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

№ 3 (березень)

Київ – 2019

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І.Вернадського. – К., 2019. – №3 (березень) . – 80 с.

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

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

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

ЗМІСТ

Стан кібербезпеки в Україні 4
Кібервійна проти України 8
Боротьба з кіберзлочинністю в Україні 12
Міжнародне співробітництво у галузі кібербезпеки 18
Світові тенденції в галузі кібербезпеки 19
Сполучені Штати Америки 33
Країни ЄС 37
Китай 39
Інші країни 40
Протидія зовнішній кібернетичній агресії 43
Захист персональних даних 46
Кіберзлочинність та кібертероризм 52
Діяльність хакерів та хакерські угруповування 57
Вірусне та інше шкідливе програмне забезпечення 62
Операції правоохоронних органів та судові справи проти кіберзлочинців 67
Технічні аспекти кібербезпеки 68
Виявлені вразливості технічних засобів та програмного забезпечення 68
Технічні та програмні рішення для протидії кібернетичним загрозам 72
Нові надходження до Національної бібліотеки України імені В.І. Вернадського 77

«Начальник Департамента киберполиции Национальной полиции Украины Сергей Демедюк предложил изучать в школах основы кибербгигиены, что должно повысить безопасность граждан в интернете…

Пока готовы два видеоролика о правилах защиты информации от взлома и безопасного шопинга в интернете, передает Интерфакс-Украина. По словам начальника Департамента киберполиции, они будут демонстрироваться по телевиденью и продвигаться в соцсетях, а буклеты «5 правил защиты информации от взлома в Интернете» и «5 правил безопасного шопинга в Интернете» — бесплатно распространяться в школах.» ***(В Украине предложили преподавать в школе кибергигиену // hpib.life (http://hpib.life/v-ukraine-predlozhili-prepodavat-v-shkole-kibergigienu/). 07.03.2019).***

***

«Ряд проблем с кибербезопасностью информационных ресурсов Вооруженных сил Украины, среди которых – проблемы с Аккредитованным центром сертификации ключей Вооруженных сил и почтовым сервером ВСУ, обнаружил эксперт по информационной безопасности Андрей Перевезий. Эксперт отмечает: вопросы далеко не критические, но Минобороны стоит уделять больше внимания кибербезопасности…

Андрей Перевезий обнаружил на сайте Аккредитованного центра сертификации ключей Вооруженных сил Украины инсталляционные файлы электронных ключей, используемых Минобороны. Кроме этого, в Минобороны на данном сайте используют незащищенный протокол передачи данных (что повышает риск перехвата информации). Также в МОУ никак не ограничивают доступ посторонних к административной панели почтового сервера…

Андрей Перевезий объясняет: для специалистов по информационной безопасности обнаруженное – это абсурдные, детские проблемы, которые специалисты Минобороны страны должны оперативно устранять…

Проблемой называет эксперт и тот факт, что почтовый сервер Министерства обороны mil.gov.ua имеет удаленную систему входа.

– Данный почтовый сервер, mil.gov.ua, имеет удаленную систему входа. По тому же принципу, как вы заходите на почту от Google. Только Google при этом более защищен, и есть вероятность подбора злоумышленником пароля, зная, например, почтовый ящик пользователя, – объясняет Андрей Перевезий.

Эксперт подчеркивает: обнаруженные бреши не критичны и легко исправляются, но само их наличие может повлечь репутационные риски…» ***(Владимир Кондрашов. Эксперт: Минобороны хорошо бы уделить внимание вопросу кибербезопасности // Internetua (http://internetua.com/ekspert-minoborony-horosho-by-udelit-vnimanie-voprosu-kiberbezopasnosti-1). 22.03.2019).***

***

«Эксперт по кибербезопасности Александр Галущенко обнаружил в свободном доступе в сети несколько терабайт данных «Укрпочты», среди

которых – списки клиентов и почтовых отправлений, финансовая информация компании и другие конфиденциальные данные. По подсчетам эксперта, «дыра» в безопасности, в случае её использования злоумышленниками, могла стоить национальному почтовому оператору полмиллиарда гривен…

Информацию об уязвимости эксперт подкрепил скриншотами с обнаруженного в сети диска с данными Укрпочты…

Александр Галущенко уточнил, что обнаружил информацию на устройстве в одной из областей Украины, где были доступы к системе перевода денег, данным по пенсиям, доступ к бухгалтерии и другим критически важным ресурсам.

