Науково-дослідний інститут інформатики і права
Національної академії правових наук України
Національна бібліотека України імені В. І. Вернадського

КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

№ 1 (січень)

Київ – 2019

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. 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

«В ексклюзивному інтерв`ю Михайло Шелемба, генеральний директор телекомунікаційної компанії Датагруп, розповів про кібератаки та шляхи захисту від них…

– Кібератак варто очікувати завжди. Це стосується і компаній, і кожної людини, і тим більше країни. Рано чи пізно кожен об'єкт буде атакований. Це правило, – впевнений експерт.

Уряд часто стикається зі спробами втручання у внутрішні справи країни…

– Такі речі, як вибори, День незалежності, важливі політичні свята підвищують ризик бути атакованими…

Звичайно, кібератакам у більшості випадків піддаються комерційні компанії. Але якщо вони, усвідомивши ризики, почали активно захищати свої ресурси, то в державних структурах усе набагато складніше…

До контролю напередодні виборів долучились і міжнародні організації. Євразійський центр Атлантичної ради, Трансатлантична комісія з чесних виборів та Фонд Віктора Пінчука створили робочу групу. Вони стежитимуть за виборчим процесом та інформуватимуть суспільство у разі виявлення порушень.

Та Шелемба нагадує, що така робота має проводитись регулярно, а не лише перед виборами…

Перший крок до захисту – це розуміння того, де знаходиться компанія, який у неї рівень захисту, пояснює Шелемба. У результаті діагностики отримуємо мапу слабких місць, які дають розуміння того, де і що потрібно "лікувати".

Але захистити все відразу – складно і дуже дорого. Саме тому наступний крок – визначити пріоритети. Треба перебудувати архітектуру зберігання даних і обміну інформацією таким чином, щоб знизити кількість потенційних точок атак…» ***(Лілія Ященко. Світові збитки понад $600 млрд: як боротись з кібератаками в Україні // ФАКТИ. ICTV (https://fakty.com.ua/ua/ukraine/20190108-svitovi-zbytky-ponad-600-mlrd-yak-borotys-z-kiberatakamy-v-ukrayini/). 08.01.2019).***

***

«Служба безпеки України виявила та блокувала 360 кіберінцидентів протягом 2018 року…

Співробітники СБУ притягнули до відповідальності 49 адміністраторів соцмереж за антиукраїнську пропаганду та 29 особам оголосили про підозру. У 2018 році 20 вироків набрали чинності.» ***(В СБУ заявили про 360 кібератак у минулому році // Espreso.tv (https://espreso.tv/news/2019/01/09/v_sbu_zayavyly_pro_360_kiberatak_u_mynulomu_roci). 09.01.2019).***

***

«Спикер Украинского киберальянса, известный в сети под ником Шон Таунсенд, опубликовал на своей странице в Facebook скриншот

видоизменного сайта официального вестника Кабинета Министров Украины «Урядовий кур'єр». Хактивисты УКА, используя XSS-уязвимость на сайте правительственного вестника, изменили содержимое ряда публикаций…

Таким образом УКА в рамках флешмоба #fuckresponsibledisclosure уже не первый раз пытается привлечь внимание властей к безопасности государственных информационных ресурсов…» ***(Украинские хакеры поиздевались над официальным вестником Кабинета Министров // Goodnews.ua (http://goodnews.ua/technologies/ukrainskie-xakery-poizdevalis-nad-oficialnym-vestnikom-kabineta-ministrov/). 16.01.2019).***

***

«Украинцы получат сообщения от своих операторов и провайдеров с предложением ознакомиться с основными правилами безопасности в киберпространстве. Соответствующие рекомендации операторам, провайдерам телекоммуникаций утвердила Национальная комиссия, осуществляющая государственное регулирование в сфере связи и информатизации…

Текстовое сообщение будет иметь следующую форму: «Шановний абоненте! У разі потреби або керуючись необхідністю підвищення рівня захисту персональних даних під час використання Інтернету, пропонуємо застосувати правила безпеки в кіберпросторі, з якими можна ознайомитися на офіційному сайті CERT-UA за відповідним посиланням».

По результатам обработки соответствующего обращения НКРСИ приняла решение предоставить операторам рекомендации о распространении среди пользователей правила безопасности в киберпространстве. Решение НКРСИ будет опубликовано в ближайшее время…» ***(Всем украинцам разошлют инструкции по кибербезопасности (обновлено) // Goodnews.ua (http://goodnews.ua/technologies/vsem-ukraincam-razoshlyut-instrukcii-po-kiberbezopasnosti-obnovleno/). 16.01.2019).***

***

«Европейский B2B акселератор Startup Wise Guys, главный офис которого находится в Эстонии, 28-29 января проведет в Киеве отбор украинских стартапов на ранней стадии для участия в SaaS-программе и первой в Европе программе по кибербезопасности с применением искусственного интеллекта CyberNorth… По итогам отбора Startup Wise Guys пригласят ряд стартапов на финальный отборочный тур по направлениям SaaS и кибербезопасность, где в каждую программу отберут до 11 проектов. Отобранные стартапы получат возможность привлечь инвестиции в размере до 30 тыс. евро, а также пройти 3-месячный интенсив, работая с более чем 150 менторами и инвесторами мирового уровня. Startup Wise Guys проводят Ukraine Startup Hunt уже во второй раз. В ближайшие два года в планах акселератора инвестировать до 2 млн евро в украинские стартапы на ранней стадии» ***(Европейский акселератор вложит 2 млн евро в украинские стартапы // PaySpace Magazine (https://psm7.com/technology/ukrainskie-startapy-smogut-poluchit-30-tys-evro-investicij.html). 15.01.2019).***

***

«С теневыми ресурсами Москвы в Украине не ведется должной борьбы…

"Когда сломали электронную шкатулку советника Путина Владислава Суркова, там была информация о финансировании Россией партий на местных выборах в Украине 2015-го. Правоохранители на это никак не отреагировали…", - сказала координатор избирательных программ Гражданской сети "Опора" Ольга Айвазовская...

"Есть также угроза кибератак. Перед последним днем голосования могут украсть данные, которые важны для избирательного процесса. И для их восстановления понадобится некоторое время…", - отметила Айвазовская.» ***(К чему прибегнет Кремль на выборах в Украине // Gazeta.ua (https://gazeta.ua/ru/articles/politics/_k-chemu-pribegnet-kreml-na-vyborah-v-ukraine/880725). 18.01.2019).***

***

«…Компетентні органи України систематично виявляють кібератаки на інформаційні ресурси, що використовуються структурними підрозділами Міністерства закордонних справ та закордонними дипломатичними представництвами України», — повідомили у Міністерстві закордонних справ України.

“Протягом 2018 року значно зросла кількість вірусних атак, які спрямовані на закордонні дипломатичні установи України (ЗДУ) та кількість „фішингових“ атак, що є досить поширеним явищем, зокрема у Міністерстві було зафіксовано та усунуто наслідки 5 кіберінцидентів”, — зазначили у МЗС…» ***(Саша Картер. Зросла кількість вірусних атак проти закордонних дипустанов України // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/exclusive/1775286-zrosla-kilkist-virusnikh-atak-proti-zakordonnikh-dipustanov-ukrayini). 23.01.2019).***

***

«За 2018 рік Росія здійснила 190 провокацій, щоб дестабілізувати українське суспільство…

Таку кількість провокацій з боку РФ зафіксувало Міністерство з питань тимчасово окупованих територій та внутрішньо переміщених осіб в Україні.

Росія не раз намагалася перешкодити роботі державних органів. Так, на початку грудня 2018 року російські спецслужби атакували інформаційно-телекомунікаційні системи судової влади України. Російські хакери розсилали електронною поштою заражені вірусом підроблені бухгалтерські документи…

А у Львові правоохоронці викрили комерційну структуру, яка за допомогою забороненого російського програмного забезпечення "Парус" та "Афіна" намагалася отримати інформацію з державних ораганів.

У Міністерстві зазначили, що такі дії з боку Росії є традиційними. Особливо увага російських хакерів до України посилюється під час передвиборчої кампанії. Вони збирають дані та зламують доступ до поштових скриньок…

Також у Міністерстві додали, що найбільше російських кібератак сталося у Запорізькій (26%), Києві та Київській області (15%), Дніпропетровській (12%), Донецькій (10%) та Херсонській (9%) областях.» ***(Російська агресія у кіберпросторі: за минулий рік Кремль здійснив майже 200 провокацій // Телеканал новин «24» (https://24tv.ua/rosiyska_agresiya_u_kiberprostori_za_minuliy_rik_kreml_zdiysniv_mayzhe_200_provokatsiy_n1101233?utm_source=rss). 23.01.2019).***

***

«…Російська влада додатково виділила своїм спецслужбам 350 мільйонів доларів для реалізації підривної діяльності в Україні у 2019 році.

Про це розповів голова Служби зовнішньої розвідки Єгор Божок…

За словами голови СЗР, ці гроші будуть спрямовані на проплату фейкових новин і підкуп, організацію провокацій, протестів, внутрішньополітичного тиску на керівництво держави, а також для підготовки кібератак…» ***(Кремль додатково виділив гроші на втручання у вибори в Україні: СБУ дізналася суму // 5 канал (https://www.5.ua/polityka/kreml-dodatkovo-vydilyv-hroshi-na-vtruchannia-u-vybory-v-ukraini-sbu-diznalasia-sumu-185353.html). 24.01.2019).***

***

«Екс-посол США та колишній заступник генсека НАТО Александер Вершбоу заявив, що Україна є потенційною гарячою точкою в світі та має бути готовою до того, що Росія може почати нову відкриту агресію, аби захопити Азовське море або прибережні його території…

На його думку, пряме зіткнення України та Росії можливе, але навряд чи Кремль використає таку форму агресії.

"Росіяни можуть досягти багатьох своїх цілей заплутанішими формами агресії: кібератаками, дезінформацією, розпалюванням сепаратизму, корупцією та іншими засобами створення нестабільності в Україні…", — підкреслив експерт…» ***("Україна має приготовуватися до нової атаки": в США зробили тривожний прогноз // ONLINE.UA https://novyny.online.ua/805113/ukrayina-mae-prigotovuvatisya-do-novoyi-ataki-v-ssha-zrobili-trivozhniy-prognoz/). 21.01.2019).***

***

«Президент України Петро Порошенко в інтерв'ю телеканалу "Україна" розповів про деякі деталі зустрічі з канцлером ФРН Ангелою Меркель щодо запобігання втручання РФ у вибори…

"Йдеться про кібербезпеку. Це йдеться, в тому числі про обмін даними...", — зазначив Порошенко.

Водночас він підкреслив, що не може розкривати зміст домовленостей щодо спецслужб та всіх механізмів забезпечення кібербезпеки…

Глава держави нагадав, що за українською ініціативою був створений трастовий фонд НАТО щодо кібербезпеки, а також є конкретні двосторонні угоди, починаючи з США та Великобританії і закінчуючи Німеччиною…» ***(Тоня Туманова. Порошенко розповів деякі деталі зустрічі з Меркель // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1775703-poroshenko-rozpoviv-deyaki-detali-zustrichi-z-merkel). 24.01.2019).***

***

«Хакери, які скоріш за все, співпрацюють з Росією, нарощують зусилля для зриву виборів Президента України за допомогою кібератак на сервери ЦВК та персональні комп'ютери працівників ЦВК…

За словами глави кіберполіції України Сергія Демидюка, кібер-зловмисники використовували заражені вірусом вітальні листівки, запрошення магазинів, пропозиції оновлення програмного забезпечення та інші шкідливі "фішингові" матеріали, призначені для крадіжки паролів і особистої інформації.

За десять тижнів до виборів хакери також почали купувати особисті дані співробітників ЦВК, сказав Демедюк, розплачуючись при цьому криптовалютою через Darknet, частини Інтернету, доступну тільки через певне програмне забезпечення і яка зазвичай використовується анонімно…» ***(Ілля Нежигай. Кіберполіція: Росія планує кібератаки під час виборів в Україні // Інформаційне агентство «Українські Національні Новини»https://www.unn.com.ua/uk/news/1776121-kiberpolitsiya-rosiya-planuye-kiberataki-pid-chas-viboriv-v-ukrayini). 27.01.2019).***

***

Боротьба з кіберзлочинністю в Україні

«Суд простил юному хакеру-неудачнику распространение вируса-шифровальщика…

Согласно определению суда, студент кафедры французской филологии Львовского национального университета имени Ивана Франко 11 марта 2017 года зарегистрировался на известном в сети «Форуме социальной инженерии». Дабы нарастить себе рейтинг на этом сайте, парень нашел на одном из ресурсов в сети вредоносное ПО Encorder.Builder2.4… и разместил ссылку на него на данном форуме.

…студент-филолог осознавал, что размещенное им в свободном доступе вредоносное программное обеспечение приводит к потере и блокированию информации, однако, «несмотря на осведомленность, предоставил пользователям сети Интернет доступ к указанному вредоносному программному обеспечению, то есть совершил преступление, предусмотренное ч. 1 ст. 361-1 УК Украины».

…суд принял решение освободить студента ЛНУ имени Франко от уголовной ответственности и закрыть уголовное производство в связи с деятельным раскаянием. Тем не менее, …он должен оплатить расходы на проведение комиссионной компьютерно-технической экспертизы (18304 грн) и комплексной судебной компьютерно-технической экспертизы, экспертизы телекоммуникационных систем и средств (29315 грн)…» ***(Владимир Кондрашов. Пойманный хакер заплатит 47 тысяч за судебные экспертизы // Internetua (http://internetua.com/poymannyi-haker-zaplatit-47-tysyacs-za-sudebnye-ekspertizy). 04.01.2019).***

***

«…Працівники Поліського управління Департаменту кіберполіції із залученням працівників Управління інформаційних технологій та програмування в західному регіоні, спільно зі слідчими Рівненської поліції, за процесуального керівництва Рівненської місцевої прокуратури, викрили групу осіб у створенні вірусів та їх використанні для незаконного збагачення.

…злочинна група складалася з чотирьох осіб віком від 26 до 30 років. Використовуючи спеціальні технічні засоби вони сканували комп’ютери, які під’єднані до мережі Інтернет на наявність віддаленого доступу. В подальшому, використовували створені віруси для отримання повного контролю над ураженим комп’ютером.

