: ВС66071

***

Нашинець-Наумова А. Ю. До питання щодо боротьби з кібершпіонажем: вивчення та осмислення / А. Ю. Нашинець-Наумова // Актуальні проблеми правознавства. - 2019. - Вип. 1. - С. 126-131.

Висвітлено загрози інформаційної безпеки. Розглянуто одну з найбільш актуальних проблем сучасногоінформаційного суспільства – кібершпіонаж. Проаналізовано підходи щодо протидії загрозам, а також форми і методи, необхідні для вирішення цих завдань. Відзначено доцільність створення спеціалізованої служби, здатної відповідати мінливим викликам сучасного інформаційного суспільства.

Шифр зберігання НБУВ: Ж70813

***

Правове життя сучасної України : матеріали Міжнар. наук.-практ. конф., 17 трав. 2019 р. - Одеса, 2019. - Т. 1. - 721 с.

Зі змісту:

- Трофименко О.Г. Моніторинг стану кібербезпеки в Україні.

Шифр зберігання НБУВ: В357845/1

***

Правове життя сучасної України : матеріали Міжнар. наук.-практ. конф., 17 трав. 2019 р. - Одеса, 2019. - Т. 2. - 787 с.

Зі змісту:

- Стаурська О.М. Проблеми боротьби із кіберзлочинністю у контексті міжнародного співробітництва;
- Мазуренко С.В. Правові проблеми забезпечення кібербезпеки.

Шифр зберігання НБУВ: В357845/2

***

Ричка Д. О. Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : автореф. дис. ... канд. юрид. наук : 12.00.08 / Ричка Денис Олегович ; Держ. фіск. служба України, Ун-т держ. фіск. служби України. - Ірпінь, 2019. - 18 с.

Розкрито особливості кримінально-правової кваліфікації у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Визначено ознаки кібернетичних злочинів. Висвітлено ґенезу та поняття злочинів у сфері використання електроннообчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Досліджено різновиди як міжнародних, так і національних кібернетичних злочинів. Проведено комплексний аналіз елементів складу злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Розглянуто кваліфікуючі ознаки та здійснено їх відмежування від суміжних складів, на підставі чого сформовано нововведення та доповнення до чинного законодавства України з питань здійснення кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Шифр зберігання НБУВ: РА440000

***

Суспільство XXI століття: крізь призму історії до сьогодення : матеріали Звіт. всеукр. наук. конф. студентів та аспірантів, 18 трав. 2019 р. - Одеса, 2019. - 911 с.

Зі змісту:

- Афрамчук А.О. Інформаційні технології та кібербезпека у сучасному світі;
- Мозгова Т.С. Інформаційні технології та кібербезпека у сучасному світі.

Шифр зберігання НБУВ: ВА834951

***

Тези доповідей VII Міжнародної науково-практичної конференції «Інформаційні технології в освіті, науці і виробництві (ІТОНВ-2019)», м. Луцьк, 23-25 травня 2019 р.- Луцьк : НТУ, 2019. - 227 с.

Зі змісту:

- Савенко О.С., Нічепорук А.О., Лигун О.О. Метод визначення фрагментів ботнерів в локальній мережі на основі аналізу мережевого трафіку;
- Черняшук Н.Л. Технології захисту інформації в Wi-Fi мережах;
- Ящук А.А. Аналіз проблеми безпеки Інтернету речей.

Шифр зберігання НБУВ: ВА834420

***

Якимчук О.Ф. Державне управління кібербезпекою в умовах гібридної війни / Якимчук Олег Феодосійович // Актуальні проблеми державного управління. - 2019. - № 1. - С. 35-40.

Розроблено напрями стимулювання реалізації заходів з національної безпеки, у тому числі із кібербезпеки. Виявлено основні загрози розвитку надійної системи

кібербезпеки в Україні. Запропопоновано рекомендації щодо її удосконалення на основі впровадження заходів із посилення інформатизації суспільства

Шифр зберігання НБУВ: Ж69634

***

Katerynchuk P. Protection of Cyberspace as a Component of Ukraine's Information Security / P. Katerynchuk // Медіафорум: аналітика, прогнози, інформаційний менеджмент. - 2018. - Вип. 6. - С. 57-70.

Розглянуто питання захисту кіберпростору як складової національної безпеки держави, створення кіберполіції, державної стратегії кібербезпеки, приняття низки нормативних актів щодо кібербезпеки, посилення державного захисту у сфері захисту вітчизняного кіберпростору.

Шифр зберігання НБУВ: Ж74132

***