Укрпочта довольно оперативно отреагировала на инцидент…» ***(Владимир Кондрашов. Укрпочта засветила в сети конфиденциальные данные // Internetua (http://internetua.com/ukrpocsta-zasvetila-v-seti-konfidencialnye-dannye-na-polmilliarda-griven). 18.03.2019).***

***

«В "Укренерго" розробили Концепцію розвитку кібербезпеки компанії на найближчі 4 роки. Про це повідомляється на сайті НЕК "Укренерго…

«...В її основі – аналіз поточного стану інформаційної безпеки в "Укренерго", власний досвід та досвід світових лідерів у галузі кіберзахисту й інформаційних технологій, перш за все Ізраїлю», - йдеться у повідомленні.

Повідомляється, що у складі концепції загалом 30 проектів. Серед них: створення захищеної транспортної мережі підприємства для безпечної взаємодії з зовнішнім світом, організація захищеної базової інфраструктури та центрів обробки даних, а також створення Операційного центру безпеки та професійного навчання персоналу. Реалізація найвагоміших з них запланована вже у 2019-2020 рр.

В "Укренерго" зазначили, що реалізацію проекту вже розпочато. Зокрема, створюється Операційний центр безпеки (SOC) з власним інструментарієм та системою збору та аналізу інцидентів інформбезпеки. Також розпочато процес фізичного розділення мереж на корпоративну та технологічну…» ***(Ангеліна Літінська. В "Укренерго" розробили систему кіберзахисту // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1786019-v-ukrenergo-rozrobili-sistemu-kiberzakhistu). 13.03.2019).***

***

«ДП «Украинская сеть обмена трафиком UA-IX» в партнерстве с ООО «Хайлоад Системс» запускает услугу противодействия DDoS-атакам…

Как стало известно, услуга будет предоставляться ООО «Хайлоад Системс» Участникам UA-IX с использованием внедренной в декабре 2018 автоматизированной системы управления VLAN…

Для участников UA-IX операторов/провайдеров предусмотрено несколько уровней услуги…» ***(Владимир Кондрашов. ИнАУ: в UA-IX запускается услуга противодействия DDoS-атакам // Internetua (http://internetua.com/inau-v-ua-ix-zapuskaetsya-usluga-protivodeistviya-ddos-atakam). 14.03.2019).***

***

«…Киевский IT-предприниматель Алекс Рябцев, который давно занимается веб-разработкой и поддержкой сайтов, решил просканировать украинские IP-адреса на предмет кибербезопасности…

Издание AIN.UA пообщалось с энтузиастом об этом эксперименте. Мы делаем резюме этого общения:

1. IP-адреса выдаются на каждую страну и их списки публикуются. Можно скачать такой список и отфильтровать. Для работы с IP-адресами можно использовать сервис Shodan.io.

2. Украине принадлежит почти столько же IPv4 адресов, как и Австрии: 11640409. Для сравнения в Австрии — 11170487.

3. С украинскими IP-адресами можно найти 5669 машин под Windows с прямым доступом к сети (что очевидно опасно). Среди них есть и те, которые уязвимы к атаке эксплойта ETHERNALBLUE, известного еще с 2017 года. В Австрии не было ни одной такой машины.