Після цього підбирали паролі для доступу в систему. Користуючись комп’ютером на правах власника, хакери отримували доступ до програми онлайн-банкінгу, встановленої на комп’ютері, та перераховували кошти на підконтрольні рахунки або переводили у криптовалюту…

Також, для отримання доступу над комп’ютерами, зловмисники використовували спам-розсилку інфікованих електронних листів. Зазвичай, такі листи надходили на адреси представників юридичних осіб…

Кримінальне провадження розпочато за декількома статтями кримінального кодексу України: ст.361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) та ст.185 (крадіжка) КК України.» ***(Кіберполіція викрила групу хакерів, які ошукали українців більш як на 5 мільйонів гривень // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-grupu-xakeriv-yaki-oshukaly-ukrayinczіv-bilsh-yak-na--miljoniv-gryven-968/). 10.01.2019).***

***

«…В Украине и мире продолжается распространение шифровальщика #Scarab через массовые рассылки фишинговых электронных писем на русском или украинском языках (возможно с ошибками)…

Более того, эксперты украинской команды по реагированию на компьютерные чрезвычайные события CERT-UA также предложили украинцам ознакомиться с подобным вариантом зараженного сообщения. «Добрый День! Не получается связаться с вами по телефону. Повторно направляю вчерашний акт сверки», — говорится в тексте фишингового сообщения.

Так, после запуска вируса, на компьютере запускается специальный процесс, который приводит к полному блокированию техники. После этого он начинает вымогать оплату в виде биткоинов…» ***(Популярный бренд установил на смартфоны вирус-шпион // Politeka (https://politeka.net/news/hightech/873287-populjarnyj-brend-ustanovil-na-smartfony-virus-shpion/). 15.01.2019).***

***

«…Працівники Донецького управління Департаменту кіберполіції спільно зі слідчими поліції Донеччини, за процесуального керівництва Маріупольської місцевої прокуратури, викрили двох мешканців міста Маріуполь у здійсненні DDoS-атак на ряд регіональних інформресурсів. Це стало причиною недоступності сайту на деякий період.

Працівники кіберполіції встановили, що 22-річний молодик створив два програмних коди для здійснення DDoS-атак. За допомогою створених програмних засобів він, спільно зі своїм 21-річним товаришем, здійснював втручання в роботу Інтернет-порталу. Так, програма надсилала щосекундно близько сотні автоматичних запитів до ресурсу. У результаті, це призвело до відмови від обслуговування новинного порталу…

За даним фактом поліція розпочала кримінальне провадження за ст.361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України.» ***(Кіберполіція встановила двох чоловіків, які вчиняли DDoS-атаки на українські Інтернет-ресурси // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vstanovila-dvox-cholovikiv-yaki-vchinyali-DDoS-ataki-na-ukrajinski-Internet-resursi/). 18.01.2019).***

***

«Безработный, ранее несудимый, гражданин Украины заплатит почти 12 тысяч гривен штрафа и 2145 гривен издержек на судебную экспертизу за распространение в сети вредоносного программного обеспечения…

Согласно приговору Центрального районного суда Николаева, …12 декабря 2017 года в 01:40, действуя умышленно, с целью получения удаленного доступа к компьютерной технике пользователей сети Интернет и вмешательства в работу компьютеров, обвиняемый настроил компьютерную программу «amazon 2.0.exe», где в качестве сервера указал динамический IP-адрес, который на тот промежуток времени был выделен ему Интернет-провайдером ООО «Дикий Сад».

Мужчина добавил вредоносное ПО «amazon 2.0.exe» к архивному файлу «Amazon.rar», и в 01:44 12 декабря 2017 года загрузил его с целью распространения на облачное хранилище «MEGA.nz», зарегистрированное на электронный ящик обвиняемого и его аккаунт, авторизованный в веб-браузере Google Chrome.

– Таким образом, своими умышленными и противоправными действиями обвиняемый совершил уголовное преступление, предусмотренное ч.1 ст.361-1 УК Украины, а именно распространение вредоносных программных средств, предназначенных для несанкционированного вмешательства в работу электронно-

вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей, – говориться в приговоре.

Мужчина пошел на сделку о признании виновности…» ***(Владимир Кондрашов. Хакер-неудачник заплатит 14 тысяч за распространение компьютерного ви руса // Internetua (http://internetua.com/haker-neudacsnik-zaplatit-14-tysyacs-za-rasprostranenie-kompuaternogo-virusa). 21.01.2019).***

***

«Безработный уроженец Запорожья осужден на год условно за перепродажу специализированного программного обеспечения для взлома банкоматов…

Согласно материалам дела, приблизительно в марте 2018 года мужчина, находясь в Василькове Киевской области, нашел на неустановленном следствием сайте сообщение о продаже вредоносного программного обеспечения «CutletMaker», предназначенного для осуществления несанкционированного вмешательства в работу банкоматов торговой марки «Wincor Nixdorf».

…Безработный за 18 тысяч гривен приобрел у неустановленного лица вышеуказанное ПО, которое в дальнейшем загрузил на свою флешку и хранил при себе с целью дальнейшего сбыта.

Позже обвиняемый через мессенджер «Telegram» в закрытой группе разместил объявление о продаже «CutletMaker», и 4 мая прошлого года продал его за 20 тысяч гривен.

Ещё раз продать ПО для взлома банкоматов мужчине помешали правоохранители.

28 сентября между обвиняемым и прокурором была заключена сделка о признании виновности. Согласно ей, стороны договорились о правовой квалификации действий обвиняемого по ч. 1 ст. 361-1 УК Украины, а также наказание, которое он должен понести в виде одного года лишения свободы с освобождением от отбывания наказания с испытательным сроком один год…» ***(Владимир Кондрашов. Безработного украинца осудили за перепродажу ПО для взлома банкоматов // Internetua (http://internetua.com/bezrabotnogo-ukrainca-osudili-za-pereprodaju-po-dlya-vzloma-bankomatov). 19.01.2019).***

***

«Ранее несудимый безработный хакер взломал систему «Власний рахунок» сети супермаркетов «Сільпо» и заставил систему начислить ему бонусные денежные средства…

Об этом говорится в определении Херсонского городского суда Херсонской области…

По версии следствия, начиная с ноября 2016 года мужчина, обладая необходимыми знаниями в пользовании электронно-вычислительной техникой, умышленно, из корыстных побуждений, через Интернет, путем использования программного обеспечения, с функцией автоматического перебора паролей, установленного в операционной системе KaliLinux, совершил

несанкционированный доступ к учетным данным в программе «Власний рахунок» (ООО "Сільпо-Фуд")…

Согласно информации из электронной базы данных «Власний рахунок», имеющейся у следствия, мужчина провел расчеты на кассах супермаркета «Сільпо» – рассчитался бонусами на сумму 7056, 09 гривен, чем нанес ООО «Сільпо-Фуд» материальный ущерб в указанном размере.

…ООО «Сільпо-Фуд» отказалось от обвинений, поскольку хакер полностью возместил нанесенный ущерб. Суд, заслушав мнение прокурора и стороны защиты, принял решение закрыть уголовное производство.» ***(Владимир Кондрашов. Хакер взломал «Сільпо», чтобы потратить бонусные деньги в супермаркете // Internetua (http://internetua.com/haker-vzlomal-silpo-cstoby-potratit-bonusnye-dengi-v-supermarkete-1). 18.01.2019).***

***

«У понеділок, 28 січня 2019 року, заступник Генерального прокурора Євгеній Єнін під час спільного брифінгу з Головою Нацполіції України Сергієм Князєвим, повідомив, що у четвер, 24 січня 2019 року, міжнародна спільна група, до складу якої входили співробітники Генеральної прокуратури України, Національної поліції, а також Федерального підрозділу по боротьбі із комп'ютерною злочинністю (FCCU) Бельгії, за сприяння Європолу, Федерального бюро розслідувань США (FBI) та Служби внутрішніх доходів США (IRS) у м. Тампа (штат Флорида) провели обшуки у дев'яти локаціях в Україні…

Вказані обшуки проведено в рамках розслідування кримінальних проваджень щодо незаконного онлайн магазину «xDedic», на якому пропонувався до продажу доступ до десятків тисяч компрометованих (зламаних) серверів потерпілих (компаній та приватних осіб)…

Хакерська діяльність проводилася шляхом злому доступу через протокол віддаленого робочого столу (RDP). Покупці та продавці здійснювали торгівлю такими RDP серверами на цій платформі. Вартість кожного серверу складала від шести до понад десяти тисяч доларів США.

Американське розслідування злочинної групи онлайн магазину «xDedic» здійснювалося Прокуратурою США Середнього округу штату Флорида.

У четвер, 24 січня 2019 року доступ до «xDedic» було припинено відповідно до рішень американського суду, а складові кримінальної інфраструктури були конфісковані…

Федеральна прокуратура Бельгії розпочала розслідування щодо «xDedic» у червні 2016 року. Використання спеціальних методів розслідування дозволило Федеральному підрозділу по боротьбі із комп'ютерною злочинністю (FCCU) візуалізувати злочинну інфраструктуру «xDedic» та отримати цифрові копії її найбільш важливих серверів…

Завдяки скоординованим зусиллям бельгійські, українські та американські правоохоронні органи, прокуратура та поліція завдали руйнівного удару по незаконній торгівлі "зламаними" комп'ютерними системами…

Розслідування цієї справи в Україні, Бельгії та США досі триває.» ***(Міжнародною спільною групою правоохоронців ліквідовано платформу xDedic // Кіберполіція України (https://cyberpolice.gov.ua/news/pravooxoronczi-zablokuvaly-robotu-najbilshogo-majdanchyku-z-prodazhu-konfidenczijnoyi-informacziyi-u-darknet-549/). 28.01.2019).***

***

«…Працівники Департаменту кіберполіції задокументували протиправну діяльність 30-річного мешканця Запоріжжя, який розроблював та поширював шкідливе програмне забезпечення.

Створений ним вірус потрапляв у файлову систему користувачів через розсилки спам-повідомлень, а також із веб-сайтів із замаскованим у різні частини веб-сторінки вірусом. Завдяки цьому зловмисник отримував доступ до персональних комп'ютерів користувачів. Це дозволяло отримувати логіни та паролі потерпілих для авторизації в їх крипто-гаманцях. Отримавши доступи до крипто-біржових акаунтів та до комп'ютерного обладнання потерпілих, зловмисник здійснював виведення коштів на підконтрольні біткоїн-гаманці.

…Також було виявлено, що у 2017 році чоловік розповсюджував шкідливий програмний засіб під назвою «kiaracript». Цей вірус був призначений для шифрування інформації користувачів ураженого пристрою. Для дешифровки інформації потерпілий мав сплатити зловмисникам гроші у криптовалюті…

За даним фактом розпочато кримінальне провадження за ч.2 ст.361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України…» ***(Кіберполіція викрила чоловіка у поширенні вірусів за допомогою поштової спам-розсилки // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-cholovika-u-poshyrenni-virusiv-za-dopomogoyu-poshtovoyi-spam-rozsylky-3339/). 24.01.2019).***

***

Світові тенденції в галузі кібербезпеки

«Конечные показатели безопасности не всегда полностью детерминированы или имеют прямую причинно-следственную связь: например, вы можете все сделать правильно, но вас все равно взломают, или же все сделали неверно, но по счастливому случаю избежали хакерской атаки…

Если вам кажется, что это снижение эффективности контроля/противодействия безопасности надумано, существует ряд моментов, когда эффективность может постепенно падать.

Во-первых, учтите, что распределение персонала не является статичным, а члены команды - не взаимозаменяемы. Так, сокращение штата может привести к тому, что у данного инструмента или элемента управления будет меньше точек

соприкосновения, что, в свою очередь, уменьшит его полезность в вашей программе. Перераспределение обязанностей может повлиять на эффективность, когда один инженер менее квалифицирован или имеет меньший опыт, чем другой.

Аналогичным образом, изменения в самой технологии могут повлиять на эффективность…

Есть также естественное разрушение... Организация, которая не пострадала от взлома, может попытаться сэкономить на затратах на технологии или не сможет инвестировать таким образом, чтобы идти в ногу с развитием технологий…

Суть в том, что эти процессы неизбежны. Тем не менее, их предотвращение - и создание инструментария, чтобы узнать о них - отделяет лучшие программы от просто адекватных.

Начнем с того, что нет недостатка в моделях риска и подходах к измерению, моделях возможностей проектирования системной безопасности (например, NIST SP800-160 и ISO/IEC 21827), моделях зрелости и т. п., но есть одна общая черта, которая создает некоторый механизм, позволяющий измерить общее воздействие на организацию на основе конкретных элементов управления в этой системе.

Здесь есть два подкомпонента: во-первых, значение, предоставляемое каждым элементом управления всей программе; и во-вторых, степень, в которой изменения в данном контроле влияют на нее.

Первый набор данных - это, в основном, управление рисками - построение понимания ценности каждого элемента управления. Вторая часть - это создание инструментария для каждого из вспомогательных элементов управления, чтобы вы могли понять влияние изменений (положительных или отрицательных) на производительность…» ***(Ирина Фоменко. Как предотвратить крах ваших систем кибербезопасности // Internetua (http://internetua.com/kak-predotvratit-krah-vashyh-sistem-kiberbezopasnosti). 05.01.2019).***

***

«…швейцарский страховщик Zurich Insurance отказался выплачивать страховое возмещение на сумму $100 млн за ущерб, причиненный крупной продовольственной компанией Mondelez вследствие кибератаки NotPetya, которая произошла в июне 2017 года, основной целью которой была политическая и экономическая дестабилизация. В исковом заявлении Mondelez указал, что компания дважды подверглась кибератаке, вследствие чего 1700 принадлежащих ей серверов и 24 тысячи компьютеров по всему миру были выведены из строя.

…Страховщик аргументировал свой отказ наличием в договоре пункта о «враждебных или военных действиях», поддерживаемых на государственном уровне, которое не покрывается страховкой.

По мнению вице-президента компании по изучению кибер-уязвимостей HackerOne Деборы Чанг, судебный иск может стать прецедентом и оказать существенное влияние на дальнейшее развитие киберстрахования» ***(Zurich отказался выплатить $100 млн ущерба от кибератаки NotPetya // УкрСтрахование (https://www.ukrstrahovanie.com.ua/news/zurich-otkazalsya-vyiplatit-100-mln-ushherba-ot-kiberataki-notpetya). 15.01.2019).***

***

«…Исследователи Массачусетского технологического института (MIT) изучили программу вознаграждений Facebook, а также более 60 программ, запущенных на платформе HackerOne для Twitter, Coinbase, Square и других компаний.

Как выяснилось, вопреки бытующему мнению, программы вознаграждения, в которых участвует большое количество исследователей, не приносят организациям большой пользы. Как правило, только малая часть экспертов предоставляет большое количество качественных отчетов об уязвимости. Именно к ним уходит значительная часть призового фонда.