4. В Украине есть DNS-серверы, которые могут быть использованы для DDoS-атаки. Алекс сначала нашел серверы, имеющие открытый 53 порт, и получил список из 58 730 IP-адресов. Это еще не значит, что их все можно использовать для DDoS-атаки, эти серверы также должны быть open-resolver (то есть, DNS, позволяет любому клиенту себя использовать). Если сервер отвечал open-resolver-detected, то можно считать его потенциальным объектом атаки. Такие серверы в украинском интернете составляют 25% от всех (примерно так же, как и в Австрии). Среди всех украинских IP — это 0,02%.

5. Веб-серверы. 260 849 украинских IP отвечают на 80 порте (http). 125444 адреса ответили положительно (200 статус) на простенький GET-запрос, который может направить браузер. Остальные выдали те или иные ошибки. Интересно, что 853 серверы выдали 500 статус, а редчайшими статусами стали 407 (запрос на прокси авторизацию) и абсолютно нестандартный 602 (IP не в "белом списке") по одному ответу.

6. На веб-серверах Украины, по его наблюдениям, доминирует Apache, его используют 114544 серверы. Самая старая из найденных версий: 1.3.29, вышедшей 29 октября 2003. На втором месте — nginx (61659 серверов). 11 серверов используют WinCE, которая вышла в 1996 году, а закончили патчить ее в 2013 году.

7. Принтеры. Автору исследования удалось найти два принтера HP, пять Epson и четыре Canon, доступных из сети, а некоторые из них даже не требовали авторизации.

8. Веб-камеры. 75 камер транслируют себя в интернет без защиты. Посмотреть на них можно здесь.

Итоги:

«Могу сказать, что проблемы существуют довольно серьезные, но Украина — не уникальна в этом. У нас ситуация точно хуже, чем в Австрии, хотя по количеству IP мы почти одинаковы. И самое главное, что об информационной безопасности надо думать постоянно, как о гигиене. Совет прост: вкладывать

деньги в ИТ не раз в 5-10 лет, когда надо поменять компьютер или сделать новый сайт, а постоянно, потому что это такая же инфраструктура, как авто или офис », — отметил автор исследования.» ***(Киевлянин просканировал все IP-адреса в Украине. Угроза есть // Goodnews.ua (http://goodnews.ua/technologies/kievlyanin-proskaniroval-vse-ip-adresa-v-ukraine-ugroza-est/). 21.03.2019).***

***

«Вихідні коди усіх програмних продуктів, які використовує державний сектор, повинні бути відкритими для їх аналізу. Про це напередодні, 27 березня, повідомив керівник Департаменту кіберполіції Національної поліції України Сергій Демедюк під час всеукраїнської науково-практичної конференції з кібербезпеки…

За його словами, цифровий світ сьогодні є досить небезпечним і для того, щоб змінити цю ситуацію у цифровому світі, його потрібно вивчати глибше…» ***(Юля Ковтун. Вихідні коди програмного забезпечення держсектору мають бути відкритими для аналізу – кіберполіція // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1789354-vikhidni-kodi-programnogo-zabezpechennya-derzhsektoru-mayut-buti-vidkritimi-dlya-analizu-kiberpolitsiya).28.03.2019).***

***

«Украинский противофейковый сервис FakesRadar получил инвестиции от европейского акселератора StartupWiseGuys, который совместно с министерством обороны Эстонии воплощает программу кибербезопасности CyberNorth…

“FakesRadar только что успешно прошел тщательный независимый аудит безопасности и теперь рад объединить усилия с мощной командой CyberNorth. StartupWiseGuys оценил FakesRadar в 990 тыс. евро, и мы уверены, что это отличное начало”, – заявил технический директор FakesRadar Александр Павленко.

В компании рассказали, что благодаря расширению FakesRadar в Google Chrome возможно мониторить правдивость сообщений. Для этого используются базы данных международной сети признанных организаций, среди которых такие авторитетные фактчекинговые проекты, как EUvsDisinfo.eu, StopFake.org, VoxCheck и десятки других.

Компания добавила, что Chrome-плагин FakesRadar распознает фейки и сообщения от сомнительных источников в Facebook и Twitter. Плагин маркирует обнаруженные в френд-ленте фейки красной рамкой, а сообщения от источников, которые ранее распространили дезинформацию, – желтой. Это обеспечило пользователей самых популярных социальных сетей инструментом противодействия дезинформации.» ***(Украинский противофейковый сервис получит почти 1 млн евро от европейского акселератора // Finance.ua (https://news.finance.ua/ru/news/-/446464/ukrainskij-protivofejkovyj-servis-poluchit-pochti-1-mln-evro-ot-evropejskogo-akseleratora). 28.03.2019).***

***

«У Києві на кількох локаціях, що розташовані на базі різних суб'єктів кібербезпеки, відбулися міжнародні кібернавчання, організовані для отримання новітнього європейського досвіду безпеки виборчих процесів в інформаційному та кібернетичному просторі. Навчання на технічному рівні відбуваються в межах проекту ЄС «Посилення кібербезпеки в Україні перед виборами» за підтримки Естонського центру Східного партнерства та компанії CybExer Technologies, яка має великий досвід проведення таких навчань.

У кібернавчаннях окрім європейських фахівців брали участь найкращі спеціалісти СБ України, Державної служби спеціального зв'язку та захисту інформації, ЦВК, які вперше отримають унікальний досвід протидії хакерам в умовах максимально наближених до реальних за рахунок повністю віртуалізованої інфраструктури. – See more at.

В ході заходу з ґрунтовною доповіддю виступив начальник ДКІБ СБ України генерал-майор Олександр Климчук, інформує прес-служба СБУ…». ***(У СБУ розповіли про основні загрози та запобіжні заходи в ході виборчого процесу в Україні // Західна інформаційна корпорація (https://zik.ua/news/2019/03/19/u_sbu_rozpovily_pro_osnovni_zagrozy_ta_zapobizhni_zahody_v_hodi_vyborchogo_1532559). 19.03.2019).***

***

«За підтримки Європейської комісії на базі ситуаційного центру забезпечення кібербезпеки Службою безпеки України було проведено кібернавчання, спрямовані на підготовку фахівців з СБУ, ЦВК та Держспецзв'язку щодо виявлення та локалізації загроз безпечного функціонування інформаційної інфраструктури ЦВК. Про це сьогодні на брифінгу у Києві повідомив заступник голови СБУ Олег Фролов…

Заступник голови СБУ зазначив, що підтвердженням протиправних намірів можна вважати проведення саме в цей період реальних кібератак з боку Російської Федерації, спрямованих на інфраструктуру та сайт Центральної виборчої комісії.

"Тому СБУ з великою зацікавленістю сприйняло пропозицію представництва Єврокомісії щодо організації кібернавчань у новому для України форматі. Запропонований сценарій навчань дійсно дозволить нашим командам отримати нові знання, та, найголовніше, згуртувати колективи СБУ, Держспецзв'язку та ЦВК, які під час проведення виборів будуть працювати разом", - сказав він…» ***(Саша Картер. Єврокомісія організувала для СБУ кібернавчання для захисту ЦВК // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1784902-yevrokomisiya-organizuvala-dlya-sbu-kibernavchannya-dlya-zakhistu-tsvk). 07.03.2019).***

***

«СБУ попередили спроби спецслужб РФ організувати хакерські атаки на державні установи, які задіяні в підготовці до виборчого процесу та його проведенні...

“Співробітники Служби безпеки України у межах виконання завдань із контррозвідувального забезпечення інтересів держави у сфері інформаційної безпеки Оперативники спецслужби встановили, що куратори з Росії найняли хакера із Запоріжжя для розповсюдження шкідливого програмного забезпечення, призначеного для несанкціонованого втручання в роботу державних інформаційних ресурсів України”, — йдеться у повідомленні.