Согласно исследованию, семь наиболее «продуктивных» участников программы Facebook зарабатывали всего $34 255 в год при обнаружении в среднем 0,87 ошибок в месяц, а в случае с программами на HackerOne лидеры зарабатывали только $16 544 при выявлении 1,17 ошибок в месяц в среднем.» ***(MIT: собственные исследователи кибербезопасности приносят больше пользы, чем программы Bug Bounty // Информационная безопасность (http://www.itsec.ru/news/mit-sobstvennie-issledovateli-kiberbezopasnosti-prinosiat-bolshe-polzi-chem-programmi-bug-bounty). 17.01.2019).***

***

«Участники Всемирного экономического форума в Давосе (ВЭФ) ждут в этом году усиления геополитической и геоэкономической напряженности… Это затрудняет совместное решение нарастающих долгосрочных проблем в экологической, экономической и социальной областях, а также связанных с влиянием технологий на нашу жизнь, говорится в подготовленном ВЭФом докладе «Глобальные риски в 2019 г.».

Опрошенные эксперты прежде всего ожидают роста в 2019 г. рисков, связанных с «экономической конфронтацией между ведущими державами» (91% респондентов), «размыванием международных торговых правил и соглашений» (88%) и «политической конфронтацией между ведущими державами» (85%).

За ними идут «Кибератаки: кража данных или денег» (82%) и «Кибератаки: нарушение операций или работы инфраструктуры»…» ***(Михаил Оверченко. Давосский форум предупредил мир о рисках // АО Бизнес Ньюс Медиа (https://www.vedomosti.ru/economics/articles/2019/01/16/791584-davosskii-forum-riskah). 16.01.2019).***

***

«Bitdefender, ведущая глобальная компания в области кибербезопасности, технологии которой защищают более 500 миллионов систем по всему миру, с гордостью сообщает, что была признана отраслевым новатором в категории «Инфраструктура безопасности» в рамках специального выпуска SC Media Reboot 2019 года…

В рамках своего ежегодного специального выпуска Reboot, на конец года команда SC Lab выбирает инновационные продукты и поставщиков, которые

выделяются своей силой, креативностью и стратегическим положением на рынке. Reboot рассматривает только самые прогрессивные идеи за последний год, одновременно строя прогнозы на будущее…» ***(Bitdefender признана инноватором в области инфраструктуры кибербезопасности // ChannelForIT (http://channel4it.com/publications/Bitdefender-priznana-innovatorom-v-oblasti-infrastruktury-kiberbezopasnosti-33052.html#). 31.01.2019).***

***

«Подразделение Google Jigsaw, занимающееся разработкой решений в области кибербезопасности, предложило европейским политическим партиям и организациям в преддверии выборов в Европарламент защитить их сети от DDoS-атак с помощью сервиса Project Shield…

Сервис был разработан Jigsaw в 2016 году, но до сих пор компания предоставляла его только американским информационным изданиям, журналистам, правозащитным организациям и группам наблюдателей на выборах. …глава пресс-службы Jigsaw Дэн Кизерлинг подчеркнул, что свои услуги всем политическим организациям Европы их компания предлагает бесплатно, в отличие от других провайдеров аналогичных сервисов.» ***(Google обеспечит европейским партиям киберзащиту перед выборами в Европарламент // Goodnews.ua (http://goodnews.ua/technologies/google-obespechit-evropejskim-partiyam-kiberzashhitu-pered-vyborami-v-evroparlament/). 29.01.2019).***

***

Сполучені Штати Америки

«…Министерство здравоохранения и социальных служб США представило новое руководство по кибербезопасности под названием «Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients» для организаций в сфере здравоохранения, включающее принципы и практики по обеспечению безопасности.

Руководство состоит из четырех томов, содержащих гибкий набор рекомендаций, которые могут использовать как небольшие клиники, так и крупные организации в области здравоохранения. Документ концентрируется на пяти наиболее распространенных угрозах кибербезопасности - фишинговых атаках; атаках с использованием вымогательского ПО; потере или краже оборудования или данных; утечках данных (непреднамеренные, намеренные или в результате действий инсайдеров); атаках на подключенное к интернету медицинское оборудование, которые могут поставить под угрозу безопасность пациентов.

Документ также содержит набор рекомендаций для минимизации влияния угроз кибербезопасности на работу организаций, включая практики по защите систем электронной почты, конечных устройств, управлению доступом и сетями, защите данных и предотвращению их утечек, реагированию на инциденты безопасности, устранению уязвимостей, обеспечению безопасности медицинских приборов и пр…» ***(Минздрав США выпустил новое руководство по***

кибербезопасности // SecurityLab.ru https://www.securitylab.ru/news/497356.php).(09.01.2019).

***

«…В рамках кампании «Know the Risk, Raise Your Shield» («Знайте риск, поднимите щит») Национальный центр контрразведки и безопасности США (National Counterintelligence and Security Center, NCSC) запустил программу, призванную помочь частным американским предприятиям обеспечить защиту от хакерских атак и других угроз, связанных с проправительственными киберпреступными группировками.

Ведомство начало распространять материалы с инструкциями по защите от атак на цепочки поставок (или компоненты, произведенные за пределами США), фишинговых кампаний или экономического шпионажа, такого как кража интеллектуальной собственности…» **(Контрразведка США запустила программу по защите фирм от кибератак // SecurityLab.ru (https://www.securitylab.ru/news/497351.php). 09.01.2019).**

***

«…Министерство внутренней безопасности США (МВБ) выпустило "чрезвычайную директиву", предписывающую федеральным гражданским агентствам обеспечить защиту логинов и паролей для учетных записей доменных имен.

Согласно приказу, ведомства должны включить многофакторную аудентификацию в DNS-аккаунтах, изменить пароль для учетных записей, провести проверку DNS-записей и сертификатов. На выполнения требования ведомствам предоставлено 10 рабочих дней…

Приказ последовал за отчетом ИБ-компании FireEye, описывающим, как злоумышленники манипулировали DNS-записи для перехвата и перенаправления целевого трафика через вредоносные серверы. Кампания была направлена на организации на Ближнем Востоке, в Северной Африке, Европе и Северной Америке, включая государственные ведомства и коммерческие предприятия.

Частичная приостановка работы правительства США, которая продолжается уже два месяца, может осложнить исполнение директивы. На данный момент 800 тыс. госслужащих находятся в принудительном отпуске или работают без оплаты...» ***(МВБ США озаботилось защитой от перехвата DNS // SecurityLab.ru (https://www.securitylab.ru/news/497565.php). 23.01.2019).***

***

«Власти США ведут уголовное расследование в отношении Huawei, подозревая ее в краже технологий у американских партнеров…

Huawei, основанная бывшим китайским офицером и ставшая крупнейшим производителем телекоммуникационного оборудования в мире, уже давно вызывает опасения у властей США. Они считают, что Китай может использовать ее оборудование для кибершпионажа, поэтому запрещают использовать его для основных сетей. С приходом к власти президента Дональда Трампа давление на

компанию усилилось, так как он хочет положить конец краже Китаем интеллектуальной собственности американских компаний. Поэтому США начали призывать союзников отказаться от оборудования Huawei в 5G-сетях.

В среду республиканцы и демократы предложили законопроект, запрещающий экспорт американских компонентов китайским телекоммуникационным компаниям, нарушающим санкции США или законы о контроле за экспортом... Представитель министерства иностранных дел Китая назвала законопроект «истерией» и свидетельством того, что власти США ищут все возможные способы, чтобы помешать развитию китайских технологических компаний…» ***(Алексей Невельский. США и другие западные страны усиливают давление на Huawei // АО Бизнес Ньюс Медиа (https://www.vedomosti.ru/technology/articles/2019/01/18/791827-ssha-davlenie-huawei). 18.01.2019).***

***

Країни ЄС

«...Польша может рассмотреть вопрос о запрете использования продуктов Huawei государственными органами, заявил курирующий вопросы кибербезопасности чиновник Кароль Оконьски (Karol Okonski). Сообщение последовало после ареста китайского представителя Huawei в Польше на прошлой неделе.

Правительство страны может также ужесточить законодательство, что позволит властям ограничить доступность продуктов, производимых любой компанией, которая может представлять угрозу безопасности…

Представитель службы безопасности заявил в пятницу телекомпании TVP, что чиновник, арестованный Агентством внутренней безопасности страны (Agencja Bezpieczeństwa Wewnętrznego), отвечал за выдачу сертификатов безопасности на оборудование, используемое государственной администрацией.

Huawei уже заявила об увольнении своего сотрудника, добавив, что его предполагаемо незаконные действия никак не связаны с компанией.

Министр внутренних дел Польши Йоахим Брудзинськи (Joachim Brudzinski) поддержал позицию Кароля Оконськи в отношении Huawei и призвал Европейский союз и НАТО выработать совместную позицию относительно того, следует ли исключать Huawei с рынков…» **(Польша задумалась о запрете на использование продуктов Huawei // SecurityLab.ru (https://www.securitylab.ru/news/497453.php). 15.01.2019).**

***

«…прем'єр-міністр Чехії Андрей Бабіш закликав 160 державних і приватних організацій перевірити, чи вони не є вразливими через використання програм і техніки китайських компаній Huawei та ZTE. Зокрема, хвилювання викликала запущена минулого року у Чехії мережа 5G, де використали технології Huawei…

Уряд країни також наказав операторам ключової інфраструктури провести аналогічні перевірки. Оцінити ризики просять банки, аеропорти, мобільних та інтернет-операторів, електростанції та інші організації.

Національне агентство з питань кібернетики та інформаційної безпеки Чехії допоможе у проведенні аналізу можливих ризиків…» ***(У Чехії оцінюють загрози кібербезпеці від використання техніки Huawei і ZTE // MediaSapiens (https://ms.detector.media/web/cybersecurity/u_chekhii_otsinyuyut_zagrozi_vid_vikoristannya_tekhniki_huawei_i_zte/). 10.01.2019).***

***

«…Европейский Союз рассматривает предложения, которые фактически являются запретом на использование оборудования Huawei Technologies Co для внедрения мобильных сетей следующего поколения, что "усилит международное давление мира на крупнейшего производителя телекоммуникационного оборудования".

По словам высокопоставленных чиновников ЕС, один из вариантов, рассматриваемых Европейской комиссией, заключается в том, чтобы внести поправки в закон о кибербезопасности от 2016 года. Согласно документу, предприятия, занимающиеся созданием критической инфраструктуры, должны принимать соответствующие меры безопасности…» ***(ЕС может не допустить Huawei к внедрению 5G-связи – Reuters // УНИАН (https://economics.unian.net/telecom/10428918-es-mozhet-ne-dopustit-huawei-k-vnedreniyu-5g-svyazi-reuters.html). 31.01.2019).***

***

Китай

«В Китае создадут национальный индустриальный парк, который возьмет на себя разработку и производство обеспечивающих кибербезопасность продуктов. Строительство идет уже с 2017 года, а производство планируется начать в ближайшее время. По оценкам чиновников, к следующему году масштаб выпуска продукции превысит 100 млрд юаней, что эквивалентно приблизительно $14,5 миллиардам. Сам парк разместится в столице Китая, а именно в двух районах — на западе (Хайдянь) и востоке (Тунчжоу)…» ***(Олег Иванов.В Пекине создадут национальный парк кибербезопасности // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2019-01-17-1447/28571). 17.01.2019).***

***

Російська Федерація та країни ЄАЕС

«Координационный центр доменов .RU/.РФ (КЦ) изучил проблемы, связанные с перехватом трафика и подменой имен в Рунете… Результаты

исследований размещены на информационно-аналитическом портале «Нетоскоп», который публикует данные о борьбе с сетевыми киберугрозами.

Первая работа посвящена подмене DNS-зон в результате перехвата управления адресацией в доменах второго уровня, размещенных в зонах .RU, .РФ и .SU. Это становится возможным при возникновении ошибок делегирования — отнесения доменных имен к некорректным серверам (NS, name server)…

Второе исследование рассматривает проблему перехвата электронной почты в результате подмены имен MX-серверов (mail exchanger). Специалисты проанализировали ситуацию в доменах .RU, .РФ, .SU, .MOSCOW, .TATAR, .ДЕТИ, .МОСКВА…» ***(Dmitry Nazarov. Эксперты оценили защиту российского трафика от перехвата // Threatpost (https://threatpost.ru/experts-examined-russian-domains-security-against-spoofing/30614/). 19.01.2019).***

***

«…Дочерняя компания Сбербанка BI.ZONE, которая специализируется на защите активов и репутации бизнеса в интернете, будет обучать специалистов по кибербезопасности. Вместе с технологическим сообществом Binary District компания проведет курсы по безопасности веб-приложений и расследованию кибератак. Два интенсива пройдут 16-17 февраля на площадке Digital October в Москве.

Слушатели курса «Безопасность веб-приложений» научатся выявлять уязвимости и бороться с ними, познакомятся с актуальными механизмами защиты. Курс подойдет разработчикам веб-приложений, специалистам в области кибербезопасности и тестированию на проникновение…» ***(BI.ZONE будет учить кибербезопасности // SecurityLab.ru (https://www.securitylab.ru/news/497561.php). 23.01.2019).***

***

Інші країни

«…В'єтнам звинуватив соцмережу Facebook у порушенні нового закону про кібербезпеку країни за дозвіл користувачам залишати антиурядові коментарі…

«Facebook порушила новий закон про кібербезпеку В'єтнаму, дозволяючи користувачам розміщувати антиурядові коментарі», - йдеться в повідомленні.

У Міністерстві інформації і зв'язку В'єтнаму заявили, що Facebook дозволяє користувачам завантажувати пости, які містять «наклепницький», антиурядовий контент проти окремих осіб і організацій…» ***(Влада В'єтнаму обурена, що Facebook дозволяє антиурядові коментарі // "Українські медійні системи" (https://glavcom.ua/news/vlada-vjetnamu-oburena-shcho-facebook-dozvolyaje-antiuryadovi-komentari-559465.html). 09.01.2019).***

***

«Министр внутренних дел и связи Японии Масаши Ишида (Masashi Ishida) утвердил правительственные поправки в законодательство, которые позволят госслужащим вторгаться на пользовательские устройства «интернета вещей» в рамках масштабной «переписи» IoT-девайсов.

Сотрудники Национального института информационных и коммуникационных технологий (NICT) методом перебора применят пароли по умолчанию, а также используют «словарные атаки» для взлома случайно выбранных IoT-устройств и составления списка уязвимых девайсов.

На такие меры власти решили пойти преддверие Летних Олимпийских игр 2020, которые пройдут в столице страны, Токио. Во время Олимпиады власти страны опасаются «правительственных» кибератак на инфраструктуру игр...