За даними СБУ, зловмисник був адміністратором закритого хакерського Інтернет форуму російського походження. Він залучав, за грошове винагородження, учасників форуму до розповсюдження вірусу, яке блокувало діяльність інформаційних ресурсів через підключення до держреєстрів України…» ***(Крістіна Попова. РФ організовувала хакерські атаки на держустанови задіяні у виборчому процесі // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1784551-rf-organizovuvala-khakerski-ataki-na-derzhustanovi-zadiyani-u-viborchomu-protsesi).06.03.2019).***

***

«…Міністр закордонних справ України Павло Клімкін заявив, що абсолютно безпрецедентне втручання РФ відбувається повсюди, особливо в сфері кібербезпеки…

Клімкін сказав, що кожні 40 секунд Росія здійснює кібератаку, зокрема, є втручання, яке стосується критичної інфраструктури. Він додав, що блекаут протягом 5-7 днів перед виборами може повністю змінити результати голосування…» ***(Росія кожні 40 секунд здійснює кібератаку на Україну, – Клімкін // Телеканал новин «24» (https://24tv.ua/rosiya_kozhni_40_sekund_zdiysnyuye_kiberataku_na_ukrayinu__klimkin_n1122155?utm_source=rss). 05.03.2019).***

***

«Россия збільшила свої зусилля в Україні з наближенням президентських виборів в Україні. Відповідні висновки зробили розвідувальні служби США в недавньому звіті.

Наголошується, що на даний момент Кремль прагне застосувати всі інструменти, щоб скористатися хитким станом економіки Києва, широкої корупцією, кібер-вразливістю і громадським невдоволенням"…

Кремль має намір загострити політичну атмосферу, крім того, Росія активізувала кібератаки проти українських чиновників і Центрального виборчого ради України…» ***(Путін готується до виборів в Україні: кібератаки, залякування кандидатів та сотні мільйонів доларів // znaj.ua (https://znaj.ua/society/217676-putin-gotuyetsya-do-viboriv-v-ukrajini-kiberataki-zalyakuvannya-kandidativ-ta-sotni-milyoniv-dolariv). 09.03.2019).***

***

«Служба безпеки України разом із відповідними службами докладуть зусиль для забезпечення стійкості єдиної інформаційно-аналітичної системи «Вибори».

Інформаційна система Центрвиборчкому захищена від хакерських атак напередодні виборів. Про це в ефірі телеканалу «Україна» заявив голова Служби безпеки України Василь Грицак…

За словами керівника спецслужби, українські силовики готові спільно протидіяти можливим кібератакам на сервер ЦВК, реєстр виборців та інші бази даних на виборах президента України. Служба безпеки посилила контррозвідувальний режим на всій території України, щоб на ранній стадії виявляти ознаки підготовки до вчинення злочину…» ***(Глава СБУ запевнив у захищеності системи «Вибори» від кібератак // Racurs.ua® (https://racurs.ua/ua/n118845-glava-sbu-zapevnyv-u-zahyschenosti-systemy-vybory-vid-kiberatak.html). 02.03.2019).***

***

«У Держспецзв'язку зафіксували спроби проведення кібератак на сайт Центральної виборчої комісії. Про це повідомила прес-служба Державної служби спеціального зв'язку та захисту інформації України…

При цьому в Держспецзв'язку додали, що Єдина інформаційно-аналітична система "Вибори" для проведення чергових виборів президента України на цей час ще не розгорнута, тож кібератак на неї наразі не фіксували.

Детальну інформацію щодо кібератак на сайт ЦВК у Держспецзв'язку надати не змогли, оскільки доступ до неї обмежений…» ***(Марія Мамаєва. У Держспецзв'язку повідомили про спроби кібератак на сайт ЦВК // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/exclusive/1788179-u-derzhspetszvyazku-povidomili-pro-sprobi-kiberatak-na-sayt-tsvk). 22.03.2019).***

***

«На Чернігівщині служба безпеки України викрила групу хакерів, які готували кібератаки на комп'ютерні системи органів влади під час виборів Президента. Про це повідомляє прес-служба СБУ…

"Місцевий житель разом із спільниками з РФ здійснювали ураження автоматизованих систем органів державної влади для їх компрометації під час підготовки та проведення виборів Президента України. Зловмисники використовували вірусні програми, що дозволяють дистанційно отримувати контроль над комп'ютерами держустанов", - повідомили у прес-центрі.

Зазначається, що хакер отримував гроші через платіжні системи країни-агресора…

У межах кримінального провадження, відкритого за ч. 2 ст. 361 (Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж) Кримінального кодексу України, тривають слідчі дії для притягнення до відповідальності інших осіб, причетних до організації хакерських атак…» ***(Ангеліна Літінська. Хакери України і РФ готували кібератаки напередодні виборів // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1786406-khakeri-gotuvali-kiberataki-naperedodni-viboriv). 14.03.2019).***

***

«…Палата представителей Конгресса США рассмотрит проект резолюции, которая осуждает попытки страны-оккупанта России вмешаться в украинские выборы - как президента, так и парламентские…

Документ внесла двухпартийная группа конгрессменов, членов украинского кокуса во главе с законодателем-демократом от штата Пенсильвания Бренданом Бойлом.

В тексте выражается "твердая поддержка права украинского народа свободно выбирать свое руководство и определять собственное будущее".

Также конгрессмены говорят о поддержке суверенитета и территориальной целостности Украины, "решительно" осуждая попытки Кремля и его агентов вмешиваться в выборы, в частности, путем кибератак и пытыток повлиять на общественное мнение через подконтрольные Москве СМИ и соцсети.» ***(В Конгрессе США готовят резолюцию об атаках РФ на выборы Украины // Информационное агентство ЛІГАБізнесІнформ (https://news.liga.net/politics/news/v-kongresse-ssha-gotovyat-rezolyutsiyu-ob-atakah-rf-na-vybory-ukrainy). 22.03.2019).***

***

«Накануне президентских выборов в Украине активизировались фишинговые атаки хакеров на государственные интернет ресурсы.

Под ударом могут оказаться сайты Центральной избирательной комиссии, Администрации президента, Кабмина, инфраструктурных ведомств…

"Интенсивность кибератак нарастает с каждым годом. Это процесс перманентный и не обязательно связан с выборами. В основном сейчас угрозы является со стороны фишинга, когда хакеры проникают внутрь сети, собирают данные, могут разместить какую-то ложную информацию, "свалить" какой-то сайт в день выборов и т.д. ", - рассказал руководитель Лаборатории компьютерной криминалистики Cyberlab Сергей Прокопенко.

За счет европейской финансовой помощи Украинской кибербезопасности удалось улучшить. На сегодня блокируют те угрозы, которые раньше даже и не замечали…

В зоне риска хакерских атак попадают и кандидаты в президенты. Считают, что ради пиара политики и сами могут инициировать так называемые "атаки на себя". Все эти действия будут для того, чтобы показать свою значимость.

Хакеры слили в сеть гигантскую базу данных, содержащую 2200000000 уникальных имен пользователей и паролей. Эта база втрое больше, чем предыдущая, которую выложили в открытый доступ в середине января - она насчитывала 773 млн паролей и логинов, весила 87 Гб.» ***(Хакеры начали атаковать государственные сайты // Gazeta.ua (https://gazeta.ua/ru/articles/science/_hakery-nachali-atakovat-gosudarstvennye-sajty/894189). 30.03.2019).***

***

«Служба безопасности Украины предотвратила хакерскую атаку на украинские СМИ и телекоммуникационные объекты со стороны российских спецслужб.

Об этом сообщает пресс-служба СБУ.

Исполнители на протяжении нескольких месяцев создавали несколько десятков доменов, которые по своему названию совпадают или походят на официальные домены популярных украинских электронных средств массовой информации, операторов связи и крупных телекоммуникационных компаний. Эти адреса были созданы на мощностях российских интернет-провайдеров. А учетные записи, используемые для их регистрации, ранее применялись для кибератак на украинские государственные компании.