По итогам этого исследования будет составлен перечень уязвимых устройств, использующих учетные данные по умолчанию или слишком простые пароли. Затем эта информация будет передана властям, а те, в свою очередь, передадут данные интернет-провайдерам, чтобы те могли связаться с владельцами устройств, уведомить их о проблемах и обезопасить «дырявые» IoT-девайсы…» ***(Япония берет устройства «интернета вещей» под тотальный контроль // РосКомСвобода (https://roskomsvoboda.org/44604/). 28.01.2019).***

***

Протидія зовнішній кібернетичній агресії

«Румунія обіцяє посилити кібербезпеку, захистити зовнішні кордони та посилити оборону й безпеку ЄС

Про це заявила прем'єр-міністр Румунії Віоріка Денчіле…

Особливу увагу країна обіцяє приділити посиленню стійкості до зовнішніх втручань до кібернетичного простору ЄС…» ***(Під час головування в Раді ЄС Румунія обіцяє посилити кібербезпеку та зовнішні кордони // Espreso.tv (https://espreso.tv/news/2019/01/16/pid_chas_golovuvannya_v_radi_yes_rumuniya_obicyaye_posylyty_kiberbezpeku_ta_zovnishni_kordony). 16.01.2019).***

***

«Цього року Росія може організувати кібернетичні атаки з метою вплинути на результати виборів в Литві.

…адміністрація президента зазначає, що Литва має достатній імунітет до подібних загроз, а "можливості третіх країн у справі здійснення впливу на Литву обмежені". У повідомленні також йдеться, що в цілому рівень загроз Литві в 2018 році, в порівнянні з колишніми роками, значно не змінився.

Цю позицію прес-служба президента країни Далі Грібаускайте оприлюднила після засідання Державної ради з оборони (ДРО)…» ***(РФ під час виборів у Литві може організувати кібератаки, - адміністрація президента // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (http://day.kyiv.ua/uk/news/080119-rf-pid-chas-***

vyboriv-u-lytvi-mozhe-organizuvaty-kiberataky-administraciya-prezydenta). 08.01.2019).

***

«Чехия из-за подозрений в шпионаже пригрозила России резким сокращением штата посольства РФ в Праге.

Чешская контрразведка заявила, что в 2016 и 2017 годах Россия совершала кибератаки на правительственные структуры и воровала персональные данные чиновников.

…решение о выдворении дипломатов РФ из Праги может быть принято уже в январе на заседании кабинета министров.

Контрразведка Чехии утверждает, что российские дипломатические учреждения имеют большое количество сотрудников, в особенности так называемого обслуживающего персонала. На деле же эти люди могут быть сотрудниками российских спецслужб.» ***(Россия попала в новый скандал: Чехия подготовила мощный удар по Москве // Вести-UA (https://vesti-ua.net/novosti/za-rubezhom/92381-rossiya-popala-v-novyy-skandal-chehiya-podgotovila-moschnyy-udar-po-moskve.html). 05.01.2019).***

***

«Глава Міністерства оборони Франції Флоранс Парлі розповіла про те, що з початку 2017 року на структури відомства здійснили кілька сотень хакерських атак, які були спрямовані на міністерство, французькі військові операції, технічні експертизи і шпиталь…

"У 2017 році відбулося 700 інцидентів, пов'язаних з безпекою, серед яких - близько сотні кібератак, спрямованих на структури міністерства", - сказала Парлі. "У 2018 році такі ж показники були зафіксовані вже до вересня".

Вона зазначила, що походження кібератак - різне…» ***(Хакери атакували Міноборони Франції кілька сотень разів за два роки // «Дзеркало тижня. Україна». (https://dt.ua/WORLD/hakeri-atakuvali-minoboroni-franciyi-kilka-soten-raziv-za-dva-roki-299996_.html). 18.01.2019).***

***

«Американські спецслужби попередили про загрозу з боку Росії, Китаю та КНДР, - про це йдеться у новій Національній стратегії розвідки США на наступних 4 роки…

Особливу увагу американські розвідники планують приділити кіберзагрозам. Більшість із них надходитиме, знову ж таки, від Росії та Китаю, ще частина - від терористичних та кримінальних угруповань.» ***(Спецслужби США затвердили нову розвідувальну стратегію // ООО "Национальные информационные системы" (http://podrobnosti.ua/2279896-spetssluzhbi-ssha-zatverdili-novu-rozvduvalnu-strategju.html). 23.01.2019).***

***

«Франция озаботилась вопросом инвестиции дополнительных средств в укрепление кибербезопасности страны.

Согласно новой стратегии, о которой рассказала министр обороны Флоранс Парли, правительство в ближайшие пять лет вложит 1,6 миллиардов евро в усиление кибероборонны. Помимо финансовых вливаний, Франция готова нанять дополнительно 1 тысячу специальных бойцов киберподразделения.

Таким образом, после реализации задуманного во Франции будут насчитываться 4 тысячи кибербойцов. В Министерстве обороны особо подчеркнули постоянно актуальную проблему кибервойны, к которой Франция относится со всей серьезностью. Министр отметила, что армия страны должна быть готова к ответным действиям в случае столкновения в цифровом пространстве...» ***(Олег Иванов. В ближайшие 5 лет Франция вложит €1,6 млрд в кибербезопасность страны // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2019-01-21-1447/28596). 22.01.2019).***

***

Кіберзахист критичної інфраструктури

«Инженеры и специалисты по безопасности нефтехимического завода в Саудовской Аравии могли предотвратить повторную атаку вредоносного ПО Trisis (другое название Triton) в августе 2017 года, но не сделали этого. Об этом сообщается в докладе специалистов, занимавшихся расследованием инцидента. Доклад был представлен во вторник, 15 января, на конференции S4 Conference 2019…

Первая атака на принадлежащий компании Tasnee нефтехимический завод в Саудовской Аравии была осуществлена в июне 2017 года. Как сообщил исследователь безопасности Джулиан Гутманис (Julian Gutmanis), расследованию инцидента было уделено недостаточно внимания…

Случившееся рассматривалось как технический сбой в работе, а не как кибератака, и после устранения неполадок все операции были восстановлены.

В результате недостаточного расследования злоумышленники снова атаковали завод спустя два месяца, и на этот раз атака затронула не один, а сразу шесть контроллеров. В результате каждой атаки завод прекращал работу на неделю, что привело к серьезным финансовым потерям.

В ходе атак злоумышленники использовали вредоносное ПО для АСУ ТП под названием Trisis. Вредонос проникает в системы противоаварийной защиты, в случае необходимости отключающие производственные процессы, в частности в Triconex от Schneider Electric...» ***(Второй атаки на нефтехимический завод в Саудовской Аравии можно было избежать // Goodnews.ua (http://goodnews.ua/technologies/vtoroj-ataki-na-neftexim icheskij-zavod-v-saudovskoj-aravii-mozhno-bylo-izbezhat/). 16.01.2019).***

***

«Номера кредитных карт, телефонов и паспортов, счета и письма известных политиков Германии, опубликованные в интернете через серию ссылок в Twitter, были замечены поздно вечером 3 января. Об этом на пресс-конференции рассказал представитель правительства ФРГ Мартин Фитц… В открытом доступе они находятся с конца декабря.

Фитц уточнил, что попавшие в сеть документы принадлежат как частным лицам, так и немецким политикам всех уровней от муниципальных комитетов, бундестага и Европарламента до федерального канцлера Германии Ангелы Меркель...

Предположительно, данные попали в сеть в результате кибератаки, однако правительство Германии не исключает, что речь может идти не о взломе, а об утечке информации. К расследованию инцидента подключились Федеральное ведомство по безопасности в сфере информационной техники (BSI), Федеральное ведомство уголовной полиции и Федеральное ведомство по защите конституции. Спецслужбы блокируют доступ к выложенным в открытый доступ данным…» ***(В интернет выложены личные данные Меркель и других политиков Германии // АО Бизнес Ньюс Медиа (https://www.vedomosti.ru/politics/news/2019/01/04/790828-dannie-merkel). 04.01.2019).***

***

«Персональные данные сотен немецких политиков, в частности канцлера Ангелы Меркель, опубликованные онлайн в результате массовой хакерской атаки в Германии.

…расследование может пролить свет на проблему постоянных хакерских атак, которые часто бьют по Германии. Если, например, немцы докажут причастность к ним российских спецслужб, это станет очередным витком кризиса между Западом и РФ, а также создаст очередной повод сохранить антироссийские санкции…» ***(Эксперт рассказал, чему Украину должна научить хакерская атака на Германию // Gazeta.ua (https://gazeta.ua/ru/articles/life/_ekspert-rasskazal-chemu-ukrainu-dolzhna-nauchit-hakerskaya-ataka-na-germaniyu/879397). 13.01.2019).***

***

«Базу даних у мережі знайшов експерт з питань веб-безпеки Трой Хант (Troy Hunt). Файл з інформацією був розміщений на хмарному сервісі …MEGA, а також «популярному для хакерів форумі».

Файл з інформацією називався Collection #1 (колекція #1), важив 87 гігабайт та містив 12 тис. папок. У них була інформація із 772,9 млн електронними поштами та 21,2 млн паролями…

Такі списки даних можуть полегшити хакерам злам електронних пошт…

Пан Хант очистив знайдені дані та додав до бази сайту «Have I Been Pwned».

…у знайденому списку були 140 млн пошт і 10 млн паролів, яких раніше не було у базі Троя Ханта. Тобто ця інформація не була скопійована з попередніх витоків даних…» ***(У мережу виклали 770 млн викрадених електронних адрес та 21 млн паролів // MediaSapiens (https://ms.detector.media/web/cybersecurity/u_merezhu_viklali_770_mln_elektronnikh_adres_ta_21_mln_paroliv/). 18.01.2019).***

***

«Система бронирования авиабилетов Amadeus, которую использует почти половина авиалиний по всему миру, оказалась уязвима перед брутфорс-атаками…

ИБ-эксперт Ноам Ротем (Noam Rotem) обнаружил проблему, когда покупал билеты у одной из израильских авиакомпаний. Он обратил внимание, что при отправке данных в Amadeus в URL содержится номер бронирования. На следующей странице можно увидеть уникальный идентификатор пассажира (passenger name record, PNR), который открывает доступ к значительному массиву личной информации.

…По словам эксперта, через эту лазейку злоумышленники могут попасть в личный кабинет пользователя, поменять его данные, перевести бонусные мили на свой счет, изменить или отменить запланированные поездки.

Атаку можно автоматизировать с помощью скрипта, который будет перебирать номера бронирования в адресе и сохранять собранную информацию…

По информации на сайте Amadeus, систему используют свыше 100 авиакомпаний более чем на 260 сайтах. Эксперты утверждают, что все они уязвимы перед описанной атакой, поскольку в каждом случае обмен данными происходит одинаково.

Специалисты Safety Detective, с которыми сотрудничает Ротем, сообщили об уязвимости Amadeus. Разработчики быстро отчитались об устранении угрозы, однако при внимательном изучении принятые меры оказались косметическими.

Как объяснили эксперты, персональные данные пассажира действительно пропали со страницы бронирования, но их по-прежнему можно увидеть в HTML-коде. В отсутствие защиты от атак перебором злоумышленники могут реализовать тот же сценарий с минимальными изменениями…» ***(Egor Nashilov. Авиапассажирам угрожает уязвимая система бронирования // Threatpost (https://threatpost.ru/amadeus-that-rocked/30597/). 18.01.2019).***

***

«…Аналитический центр InfoWatch составил дайджест крупнейших утечек из банков, финансовых и страховых компаний за 2018 год.

Австралийский банк Содружества (The Commonwealth Bank) признался, что допустил утечку данных 19,8 млн счетов, которые были открыты 12 млн человек

(примерно половина населения Австралии). Инцидент произошел в процессе демонтажа устаревшего дата-центра…

В США компания Government Payment Service, которая управляет онлайн-платежами 2300 государственных структур в 35 штатах, непреднамеренно скомпрометировала данные порядка 14 млн клиентов. В течение как минимум шести лет на сайте компании была доступна такая информация, как имена, адреса, номера телефонов и последние четыре номера кредитных карт…

Американский SunTrust Bank заявил, что бывший сотрудник распечатывал данные клиентов и передавал эти файлы представителям преступного мира. Всего могла быть скомпрометирована информация 1,5 млн клиентов: имена, адреса, номера счетов и сумма остатков.

Один из ведущих финансовых провайдеров в ЮАР, компания Liberty, сообщила о взломе, в результате которого были украдены данные около миллиона клиентов. Нарушение затронуло имена, ID-номера, мобильные номера, электронные адреса и незашифрованные пароли.

Крупные финансовые потери в минувшем году главным образом понесли криптовалютные биржи. Судя по всему, уровень киберзащиты многих подобных стартапов пока значительно ниже, чем у классических финансовых компаний…» ***(Крупнейшие утечки из финансового сектора в 2018 году // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5559264-Krupnejshie-utechki-iz-finansovogo.html#ixzz5dLJPsCGv). 21.01.2019).***

***

«Исследователь проблем кибербезопасности Боб Дьяченко обнаружил в сети очередную незащищенную базу данных MongoDB. Новая находка впечатляет масштабами: размер базы данных на момент обнаружения составлял около 854 гигабайт.

База содержала 202 730 434 записи персональных данных граждан КНР, ищущих работу. Информация включала имена, даты рождения, номера телефонов, адреса электронной почты, а также описания профессиональных навыков и ожидания соискателей по уровню заработной платы. По словам экспертов, такой массив данных - настоящая золотая жила для киберпреступников, специализирующихся на организации фишинговых атак…» ***(Данные свыше 200 миллионов жителей КНР нашлись в открытом доступе // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5558112-Dannye-svyshe-200-millionov-zhitele.html#ixzz5dLKO0cT7). 15.01.2019).***

***

«…Базу клиентов небанковского сервиса кредитования Moneyveo.UA, актуальную на 2017 год и содержащую 256 625 записей о клиентах, включая их фамилии, дату рождения, телефон, e-mail, и паспортные данные, обнаружил в сети специалист по кибербезопасности Андрей Перевезий…

Как оказалось, в компании знают об утечке данных и по этому факту возбуждено уголовное дело…

В Moneyveo подчеркнули, что постоянно совершенствуют все уровни защиты информации, которую пользователи предоставляют компании, а на предприятии установлена многоуровневая система доступа сотрудников к данным…

Также в компании уверяют, что регулярно проверяют систему доступа к данным сервиса и не допускают появления в ней уязвимостей…» ***(Владимир Кондрашов. Эксперт: база клиентов крупного сервиса онлайн-кредитов "ушла" к хакерам // Internetua (http://internetua.com/ekspert-baza-klientov-krupnogo-servisa-onlain-kreditov-ushla-k-hakeram). 28.01.2019).***

***

«В сети распространилась обширная база ворованных данных, составленная из 2,2 миллиарда уникальных логинов и паролей пользователей…

По мнению специалистов, база составлена из различных массивов данных, полученных хакерами в последние годы. Среди основных источников они назвали утечки из хранилищ Yahoo, LinkedIn и Dropbox.