"Замысел кибератаки вполне вероятно заключался в создании максимального общественного резонанса и негативного информационного воздействия накануне проведения выборов президента Украины", - отметили в СБУ.

Накануне президентских выборов в Украине активизировались фишинговые атаки хакеров на государственные интернет-ресурсы. Под ударом могут оказаться сайты Центральной избирательной комиссии, Администрации президента, Кабмина, инфраструктурных ведомств». ***(Спецслужбы РФ готовили предвыборные кибератаки на украинские СМИ // Gazeta.ua (https://gazeta.ua/ru/articles/life/_specsluzhby-rf-gotovili-predvybornye-kiberataki-na-ukrainskie-smi/894216). 30.03.2019).***

***

Боротьба з кіберзлочинністю в Україні

«Зменшення кількості вчинених кібершахрайств під час купівлі-продажу в інтернеті та захист персональних даних у мережі – це основна мета проекту. Презентація проекту відбулася 6 березня за участі керівника української кіберполіції Сергія Демедюка, керівника програми від Координатора проектів ОБСЄ в Україні Лілії Грудко та представників найбільших інтернет-торгових майданчиків України. Про це йдеться у повідомленні на сайті Департаменті Кіберполіції.

За словами начальника Департаменту кіберполіції Сергія Демедюка, з кожним роком жертв від протиправних дій кіберзлочинців стає все більше і ця тенденція не обмежується кордонами якоїсь однієї країни. Тільки в минулому році по всьому світу мільйони осіб постраждали внаслідок нехтування елементарними заходами безпеки в мережі, починаючи від слабкого паролю, закінчуючи використанням не ліцензійного програмного забезпечення.

«Цей проект є для нас дуже важливим, так як ми поширюємо інформацію щодо основних понять, які повинен знати кожен користувач аби не стати жертвою кіберзлочинів. Крім того, в рамках проекту ми закликаємо громадян повідомляти правоохоронні органи про виявлені кіберзлочини, навіть якщо сума збитків не є значною», - зазначив очільник української кіберполіції…

«В рамках сьогоднішньої акції ми хотіли б вкотре звернути увагу на основні правила захисту та безпеки в інтернеті, які в подальшому завадять злодіям отримати доступ до корпоративної інформації або ж не дадуть їм жодного шансу заволодіти коштами наших громадян», - наголосила керівник програми від Координатора проектів ОБСЄ в Україні.

За словами представників приватного сектору, сьогодні від кіберзлочинів страждають не тільки клієнти, а й самі інтернет-ресурси. Так, потрапляючи на фішинговий сайт (який виглядає цілком легітимно) користувач втрачає свої заощадження і в такому випадку довіра до оригінальних ресурсів може знижуватися. Тож приватні структури зі свого боку вживають додаткових заходів безпеки та активно співпрацюють з кіберполіцією у цьому напрямку.

«Ми підтримаємо цю ініціативу. Ми будемо інформувати та поширювати своїми каналами матеріали цієї кампанії і сподіваюся досягнення позитивного результату», - зазначив один із керівників приватної компанії Олексій Король.

Зокрема, у рамках проекту, кіберполіція ініціює поширення соціальної реклами націленої на підвищення рівня обізнаності громадян з кібербезпеки та створення окремого ресурсу на сайті кіберполіції для перевірки легітимності інформації (сайт, номер мобільного телефону, номер банківської картки). Крім того, серед громадян буде поширюватися друкована інформація з елементарними правилами кіберзахисту.» ***(Кіберполіція запустила новий проект // «Херсонщина за день» (http://ksza.ks.ua/news/society/82214-kberpolcya-zapustila-noviy-proekt.html). 07.03.2019).***

***

«Михаилу Бродскому грозит судебное разбирательство в случае, если будет доказана его причастность к сокрытию международного киберпреступника. Полиция проверяет связь между киевским бизнесменом и украинским хакером, которого разыскивает спецслужба Великобритании.