Сотрудник Института имени Хассо Платтнера в Германии Дэвид Джагер (David Jaeger) предположил, что некоторые части массива могли быть получены с помощью автоматического взлома небольших и малоизвестных сайтов. Это означает, что часть паролей была опубликована впервые.

Массив получил название Collection #2-5. За несколько дней он был загружен более тысячи раз…» ***(Обнаружена еще одна крупнейшая в истории база ворованных данных // Goodnews.ua (http://goodnews.ua/technologies/obnaruzhena-eshhe-odna-krupnejshaya-v-istorii-baza-vorovannyx-dannyx/). 31.01.2019).***

***

Кіберзлочинність та кібертероризм

«Совместная команда ученых и исследователей в области кибербезопасности описала новую атаку по сторонним каналам, эффективную против систем на базе Windows и Linux…

Целью новой атаки являются так называемые «страничные кэши» — область памяти, куда операционная система загружает код (исполняемые файлы, библиотеки, пользовательские данные), используемые одним или несколькими приложениями. В отличие от классической аппаратной кэш-памяти такие кэши управляются на уровне операционной системы…

Новый метод эксплуатирует механизмы в ОС Windows (системный вызов «QueryWorkingSetEx») и Linux («mincore»), позволяющие разработчику/приложению проверить наличие страницы памяти в страничном кэше…

Данная атака может использоваться для обхода песочниц, модификации пользовательского интерфейса и записи нажатий клавиш. Исследователи отмечают,

что метод может быть адаптирован для удаленного применения, но в таком случае он будет менее эффективен, поскольку не позволит обойти песочницы.

Компания Microsoft уже исправила проблему в сборке 18305 для Windows Insiders, разработчики Linux также готовят соответствующий патч…» ***(Новая атака по сторонним каналам представляет угрозу для ПК на Windows и Linux // Goodnews.ua (http://goodnews.ua/technologies/novaya-ataka-po-storonnim-kanalam-predstavlyaet-ugrozu-dlya-pk-na-windows-i-linux/). 09.01.2019).***

***

«В сети обнаружена новая версия печально известного вредоносного ПО Shamoon. Отличительной особенностью версии является то, что зловред тщательно замаскирован под легитимный продукт – средство оптимизации системы от крупной китайской технологической компании Baidu.

Образец вредоносного ПО был загружен в базу VirusTotal из Франции 23 декабря.

Исполняемый файл носит имя Baidu PC Faster и даже снабжен цифровым сертификатом подлинности от Baidu. Сертификат, впрочем, был выпущен 25 марта 2015 года и срок его действия истек 26 марта 2016.

Shamoon – опасное вредоносное ПО, рассматриваемое многими как средство ведения кибервойны. Зловред способен распространяться как вирус, уничтожая информацию на жестких дисках компьютеров без возможности восстановления…» ***(Обнаружена новая версия зловреда Shamoon // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5556958-Obnaruzhena-novaya-versiya-zlovreda.html#ixzz5dLKqWil4). 09.01.2019).***

***

«APT-группировка DarkHydrus запустила новую вредоносную кампанию. Злоумышленники взяли на вооружение обновленный вариант трояна RogueRobin и в качестве альтернативного канала связи с ним используют Google Диск.

В ходе последней кампании группировка атаковала цели на Среднем Востоке. Троян попадал на компьютеры жертв через документ Excel с вредоносным кодом VBA (макросом). Атака была зафиксирована 9 января 2019 года специалистами китайского 360 Threat Intelligence Center (360 TIC). Эксперты отнесли ее на счет группировки DarkHydrus, которую «Лаборатория Касперского» называет Lazy Meerkat…

DarkHydrus компилировали RogueRobin с добавлением новой функции, позволяющей трояну использовать Google Диск в качестве альтернативного канала связи для получения инструкций. Команда x_mode отключена по умолчанию, однако ее можно включить через канал туннелирования DNS – основной канал связи трояна с C&C-сервером.» ***(APT-группировка DarkHydrus управляет трояном RogueRobin через Google Диск // Информационная безопасность (http://www.itsec.ru/news/apt-gruppirovka-darkhydrus-upravliayet-trojanom-rogue-robin-cheres-google-disc). 21.01.2019).***

***

«Злоумышленник получил доступ к устройству с помощью ранее утекших учетных данных.

Смарт-камера Nest, использовавшаяся для видеонаблюдения за домом, вызвала панику у американской семьи, сообщив о запуске Северной Кореей межконтинентальных баллистических ракет, якобы направляющихся на Лос-Анджелес, Чикаго и Огайо.

…В один воскресный день в доме Лайонс раздалась сирена тревоги и голос сообщил о ядерном ударе по США со стороны Северной Кореи.

…Как оказалось, источником тревоги являлся динамик «умной» камеры Nest, установленной в доме...» ***(«Умная» камера испугала пользователей сообщением о ядерном ударе по США // SecurityLab.ru (https://www.securitylab.ru/news/497560.php). 23.01.2019).***

***

«Специалистам в области кибербезопасности со всего мира удалось объединиться и прикрыть около 100 00 вредоносных сайтов.

Такое стало возможным благодаря тому, что эксперты делились между собой URL, которые использовались во вредоносных кампаниях. Этот проект получил имя URLhaus, его инициатором выступила некоммерческая ИБ-организация abuse.ch, которая базируется в Швейцарии.

URLhaus запустили в марте 2018 года, в день поступало около 300 сообщений от 265 исследователей. Чтобы «положить» злонамеренные сайты, потребовалось привлечь к инициативе хостинговые компании, которые предоставляли площадку таким ресурсам...» ***(Олег Иванов. Эксперты общими усилиями положили 100 000 вредоносных сайтов // ООО «АМ Медиа» (https://www.anti-malware.ru/news/2019-01-23-1447/28640). 23.01.2019).***

***

Діяльність хакерів та хакерські угруповування

«…У вересні 2017 року Комісія з цінних паперів і бірж Сполучених Штатів Америки (SEC) заявила про виявлення зламу своєї корпоративної бази даних Edgar. Ці сервери використовують компанії, які керують капіталами…

У США вважають, що до хакерської атаки причетний 27-річний Олександр Єременко з Києва та кілька його спільників. Хакери зуміли отримати доступ до тисяч документів та оголошень про доходи.

Базу даних SEC зламали через литовський сервер, а викрадену інформацію надали вісьмом трейдерам із США, Російської Федерації та України. Вони, торгуючи вкраденими даними, заробили понад 4,1 млн дол.

До окружного суду США в Ньюарку, штат Нью-Джерсі, вже подано обвинувальний акт. Міністерство юстиції США звинуватило хакерів у комп’ютерному шахрайстві та інших злочинах.

SEC подала відповідні цивільні обвинувачення проти Єременка і ще вісьмох підозрюваних…» ***(Українського хакера звинуватили у зламі бази даних Комісії з цінних паперів і бірж США — Reuters // Racurs.ua® (https://racurs.ua/ua/n116854-ukrayinskogo-hakera-zvynuvatyly-u-zlami-bazy-danyh-komisiyi-z-cinnyh-paperiv-i-birj-ssha-reuters.html). 15.01.2019).***

***

«…По данным исследователей кибербезопасности из команды Crowdstrike, с августа 2018 г., когда появилось ransomware Ryuk, преступники с его помощью получили от жертв в 53 транзакциях на 37 Bitcoin-кошельков 705,8 BTC (3,7 млн долл.)…

Факты, которыми располагают эксперты, позволяют предположить, что программу, известную как Ryuk, создала криминальная группа Grim Spider, усовершенствовав купленную на хакерском форуме версию конструктора ransomware – Hermes...

CrowdStrike утверждает, что Grim Spider вероятнее всего является ячейкой базирующейся в России крупной преступной организации Wizard Spider, которая считается ответственной за создание банковского трояна TrickBot.

По данным CrowdStrike, Kryptos Logic и FireEye многие жертвы Ryuk были предварительно инфицированы TrickBot. Исследователи предполагают, что из десятков тысяч заражённых TrickBot компьютеров злоумышленники выбирали цели для применения Ryuk…» ***(Операторы ransomware Ryuk охотятся за «крупной дичью» // «Компьютерное Обозрение» (https://ko.com.ua/operatory_ransomware_ryuk_ohotyatsya_za_krupnoj_dichyu_127423). 15.01.2019).***

***

«Хакеры, следы которых ведут в Россию, в 2016-2017 годах проводили целенаправленные атаки на сотни подрядчиков в США и готовили плацдарм для масштабной диверсии с целью вывода из строя энергетической системы США…

В Министерстве внутренней безопасности (МВБ) США пришли к выводу, что у атак был российский след. Некоторые подробности произошедшего стали известны из бесед с представителями подвергнувшихся взлому предприятий, благодаря изучению документов и архивов компьютерных данных, интервью с бывшими и действующими должностными лицами США, а также с экспертами. Просуммировав данные, WSJ пришла к выводу, что российские хакеры в 2016-2017 годах с целью внедрения в компоненты энергосистемы Соединенных Штатов проводили диверсии в отношении сотен фирм-подрядчиков в 24 американских штатах, а также в Канаде и Великобритании…

Российская сторона обвинения в причастности к хакерским нападениям неоднократно отвергала…» ***(Российские хакеры атаковали американскую енергетику // CRiME (http://crime-ua.com/node/24951). 12.01.2019).***

***

«Северокорейским киберпреступникам удалось проникнуть в компьютерную сеть компании Redbanc, обслуживающей инфраструктуру банкоматов всех банков в Чили, благодаря наивному сотруднику фирмы и одному звонку в Skype.

Предположительно, взлом был осуществлен проправительственной группировкой Lazarus Group (она же Hidden Cobra), известной своими атаками на банки, финансовые организации и криптовалютные биржи по всему миру.

…атака стала возможна благодаря одному из сотрудников Redbanc, ответившему на объявление о вакансии разработчика в соцсети LinkedIn. Компания, разместившая объявление, оказалась прикрытием участников Lazarus Group, которые не преминули воспользоваться предоставленной возможностью…

Вредоносная программа собирала информацию о компьютере сотрудника Redbanc и отправляла ее на удаленный сервер. Данные включали имя ПК, сведения об аппаратном обеспечении и операционной системе, настройках прокси, текущих процессах, общедоступных папках, статусе подключения по RDP и пр. На основе данной информации злоумышленники могли сделать вывод о «ценности» инфицированного ПК и решить, стоит ли загружать дополнительное более интрузивное вредоносное ПО…» ***(Для доступа к сети банкоматов в Чили оказалось достаточно звонка в Skype // Goodnews.ua (http://goodnews.ua/technologies/dlya-dostupa-k-seti-bankomatov-v-chili-okazalos-dostatochno-zvonka-v-skype/) 16.01.2019).***

***

«Группировка Silence провела масштабную атаку на российский финансовый сектор, для прикрытия воспользовавшись деловой повесткой. Письмо с опасным зловредом, замаскированное под приглашение на предстоящий в феврале форум iFin-2019, получили десятки тысяч сотрудников банков и крупных платежных систем.

Первые зараженные сообщения были зафиксированы 16 января, через несколько часов после рассылки официального приглашения на форум…

Помимо этой рассылки в рамках январской кампании специалисты Group-IB обнаружили еще две — от имени несуществующих банков «Банк ICA» и «Банкуралпром». В тексте содержалась просьба оперативно открыть корреспондентский счет, во вложении якобы находился договор.

Во всех случаях при открытии прикрепленного ZIP-архива на компьютер жертвы загружался троян Silence, он же TrueBot. При помощи этого зловреда преступники закрепляются в зараженной системе и мониторят работу организации. Собрав необходимую информацию, они крадут средства со счетов банка…» ***(Julia Glazova. Атака APT Silence затронула более 80 тыс. адресатов // Threatpost (https://threatpost.ru/new-silence-attack-had-80-thousand-addressees-in-russian-financial-organizations/30620/). 19.01.2019).***

***

«Официальный репозиторий пакетов PEAR (PHP Extension and Application Repository) подвергся взлому. Около полугода назад неизвестные

получили несанкционированный доступ к web-серверу PEAR и внесли изменения в файл go-pear.phar, содержащий установочный комплект с пакетным менеджером go-pear…

В связи со взломом сайт PEAR был временно отключен…» ***(Неизвестные взломали репозиторий пакетов PEAR // Информационная безопасность (http://www.itsec.ru/news/neizvestnie-vzlomali-repositoriy-paketov-pearl). 21.01.2019).***

***

«Неизвестные взломали компьютерную сеть Агентства по оборонным закупкам Южной Кореи (структура Министерства национальной безопасности) и похитили документы, касающиеся закупки вооружения для истребителей нового поколения…

По имеющимся данным, атакующие проникли в сеть через приложение под названием «Data Storage Prevention Solution», установленное на всех правительственных компьютерах для предотвращения загрузки и сохранения конфиденциальных документов на подключенных к интернету ПК. Злоумышленникам удалось получить доступ с правами администратора к серверу приложения и с его помощью похитить информацию с подключенных к нему рабочих станций. Атакующие смогли взломать 30 компьютеров и украсть данные по меньшей мере с 10 из них…» ***(Агентство по оборонным закупкам Южной Кореи стало жертвой кібератаки // Информационная безопасность (http://www.itsec.ru/news/agenstvo-po-oboronnim-sakupkam-yuzhnoy-korei-stalo-zhertvoy-kiberataki). 17.01.2019).***

***

«Федерация экономических организаций Японии в течение продолжительного периода времени подвергалась масштабным кибератакам…

По данным японских и британских спецслужб, ответственность за кибератаку «более чем вероятно» лежит на группировке APT10, предположительно финансируемой Минобороны КНР…

Федерация экономических организаций Японии подвергалась кибератакам со стороны APT10 в течение двух лет до осени 2016 года. …в 2014 году сотрудник организации получил фишинговое письмо с вирусом, распространившимся на ее серверы.

С помощью вируса злоумышленники могли перехватывать данные, которыми обменивались федерация и правительство Японии. Вредонос перехватывал информацию и передавал ее на компьютеры за пределами страны.» ***(Федерация экономических организаций Японии подвергалась атакам APT10 // Информационная безопасность (http://www.itsec.ru/news/federaziya-ekonomicheskih-organisaziy-iaponii-podverglas-atakam-art10). 16.01.2019).***

***

«В Google Play в очередной раз обнаружили вредоносные приложения. Исследователи из Trend Micro обнаружили десятки приложений, популярные утилиты и игры, у которых есть масса обманчиво отображаемой рекламы (чтобы выжать как можно больше денег из ничего не подозревающих пользователей Android)…

Так, 85 приложений "продвигают" рекламное ПО, что в общей сложности затрагивает не менее 9 миллионов пользователей…

Исследователи протестировали все приложения и обнаружили, что большинство из них используют один и тот же или похожий код, и часто имеют одинаковые названия. При каждом клике приложение будет показывать рекламу – таким образом приложение генерирует деньги для разработчика…

Некоторые объявления могут содержать скрытый код, который пытается обманом заставить пользователей установить вредоносное ПО на свои телефоны или компьютеры. Некоторые из них: A/C Air Conditioner Remote, Police Chase Extreme City 3D Game, Easy Universal TV Remote, Garage Door Remote Control, Prado Parking City 3D Game.

Несмотря на все усилия Google по сканированию приложений до того, как они появятся в Google Play, вредоносные программы представляют собой одну из самых больших и распространенных угроз для пользователей Android…

Тем не менее, поисковый и мобильный гигант продолжает борьбу с мошенническими и вредоносными приложениями, допустив появление в Google Play по меньшей мере 13 вредоносных программ только в ноябре.» **(Ирина Фоменко. Google Play опять "грузит" пользователей Android вредоносным софтом // Internetua (http://internetua.com/google-play-opyat-gruzit-polzovatelei-android-vredonosnym-softom). 08.01.2019).**

***

«Исследователь в области кибербезопасности Брэд Данкан (Brad Duncan) рассказал о вредоносных рассылках, маскирующихся под любовные письма....

По словам эксперта, в опасных посланиях скрывается сразу три заражающих компонента. Речь идет о вирусе-шифровальщике GandCrab, спамботе Phorpiex и программе-майнере XMRig. Под удар попадают все компьютеры на Windows, а также подключенные к ним носители.

Все имена вложений начинались с сочетания Love_You_. Загрузка вредного ПО происходит после распаковки приложенного к письму ZIP-файла. В этот архив вшит загрузчик опасных программ…

Сообщается, что волна опасной рассылки началась еще в ноябре 2018 года и продолжается до сих пор…» ***(В любовных письмах нашли сразу три угрозы комп'ютеру // Goodnews.ua (http://goodnews.ua/technologies/v-lyubovnyx-pismax-nashli-srazu-tri-ugrozy-kompyuteru/). 16.01.2019).***

***

«…Китайская компания …TCL, владеющая правами на торговые марки Alcatel, Blackberry и Palm, обвинили в обмане клиентов. Так, утверждают эксперты британской компании Upstream, компания перед продажей современных телефонов устанавливала на них вирусное приложение Simplicity Weather.

Программа не только показывала погоду, но и шпионила за своих хозяином, собирая всю пользовательскую информацию (адреса электронной почты, геолокацию, IMEI-идентификатор) и отсылая данные на серверы в Китае. Кому они принадлежат, выяснить пока не получается…» ***(Популярный бренд установил на смартфоны вирус-шпион // Politeka (https://politeka.net/news/hightech/873287-populjarnyj-brend-ustanovil-na-smartfony-virus-shpion/). 15.01.2019).***

***

«Эксперты в области кибербезопасности нашли более десятка приложений для iPhone, тайно взаимодействующих с сервером, связанным с Golduck…

Программа Golduck …инфицировала классические ретро-игры на Google Play путем встраивания кода, который позволял незаметно передавать вредоносные данные на устройство. В свое время Golduck появился на гаджетах более 10 миллионов пользователей, что позволило хакерам запускать различные вирусные команды. Способом заработать деньги злоумышленники видели, к примеру, возможность отправки SMS-сообщений с зараженного смартфона.

Теперь исследователи говорят, что и приложения для iPhone, связанные с вредоносным ПО, также могут представлять опасность.

Wandera, компания по обеспечению безопасности предприятий, обнаружила 14 приложений для iOS, которые обменивались данными с одним и тем же сервером управления и контроля, используемым вредоносным ПО Golduck. Приложения, обнаруженные Wandera, также выглядят как невинные ретро-игры. Сами по себе они не являются вредоносными программами, но предлагают хакерам доступ к iOS-устройству жертвы… На момент написания новости все приложения из App Store удалили…» ***(Доверяете ли вы, всем приложениям, которые скачиваете на свой iPhone? // ProPro (http://propro.com.ua/archives/15714). 07.01.2019).***

***

«Как сообщили исследователи компании Palo Alto Networks, попав на сервер Linux, прежде чем начать майнинг, вредонос полностью удаляет облачные решения безопасности. Его распространением занимается китайскоговорящая киберпреступная группировка Rocke, специализирующая на майнинге криптовалюты Monero с помощью зараженных компьютеров под управлением Linux.

Если раньше используемое группировкой ПО пыталось обойти обнаружение путем отключения некоторых функций в облачных решениях безопасности, то теперь оно деинсталлирует эти решения полностью. По словам исследователей, киберпреступники добавили в программу код для получения административного доступа к инфицированному серверу и удаления пяти разных сервисов

безопасности от Tencent Cloud и Alibaba Cloud: Alibaba Threat Detection Service; Alibaba Cloud Monitor; Alibaba Cloud Assistant; Tencent Host Security и Tencent Cloud Monitor.

Как отмечают исследователи, данный вредонос является первым, обладающим уникальной способностью удалять с атакуемой системы облачные решения безопасности. Он запрограммирован на удаление вышеупомянутых сервисов строго в соответствии с инструкциями по их удалению, опубликованными на официальных сайтах Tencent Cloud и Alibaba Cloud…» ***(Новое ПО для криптоджекинга удаляет с атакуемых серверов облачные решения безопасности // Информационная безопасность (http://www.itsec.ru/news/novoye-po-dlia-kryptojakinga-udaliayet-s-atakuemih-serverov-oblchnie-resheniya-bezopasnosti). 18.01.2019).***

***

«Распространяемое через The Pirate Bay и замаскированное под видеофайл вредоносное ПО заражает компьютеры под управлением Windows и выполняет ряд вредоносных функций. К примеру, вредонос способен внедрять подготовленный злоумышленником контент на такие популярные сайты, как Википедия, Google или Яндекс.

Помимо внедрения контента на множество сайтов, вредонос отслеживает страницы кошельков Bitcoin и Ethereum и заменяет их другими, принадлежащими киберпреступникам.

Чтобы проделать все вышеописанное, вредонос модифицирует ключи реестра для отключения Windows Defender. ПО также принудительно устанавливает в Firefox расширение Firefox Protection и взламывает расширение для Chrome под названием Chrome Chrome Media Router, заменяя ID на «pkedcjkdefgpdelpbcmbmeomcjbeemfm».

Сразу после запуска браузера вредоносное расширение подключается к базе данных Firebase и извлекает оттуда множество настроек, в том числе JavaScript-код для внедрения в различные web-страницы.

В страницу поисковой выдачи Google вредонос внедряет нужные злоумышленнику результаты поиска (к примеру, сайты, предлагающие подозрительное антивирусное ПО). То же самое происходит и с другими поисковиками...» ***(Распространяемый через The Pirate Bay поддельный видеофайл подменяет результаты поиска в Google // Информационная безопасность (http://www.itsec.ru/news/rasprostraniayemiy-cherez-the-pirate-bay-poddelniy-videofile-podmeniayet-resultati-poiska-v-google). 16.01.2019).***

***

«Фахівці в сфері кібербезпеки заявили про поширення хакерських атак з використанням вірусу-здирника Djvu…

У комп’ютер користувача шкідливе ПЗ потрапляє під час скачування так званих кряків (програм для злому ліцензійного софту та ігор), а також додатки для блокування рекламних банерів у браузері.

Завдяки вірусу на комп'ютер завантажуються чотири файли, які паралізують роботу операційної системи. При цьому на екрані з'являється повідомлення про оновлення Windows.

Шкідлива програма також здатна шифрувати нові файли. А після зараження користувач може знайти контакти здирників. За словами аналітиків, повернути дані без надання допомоги хакерами поки неможливо.» ***(RomanK. У Windows потрапляє небезпечний вірус // BusinessUA.Com (http://businessua.com/telekom/49812u-windows-potraplyae-nebezpechnii-virus.html#). 10.01.2019).***

***

«Главной угрозой для компаний по всему миру остаются скрытые вирусы-майнеры. Об этом LetKnow.News сообщил поставщик решений по кибербезопасности Check Point Software Technologies Ltd.

Как отмечается, в прошлом году криптомайнеры стабильно занимали первые четыре строчки рейтингов самых активных угроз и атаковали 37% организаций по всему миру. В 2019 году, несмотря на снижение стоимости всех криптовалют, 20% компаний продолжают подвергаться атакам криптомайнеров каждую неделю…

На втором месте по распространенности оказались атаки мобильного вредоносного ПО, которые в 2018 году затронули 33% организаций по всему миру. Распространение вирусов происходит как через предварительно установленные приложения, так и через магазины приложений.

Третьими по распространенности стали многовекторные ботнеты: они атаковали 18% организаций с целью запуска DDoS-атак и распространения других вредоносных программ. В 2018 году 49% организаций, подвергшихся DDoS-атакам, были заражены ботнетами.

Вместе с тем, специалисты Check Point зафиксировали значительное падение доли программ-вымогателей — в 2018 году они затронули лишь 4% организаций во всем мире…» ***(Компании страдают от нашествия вирусов-майнеров // «Letknow HQ ltd.» (https://letknow.news/news/kompanii-stradayut-ot-nashestviya-virusov-maynerov-17105.html). 30.01.2019).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Федеральное управление уголовной полиции задержала подозреваемого в краже огромного количества личных данных. Речь идет о 20-летнем парне из Среднего Гессена, …который …еще учится в школе и живет с родителями… Подозреваемый временно задержан. Но свой компьютер… он уничтожил до прибытия полицейских. Расследование по факту подозрения в шпионаже и незаконной публикации личных данных ведет Генеральная прокуратура Франкфурта и Федеральное управление уголовной полиции…

Третьего и четвертого января в интернете появилось огромное количество личных данных политиков, знаменитостей, журналистов, деятелей искусства и других публичных личностей. Личные данные известных людей публиковались в Twitter еще с декабря…» ***(Виктория Холоденина. Задержан подозреваемый в осуществлении масштабной хакерской атаки // GERMANIA (https://germania.one/zaderzhan-podozrevaemyj-v-osushhestvlenii-masshtabnoj-hakerskoj-ataki/). 08.01.2019).***

***

«Решением лондонского суда Короны 30-летний житель графства Суррей Дэниел Кей (Daniel Kaye) наказан лишением свободы на 2 года и 8 месяцев за DDoS-атаки на либерийского телеоператора Lonestar Cell. В Германии за те же преступления он получил меньший срок, притом условно.

…британца нанял неназванный руководитель либерийской телекоммуникационной компании Cellcom, стремившийся подорвать репутацию конкурента. Первые заказные DDoS-атаки на Lonestar Cell были проведены в октябре 2015 года...

В сентябре 2016 года исполнитель начал строить собственную бот-сеть на основе IoT-зловреда Mirai… Через месяц новый ботнет, составленный из уязвимых IP-камер производства Dahua, был пущен в ход против той же мишени. Совокупный мусорный трафик был настолько внушителен, что перебои с интернет-связью начали испытывать все жители Либерии.

В итоге масштабные DDoS-атаки удалось остановить путем отключения C&C-домена ботнета, но заказ на подрыв репутации Кей успел выполнить: клиенты Lonestar стали переходить к другим операторам, и компания начала терять доход. Кроме того, ей пришлось потратить около 600 тыс. долларов США на меры противодействия мощным атакам. Совокупный ущерб от похождений дидосера в Либерии измеряется десятками тысяч долларов США.

К концу 2016 года владелец DDoS-ботнета предпринял попытки расширить его путем заражения роутеров в обширных сетях Deutsche Telekom, Post Office и TalkTalk. В итоге в конце ноября – начале декабря численность его армии, получившей известность как Mirai #14 и Annie, возросла до 3,2 млн. устройств. К этому времени Кей уже пользовался сетевым псевдонимом Bestbuy и предлагал свой ботнет в аренду другим дидосерам.

Тем временем правоохранительные органы Германии и Великобритании запустили расследование. По его итогам был выдан европейский ордер на арест Кея, и в феврале 2017 года тот, вернувшись на родину, оказался под стражей…» ***(Maxim Zaitsev. Британцы сурово обошлись с дидосером, атаковавшим Либерию // Threatpost (https://threatpost.ru/daniel-kaye-jailed-32-months-for-ddos-attacks-in-liberia/30520/). 14.01.2019).***

***

«Активист движения Anonymous Мартин Готтесфельд (Martin Gottesfeld) получил 10 лет тюрьмы за DDoS-атаки на детскую больницу и

некоммерческую организацию в Массачусетсе, США. Подсудимого также обязали компенсировать нанесенный вред в размере $443 тыс.

Организатор кампании хотел добиться справедливости в деле Жюстины Пеллетье (Justina Pelletier), которую в 2013 году разлучили с родителями из-за неверного диагноза…

Готтесфельд …создал ботнет из 40 тыс. роутеров и в апреле 2014 года вывел в оффлайн системы Boston Children's Hospital и WYFSN. Как следует из материалов следствия, атака была такой мощной, что затронула и другие учреждения Лонгвудского медицинского корпуса (Longwood Medical Area).

Инфраструктура WYFSN оказалась парализована на неделю, в результате чего организация понесла убытки в $18 тыс. Ущерб для госпиталя оказался еще тяжелее — его системы восстановили работоспособность только через две недели… Восстановление инфраструктуры потребовало более $300 тыс., еще столько же больница потеряла в виде пожертвований, когда атака обрушила ее краудфандинговый портал.

Правоохранительные органы нашли виновника по видео, которое он загрузил на YouTube…» ***(Egor Nashilov. В США завершился суд над участником группировки Anonymous // Threatpost (https://threatpost.ru/trial-against-member-of-anonymous-group-concluded-in-the-us/30537/). 14.01.2019).***

***

«ИБ-специалист Лукас Стефанко (Lukas Stefanko) обнаружил в Google Play девять фальшивых приложений для дистанционного управления различными устройствами. Все они вместо заявленных функций лишь демонстрировали пользователю рекламу. Вредоносные программы загружены в репозиторий одним и тем же автором и суммарно набрали более 8 млн установок. Получив сообщение исследователя, модераторы сервиса удалили зловреды из хранилища.

…Все фальшивки принадлежат разработчику Tools4TV, а самую популярную из них — Remote control for TV and home electronics со средним рейтингом 3,8 балла — загрузили более 5 млн раз…» ***(Egor Nashilov. IoT-приложения показывали рекламу пользователям Android // Threatpost (https://threatpost.ru/fake-remote-control-apps-for-android-showed-ads/30533/). 14.01.2019).***

***

«Португальская полиция задержала в Венгрии подозреваемого во взломах баз данных европейских футбольных клубов и дальнейшей публикации секретных документов на протяжении последних четырех лет на портале Football Leaks. Полиция не раскрывает его имя, но, по данным СМИ, речь идет о тридцатилетнем португальце Руи Пинто (Rui Pinto).

С 2015 года сайт Football Leaks (действующий по типу WikiLeaks) публиковал конфиденциальные документы, полученные, как утверждалось, от анонимных источников. Ресурс раскрыл подробности о ряде сомнительных футбольных трансферов, суммах отступных футбольных агентов при трансферах,

обнародовал личную переписку футболистов, в том числе Дэвида Бекхэма, названия и счета подставных фирм и много другой секретной информации.

В числе пострадавших фигурируют именитые футбольные клубы «Манчестер Сити», «Пари Сен-Жермен», «Порту», «Бенфика», «Спортинг Лиссабон». Сайт временно прекратил свою деятельность после заявлений нескольких футбольных клубов о вымогательстве со стороны оператора Football Leaks, требовавшего деньги за необнародование определенных материалов, но вскоре возобновил работу.

Некоторые клубы возложили ответственность на FIFA, утверждая, что она является единственной организацией, откуда взлоумышленник мог получить все документы. Однако португальский клуб «Бенфика» заявил, что некоторые из просочившихся документов хранились только во внутренней системе, и попросил португальскую полицию провести расследование.

В настоящее время Руй Пинто ожидает экстрадиции в Португалию, где ему грозит до десяти лет тюрьмы.» ***(В Венгрии задержан предполагаемый оператор Football Leaks // Информационная безопасность (http://www.itsec.ru/news/v-vengrii-zaderzhan-predpolagaemiy-operator-football-leaks). 18.01.2019).***

***

«Комиссия по ценным бумагам и биржам США (SEC) во вторник подала в суд на украинского хакера Александра Еременко, шесть трейдеров из Украины, России и Калифорнии и двух юридических лиц. Она обвиняет их в том, что они незаконно заработали минимум $4,1 млн на фондовом рынке, взломав ее систему раскрытия финансовых результатов компаний.

Кроме того, министерство юстиции США предъявило уголовные обвинения Еременко и другому украинцу Артему Радченко, который ему предположительно помогал.

О взломе своей системы Edgar, куда компании загружают документы с информацией о своих финансовых результатах, SEC сообщила в сентябре 2017 г., хотя хакеры проникли в нее еще в 2016 г…

SEC обнаружила взлом своей системы в октябре 2016 г. и устранила ее уязвимость. Но некоторые сотрудники регулятора, узнав о кибератаке, не сразу догадались, что к этому могут быть причастны недобросовестные трейдеры…» ***(Алексей Невельский. Как украинские хакеры заработали более $4 млн на фондовом рынке США // АО Бизнес Ньюс Медиа (https://www.vedomosti.ru/finance/articles/2019/01/16/791592-ukrainskie-hakeri-4-mln-fondovom). 16.01.2018).***

***

Технічні аспекти кібербезпеки

«…Компания Siemens опубликовала руководство, описывающее рекомендованные настройки безопасности, которые позволят

минимизировать риск для компьютеров на базе Windows, использующихся в промышленных средах.

Документ включает в себя две части – в первой представлены рекомендации по настройке физически изолированных ПК, второй раздел посвящен настройке подключенных к сети компьютеров. С рекомендациями по настройке ПК на базе Windows 7 и Windows 10 можно ознакомиться здесь и здесь…» ***(Опубликованы рекомендации по настройкам безопасности для промышленных ПК // SecurityLab.ru (https://www.securitylab.ru/news/497409.php). 11.01.2019).***

***

«По прогнозам аналитиков компании Gartner, к 2020 году 50% маршрутизаторов заменят решения SD-WAN.

…продукты SD-WAN имеют встроенные межсетевые экраны и другие функции безопасности, что делает их привлекательной целью для киберпреступников. Большинство подобных решений предлагаются как виртуальные средства на базе Linux или облачные сервисы, которые могут скомпрометировать даже скрипт-кидди.

Сложность SDN создает дополнительные риски безопасности, которые ИТ-специалистам нужно принимать во внимание, чтобы не допустить кибератаки…» ***(Эксперт рассказал о рисках сетей SD WAN // SecurityLab.ru (https://www.securitylab.ru/news/497305.php). 04.01.2019).***

***

«…55% всех программ, установленных на ПК на базе Windows, устарело и подвергает пользователей риску из-за неисправленных уязвимостей. К такому выводу пришли специалисты Avast на основании анализа данных, полученных от 163 млн компьютеров, на которых установлены решения компании.

По данным исследователей, на более чем 94% компьютеров установлены устаревшие версии программ Adobe Shockwave, VLC Media Player и Skype. Также были выявлены уязвимые версии Java Runtime Environment (93%), 7-Zip (92%), Foxit Reader (91%), Adobe Air (88%), Irfan View (86%), Mozilla Firefox (85%), с помощью которых злоумышленники могли бы скомпрометировать компьютер, где установлены данные программы.

Устаревшие ПО Microsoft Office являются еще одной категорией приложений, которые подвергают своих пользователей риску, учитывая, что 15% всех установок Office составляет версия Enterprise 2007. Microsoft прекратила поддержку данной версии в 2017 году, то есть для нее уже почти два года не выпускаются обновления и патчи.

Как выявила Avast, Windows 7 установлена на 43%, а Windows 10 – на 40% всех ПК, однако многие владельцы компьютеров до сих пор используют устаревшие версии ОС... Ситуация с Windows 10 немного лучше - только 9% пользователей используют устаревшую версию данной ОС…» ***(Устаревшее ПО подвергает пользователей ПК риску // SecurityLab.ru (https://www.securitylab.ru/news/497559.php). 23.01.2019).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Tesla пообещала подарить электромобиль Model 3 тому, кто сможет найти уязвимости в программном обеспечении машины и взломать его…

Попробовать свои силы во взломе электромобилей Tesla специалисты по кибербезопасности смогут на ежегодном соревновании Pwn2Own в Ванкувере (Канада).

Производитель электромобилей запустил программу вознаграждения клиентов за обнаружение уязвимостей в его программном обеспечении в 2014 г…» ***(Tesla пообещала Model 3 за взлом программного обеспечения электромобиля // АО Бизнес Ньюс Медиа (https://www.vedomosti.ru/technology/news/2019/01/15/791452-tesla). 15.01.2019).***

***

«…В свете недавних хакерских атак сеть отелей Hyatt запустила собственную программу выплаты вознаграждений за найденные уязвимости на платформе HackerOne. Программа является общедоступной и распространяется на основные домены Hyatt (hyatt.com, m.hyatt.com, world.hyatt.com), а также мобильные приложения компании для iOS и Android.

Награда будет выплачиваться за новые методы обнаружения исходных IP-адресов, обхода аутентификации, доступа к внутренним системам, выхода из окружения контейнера, внедрения SQL-кода, подделки межсайтовых запросов, обхода WAF и выявление XSS-уязвимостей…

За обнаружение опасных уязвимостей исследователи могут расчитывать на вознаграждение в размере до $4 тыс., проблемы средней степени опасности принесут им награду в размере $1,2 тыс., а менее серьезные - от $300 до $600.

В 2015 году жертвами кибератак стали 250 гостиниц Hyatt в разных странах, включая США, Великобританию, Китай, Германию, Японию, Италию, Францию, Россию и Канаду. В сеть отелей был внедрен инфостилер, что привело к компрометации финансовых данных клиентов, включая имена держателей платежных карт, номера карт, сроки истечения их действия и внутренние коды верификации. В 2017 году произошла аналогичная утечка данных , затронувшая более 40 отелей Hyatt» ***(Сеть отелей Hyatt наградит исследователей за найденные уязвимости // SecurityLab.ru (https://www.securitylab.ru/news/497407.php). 11.01.2019).***

***

«Trend Micro опубликовала результаты исследования A Security Analysis of Radio Remote Controllers for Industrial Applications (PDF, EN) («Анализ систем дистанционного радиоуправления промышленным оборудованием с точки зрения безопасности»). В нем эксперты компании рассматривают

уязвимости таких систем на примере устройств от семи наиболее популярных производителей, основные типы атак киберпреступников на предприятия с их использованием и ключевые методы предотвращения подобных атак…

Учитывая, что в мире используются миллионы единиц дистанционно управляемого оборудования, которые практически не защищены от воздействия злоумышленников, последние могут перехватывать управление такой техникой на программном уровне, подменять идущие от пульта управления команды, инициировать аварийное отключение и организовывать с помощью этих методов различные типы атак. Среди них следует выделить: саботаж и временную остановку деятельности предприятия, масштабы и ущерб от которой будут сильно отличаться в зависимости от того, насколько важным для отрасли является затронутое предприятие; кражу продукции из портов и автоматизированных логистических центров при помощи подъёмников и другого радиоуправляемого оборудования; вымогательство, при котором злоумышленник целенаправленно вызывает остановку производства либо повреждение ценного оборудования, что приводит к убыткам, а затем требует выкуп в обмен на прекращение атак.

В исследовании рассматриваются основные методы защиты, которые применяются при разработке систем дистанционного радиоуправления наиболее популярными производителями и их слабые места, например, защищённое подключение с использованием общего для передатчика и приёмника кода доступа, а также защита паролем терминала передатчика, разблокировка определённых функций передатчика только при помощи ключ-карты и применение дублирующих систем защиты...

В целом в ходе исследования Trend Micro выяснила, что в промышленности (в отличие от потребительской сферы) практически не развита культура киберзащиты радиоуправляемого оборудования…» ***(Trend Micro: в промышленности мало развита культура киберзащиты радиоуправляемого оборудования // «Компьютерное Обозрение» (https://ko.com.ua/trend_micro_v_promyshlennosti_malo_razvita_kultura_kiberzashhity_radioupravlyaemogo_oborudovaniya_127422). 15.01.2019).***

***

«Почти половина компаний оказалась не в состоянии отследить уязвимости в используемых IoT-устройствах…

Таковы результаты исследования компании Gemalto, охватившего 950 управленцев по всему миру — как производителей, так и корпоративных пользователей IoT-устройств. Эксперты выяснили, что лучше всего к отражению атак на Интернет вещей готовы в Индии и Бразилии. В этих странах в своей безопасности уверены 67% и 65% респондентов. На другой стороне спектра оказались компании из Японии (32%), Франции (36%) и Австралии (37%).

За прошедший год бизнес несколько нарастил инвестиции в защиту IoT…

Многие производители вынуждены выбирать между удобством пользователей и защитой IoT-устройств. Об этом заявили более 30% респондентов…

Респонденты указали, что работа с IoT затрагивает множество критически важных областей, таких как защита персональных данных, распределенное хранение больших объемов информации, надежная аутентификация, интеграция личных устройств сотрудников с корпоративной инфраструктурой. С другой стороны, внедрение средств безопасности не успевает за развитием технологий.

Так, только 59% компаний шифруют все данные Интернета вещей, а 29% вовсе оставляют информацию в открытом виде. Подход Secure By Design, который предполагает проектирование систем безопасности с самого начала работы над продуктом, практикуют менее 60% респондентов. Еще 37% планируют внедрить у себя эту концепцию, а у 5% это не входит в ближайшие задачи.

Такое положение вещей не проходит мимо внимания потребителей. В этой группе 62% ожидают от производителей больших усилий по защите Интернета вещей. Сейчас 54% опасаются за свою приватность при использовании подключенных устройств, 51% чувствуют угрозу взлома, а 50% полагают, что третьи лица могут добраться до их персональных данных.

В нынешних условиях бизнес делает ставку на блокчейн — за прошедший год применение этих технологий для защиты IoT выросло почти вдвое, приблизившись к 20%. Более 90% респондентов сейчас оценивают потенциал этих решений для своих компаний, а 23% уже точно знают, как будут использовать их в обозримом будущем.

И компании, и потребители ожидают, что государственные органы создадут стандарты, на которые можно будет опираться при разработке IoT-систем…» ***(Dmitry Nazarov. Безопасность IoT остается серой зоной для компаний // Threatpost (https://threatpost.ru/iot-security-continues-to-be-problem-for-business/30572/). 16.01.2019).***

***

«Киберпреступники взяли на вооружение уязвимость в PHP-утилите Adminer и крадут учетные данные для доступа к базам данных веб-ресурсов…

Adminer предоставляет графический интерфейс для управления базами MySQL и PostgreSQL, однако при этом может подключаться к внешним хранилищам. Как выяснил ИБ-специалист Виллем де Грут (Willem de Groot), киберпреступники сканируют Интернет в поисках файлов adminer.php, не защищенных паролем, чтобы через них открыть соединение с собственным SQL-сервером. Последний настроен таким образом, чтобы отправлять запрос на скачивание файлов любому хосту, который к нему обращается.

Обработав входящий пакет от Adminer, криминальный сервер может получить через утилиту файлы, содержащие информацию для доступа к целевым базам данных, например local.xml, где хранятся пароли CMS Magento. Обладая этой информацией, киберпреступники способны установить на сайт жертвы скрипт для кражи данных банковских карт или других сведений…

Для предотвращения взлома специалист рекомендует администраторам установить актуальный на данный момент Adminer 4.7.0, установить для SQL-базы дополнительный пароль и ограничить входящие запросы списком разрешенных IP-адресов…»***(Egor Nashilov. Сайты, использующие утилиту Adminer, подвержены***

взлому // Threatpost (https://threatpost.ru/sites-using-adminer-for-their-sql-databases-are-easily-compromised/30646/). 21.01.2019).

***

«Експерт в області кібербезпеки Батист Робер розповів про уразливість в популярній на Android програмі ES File Explorer, яка дозволяє красти будь-які дані користувачів…

Серед іншого варто відзначити, що додаток досить популярний, і його завантажили вже 500 мільйонів разів... Однак, воно здатне допомогти хакерам вкрасти ваші дані без вашого відомства.

…що програма містить відкритий порт, і якщо зловмисник і атакується користувач знаходяться в одній мережі Wi-Fi, то хакер при бажанні може отримати будь-які файли: листування, файли, відео, фото…

Експерт повідомив авторам файлового менеджера про знайдену проломи, однак ті проігнорували його запит. На сьогоднішній день всі користувачі програми в небезпеці…» ***(Популярний Android-додаток відкрив доступ до даних мільйонів користувачів // znaj.ua (https://znaj.ua/techno/204978-populyarniy-android-dodatok-vidkriv-dostup-do-danih-milyoniv-koristuvachiv). 22.01.2019).***

***

«Оставляя любое устройство в сети на долгое время, будьте уверены – рано или поздно вас взломают, пишет TechCrunch. Многие производители используют стандартные пароли, что позволяет хакеру входить в систему как "администратор". Часто нет пароля вообще.

…Почти все, что подключается к Интернету, помечается в Shodan, включая то, что делает устройство и какие интернет-порты открыты. Например, если открыт определенный порт, это может быть веб-камера.

От камер до маршрутизаторов, от больничных КТ-сканеров до детекторов взрывчатых веществ в аэропортах, - вы будете поражены и расстроены тем, что можно увидеть опубликованным в Интернете.

Shodan пугает людей. Это окно в мир абсолютной незащищенности. Это не только открытые устройства, но и базы данных - в них хранится что угодно, от двухфакторных кодов до ваших голосов на выборах…» ***(Ирина Фоменко. Изображения со взломанных компьютеров, которые хакеры выложили в сеть // Internetua (http://internetua.com/izobrajeniya-so-vzlomannyh-kompuaterov-kotorye-hakery-vylojili-v-set). 23.01.2019).***

***

«Исследователь в области информационной безопасности, известный под ником LimitedResults, провел анализ аппаратного и программного обеспечения нескольких популярных умных ламп и выяснил, что все они сохраняют пароли от точек доступа Wi-Fi в незащищенном текстовом виде. Как следствие, при желании злоумышленник может подключиться к выброшенной лампе и с легкостью узнать пароль от Wi-Fi ее бывшего хозяина.

…исследователь проанализировал три лампы популярных производителей: Yeelight (Xiaomi), LIFX и Tuya... Выяснилось, что в двух лампах есть неотключенный интерфейс JTAG, используемый для отладки, а к микроконтроллеру третьей лампы (Tuya) можно подключиться по протоколу UART.

Подключившись к микроконтроллерам, исследователь обнаружил, что они содержат сразу несколько уязвимостей. Во-первых, все лампы хранят данные о точках доступа Wi-Fi (в том числе пароли) в открытом виде... Во-вторых, устройства от некоторых производителей обладают специфичными для них уязвимостями: в частности, лампа Tuya хранит в открытом виде идентификатор DeviceID и локальный приватный ключ, имея которые злоумышленник может удаленно контролировать устройство, а лампа LIFX — корневой сертификат и значение приватного ключа RSA.

Разумеется, изученный LimitedResults сценарий взлома — не самый популярный среди злоумышленников, и его нельзя применить, если лампа находится в недоступном для правонарушителя помещении. В то же время, им можно воспользоваться в случае с выброшенными лампами…» ***(Кирилл Иртлач. Специалист по кибербезопасности: умные лампочки хранят пароль от Wi-Fi в незашифрованном виде // ООО «ХОТЛАЙН» (https://itc.ua/blogs/spetsialist-po-kiberbezopasnosti-umnyie-lampochki-hranyat-parol-ot-wi-fi-v-nezashifrovannom-vide/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+itc-ua+%28ITC.ua%29). 31.01.2019).***

***

«Исследователь кибербезопасности Мелих Севим (Melih Sevim) смог обнаружить баг в iCloud, который позволяет получить доступ к приватным данным других пользователей iPhone.

Как оказалось, Apple привязала номер телефона к платежным ведомостям Apple ID и учетной записи iCloud. Чтобы получить доступ к личным данным постороннего человека, Севим ввел его контактный номер в свой личный аккаунт.

Выдав себя за владельца смартфона, он получил доступ к …приватной информации, включая банковские счета и пароли пользователей хранящиеся в iCloud, можно получить используя случайные личные данные.

Как утверждает Мелих Севим, он сообщил Apple о своей находке в октябре 2018. В Купертино хакеру сообщили, что проблема была решена гораздо ранее его обращения. Однако специалист заметил, что на самом деле уязвимость была доступна ещё в течение некоторого времени…» ***(Александр Лазарчук. Хакер смог получить данные из iCloud по номеру телефона // ООО «ХОТЛАЙН» (https://mobidevices.ru/hacker-was-able-retrieve-data-from-icloud-by-phone-number). 31.01.2019).***

***

«Компания BlackBerry, сменившая производство смартфонов на защиту Интернета вещей, представила набор сервисов для IoT-разработчиков…

Разработки под общим названием BlackBerry Secure предлагают компаниям готовые решения для безопасности, сгруппированные в три пакета, каждый из которых отвечает за собственный набор задач:

EnablementFeature Pack защищает пользователей от компрометации IoT-устройств. Производители могут вшить в код своих продуктов защищенный идентификационный ключ (Secure Identity Service Key), который сохраняется на серверах BlackBerry. Система проверяет его достоверность при каждом включении устройства и периодически в процессе работы. При несовпадении данных аппарат блокируется.

FoundationsFeature Pack предлагает средства для создания, использования и хранения ключей шифрования, которые могут применяться в программных операциях. Функции этого пакета также позволяют отслеживать состояние IoT-устройств, причем эта информация будет доступна самим пользователям и сторонним приложениям из списка доверенных.

SecureEnterprise Feature Pack предназначен производителям IoT-компонентов, которые используются в закрытых инфраструктурах, например в промышленности. С его помощью администраторы могут контролировать данные, доступные через служебный интерфейс устройства и по стандартным протоколам вроде Bluetooth, настраивать политики безопасности в соответствии с отраслевыми и государственными стандартами…» ***(Egor Nashilov. BlackBerry представила разработки для Интернета вещей // Threatpost (https://threatpost.ru/blackberry-wants-to-make-iot-secure-with-its-feature-packs/30402/). 08.01.2019).***

***

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

Автоматика / Automatics - 2018. XXV Міжнародна конференція з автоматичного управління : матеріали конф., 18-19 верес. 2018 р., Львів, Україна. - Львів : Вид-во Львів. політехніки, 2018. - 204 с.

Зі змісту:

- Булижко А. С. Аналіз динаміки охоплення кіберпростору.

Шифр зберігання НБУВ: СО36113.

***

Актуальні питання техногенної та цивільної безпеки України. І Всеукраїнська наукова конференція, 21-22 вересня 2018 року : матеріали конф.- Миколаїв : Торубара В. В., 2018. - 206 с.

Зі змісту:

- Король В.К., Савіна О.Ю. Вплив хакерства на безпеку життєдіяльності людства.

Шифр зберігання НБУВ: ВС64620.

***

Баранов О. А. Інтернет речей: теоретико-методологічні основи правового регулювання / О. А. Баранов. - Київ, 2018. - Т. 1 : Сфери застосування, ризики і бар'єри, проблеми правового регулювання. - 342 с.

На чисельних прикладах з'ясовано унікальну роль Інтернету речей в розвитку соціуму. Обгрунтовано та запропоновано визначення терміну «Інтернет речей». У якості типових прикладів наведено методологічні підходи щодо аналізу, з'ясуванню та формулюванню правових проблем, пов'язаних із розвитком інформаційної інтраструктури Інтернету речей, застосуванням штучного інтелекту та роботів автономних автомобілів, кораблів і дронів, з використанням розумних контрактів, особливостями захисту персональних даних, авторського права та права інтелектуальної власності, із забезпеченням кібербезпеки тощо.

Шифр зберігання НБУВ: В357410/1.

***

Грані права: XXI століття : матеріали Всеукр. наук.-практ. конф., 19 трав. 2018 р. - Одеса, 2018. - Т. 2. - 561 с.

Зі змісту:

- Овчар А. С. Кіберзлочинність: кримінологічна сутність та детермінація;
- Приходько Ю. Е., Асатрян К. С. Кіберзлочинність як один із найбільш прогресивних видів сучасної злочинності;
- Шрамко М. О., Феденко Є. М. До питання профілактики розвитку кіберзлочинності в Україні;
- Шишацька Ю. О. Виявлення доказів кіберзлочину у кримінальному провадженні;
- Максимчук Ю. В. Особливості розслідування кіберзлочинів та протидії їх вчинення.

Шифр зберігання НБУВ: В357399/2.

***

Дудикевич В.Б. Квінтесенція нормаційної безпеки кіберфізичної системи / В.Б. Дудикевич, Г.В. Микитин, А.І. Ребець // Вісник Національного університету «Львівська політехніка». Інформаційні системи та мережі. - 2018. - № 887. - С. 58-68.

Подано квінтесенцію нормаційної безпеки (ІБ) кіберфізичних систем (КФС), яка розгорнута на рівні парадигми та концепції побудови багаторівневої

комплексної системи безпеки (КСБ) КФС і універсальної платформи КСБ у просторі «загрози – профілі – інструментарій».

Шифр зберігання НБУВ: Ж29409.

***

Ефективна система кримінальної юстиції як фактор сталого розвитку економіки : матеріали III панел. дискусії Другого Харків. міжнар. юрид. форуму, м. Харків, 27 верес. 2018 р. - Харків : Право, 2018. - 159 с.

Зі змісту:

- Воронов І. Забезпечення кібербезпеки в умовах європейської інтеграції.

Шифр зберігання НБУВ: ВА826786.

***

Криміналістика та судова експертологія: наука, навчання, практика. 14 Міжнародний Конгрес, 13-15 вересня, Одеса, Україна, 2018 = Criminalistics and forensic expertology: science, studies, practice. 14 internationl congress, 13-15 September, Odessa, 2018 = Kriminalistika ir teismo ekspertologija: mokslas, studijos, praktika. 14 tarptautinis kongresas, 13-15 rugséjis, Odesa, 2018. – Одеса, 2018. - Т. 2. - 542 с.

Зі змісту:

- Самойленко О., Паляничко Д., Баланюк О., Ващенко І. Інформаційні сліди в контексті механізму вчинання злочинів із використанням обстановки кіберпростору.

Шифр зберігання НБУВ: В357388/2.

***

Кожедуб Ю. Реалізація процесного підходу до керування ризиками інформаційної безпеки в документах NIST / Ю. Кожедуб // Information Technology and Security. - 2017. - Vol. 5, № 2. - С. 76-89.

Досліджено методологічні основи діяльності Національного інституту стандартів і технологій Сполучених Штатів Америки (National Institute of Standards and Technology, NIST). Зосереджено увагу на процесному підході до створення рекомендацій, настанов, керівних вказівок, рамкових документів. Проаналізовано методичні документи щодо інформаційної безпеки, кібербезпеки та комп'ютерної безпеки, що дозволяють допомогти вибрати набір заходів контролю безпеки

Шифр зберігання НБУВ: Ж74190.

***

Кучернюк П. В. Методи і технології захисту комп'ютерних мереж (мережний, транспортний та прикладний рівні) / Кучернюк П. В. // Мікросистеми, Електроніка та Акустика : науч.-техн. журн.- 2018.- Т. 23.- № 1 (102).- С. 52-58.

Розглянуто найбільш поширені рішення, які підтримуються виробниками обладнання для комп'ютерних мереж (комутатори 2-го та 3-го рівнів, маршрутизатори), реалізовані у операційних системах та протоколах. Наведено типові загрози комп'ютерним мережам мережевого, транспортного і прикладного рівнів моделі OSI. Проведено аналіз особливостей методів і технологій захисту.

Шифр зберігання НБУВ: Ж69367.

***

Матеріали III Міжнародної науково-практичної конференції «Інноваційний розвиток наукинового тисячоліття» (25-26 травня 2018 року). - Чернівці, 2018. - 199 с.

Зі змісту:

- Круць В. В. Інформаційна безпека комп'ютерних систем.

Шифр зберігання НБУВ: ВА827341.

***

Матеріали міжнародної науково-практичної конференції «Соціальні комунікації: теорія і практика сучасної науки», 4-5 травня 2018 р. - Київ, 2018. - 95 с.

Зі змісту:

- Одаренко О.В. Варіативність мережевої ідентичності в умовах сучасних кіберконфліктів.

Шифр зберігання НБУВ: ВА827004

***

Молодь: освіта, наука, духовність. XV Всеукраїнська наукова конференція студентів і молодих вчених (м. Київ, 17-19 квітня 2018 р.) = Youth: education, science, spirituality. XV National scientific conference of students and young scientists (Kyiv, April 17-19, 2018) : тези доп. - Ч. 1. - Київ, 2018. - 412 с.

Зі змісту:

- Кукарін М.В. Аналіз загроз та методи захисту комп'ютерних мереж.

Шифр зберігання НБУВ: В357392/1.

***

Субач І. Модель виявлення кібернетичних атак на інформаційно-телекомунікаційні системи на основі описання аномалій їх роботи зваженими нечіткими правилами / І. Субач, В. Фесьоха // Information Technology and Security. - 2017. - Vol. 5, № 2. - С. 145-152.

Розглянуто захист інформаційно-телекомунікаційних систем та мереж від кібернетичних атак в умовах їхнього постійного розвитку та поліморфізму шкідливого програмного забезпечення. Проведено аналіз та зроблено висновок про доцільність застосування моделей ідентифікації аномалій, що одночасно оперують якісними і кількісними даними та ґрунтуються на математичному апараті теорії

нечітких множин та нечіткого логічного виводу. Представлено удосконалену модель виявлення аномалій в роботі інформаційно-телекомунікаційних систем та мереж, яка є подальшим розвитком запропонованої раніше моделі виявлення аномалій на основі нечітких множин та нечіткого логічного виводу.

Шифр зберігання НБУВ: Ж74190.

***

Ткачук Т. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : монографія / Тарас Ткачук. - Київ : АртЕк, 2018. - 421 с.

Здійснено порівняльний аналіз правових норм щодо забезпечення інформаційної безпеки держави. Розроблено концептуальні правові засади забезпечення інформаційної безпеки держави та практичні рекомендації щодо вдосконалення відповідних механізмів в Україні.

Шифр зберігання НБУВ: ВА826776.

***

Яковів І. Інформаційно-телекомунікаційна система, концептуальна модель кіберпростору і кібербезпека / І. Яковів // Information Technology and Security. - 2017. - Vol. 5, № 2. - С. 134-144.

Аналіз інформаційних процесів інформаційно-телекомунікаційні системи (ІТС) систем було проведено на основі застосування атрибутивно-трансферного підходу до сутності інформації. За результатами аналізу розроблено концептуальну модель кіберпростору і кібербезпеки. Завдяки моделі кіберпростору було розроблено математічні критерії кібербезпеки для сегменту кіберпостору.

Шифр зберігання НБУВ: Ж74190.

***

Виготовлено в друкарні
ТОВ «Видавничий дім «АртЕк»
04050, м. Київ, вул. Мельникова, буд. 63
Тел.. 067 440 11 37
artek.press@ukr.net
www.artek.press

Свідоцтво про внесення суб'єкта видавничої справи
до державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції –
серія № ДК №4779 від 15.10.14р.