…Департамент контрразведовательной защиты интересов государства в сфере информационной безопасности Службы безопасности Украины получил запрос от коллег из Великобритании о содействии в расследовании международных преступлений. Национальное агентство по борьбе с преступностью Великобритании (NCA) подозревает гражданина Украины в соучастии в ряде краж информации, что повлекло за собой финансовые махинации.

Работая из Украины, хакер взламывал личные данные пользователей из стран ЕС, бывшего СНГ, США и Великобритании. Он охотился на электронные кошельки, биткоин-кошельки, кредитные карты, а также логины и пароли от сайтов.

Британской спецслужбе удалось установить связь между гражданином Великобритании и украинцем: они обменивались информацией на одном из форумов. Украинец добывал данные, британец – перепродавал. Пока неизвестно, сколько вырученных средств заработала преступная группировка.

Установив личность хакера, украинские правоохранители начали проводить следственные действия. Они выяснили, что подозреваемый работает не один, а имеет отношение к одной из неформальных хакерских группировок. Источник в

Нацполиции сообщил журналистам, что фигурантом дела может быть бизнесмен и политик Михаил Бродский. В данном случае, ему инкриминируют сокрытие преступника по Статье 396 Криминального кодекса Украины. Используя личные связи и влияние политик, по одной из версий, помог подозреваемому выпасть из поля зрения сыщиков. Для этого использовалась одна из его квартир под Киевом. Впрочем, пока неизвестно, выступал ли Бродский заказчиком преступных действий, озвученных британской спецслужбой. Украинские правоохранители проверяют все факты.

С недавних пор Михаил Бродский попал под пристальное внимание отдела кибербезопасности. СМИ тоже не единожды писали о его причастности хакерским группам – здесь информация о взломе австралийских серверов; а тут сообщение об атаке на сайт с петициями жителей Киева.» ***(Михаила Бродского подозревают в сокрытии хакера-преступника — источник // Politica.com.ua (http://politica.com.ua/mixaila-brodskogo-podozrevayut-v-sokrytii-xakera-prestupnika-istochnik/). 05.03.2019).***

***

«Компания Facebook подала в суд на украинцев, которые нарушили законы, связанные со взломом…

Известно, что обвиняемые - граждане Украины Андрей Горбачов и Глеб Случевский, связанные с компанией Web Sun Group, расположенной в Киеве, с 2016 до 2018 года скомпрометировали около 63 тысяч браузеров, используемых пользователями соцсети, и нанесли Facebook ущерб на сумму более 75 тысяч долларов.

Есть информация, что злоумышленники распространяли вирусы с фейковых аккаунтов, среди которых "Елена Стельмах", "Аманда Питт" и "Игорь Коломиец".

По заявлению Facebook, хакеры ориентировались на русскоговорящий сегмент пользователей и использовали онлайн-викторины и тесты. В итоге юзеры устанавливали вредоносные расширения, которые считывали данные их профилей…» ***(Facebook подал в суд на двух украинцев: хакеры взломали 63 тысячи аккаунтов // "Судово-юридична газета" (https://sud.ua/ru/news/ukraine/137050-facebook-podal-v-sud-na-dvukh-ukraintsev-khakery-vzlomali-63-tysyachi-akkauntov). 09.03.2019).***

***

«Безработный украинец получил два года лишения свободы с испытательным сроком в один год за модификацию и продажу в сети вредоносного программного обеспечения. Мужчина пошел на сделку со следствием и полностью признал свою вину, хотя следствие не установило и половину обстоятельств дела…

Согласно обвинительному акту, мужчина в неустановленном следствием месте, в неустановленное время, используя неустановленную досудебным расследованием электронно-вычислительную машину (компьютер), имея умысел на создание с целью сбыта вредоносных программных средств, предназначенных для несанкционированного вмешательства в работу электронно-вычислительных

машин (компьютеров), загрузил неустановленному пользователю Интернет-файл с названием «Revenge-RAT v.0.2.exe».

Данный файл является программой с автоматическим скрытым установлением, которая предоставляет возможность удаленного управления компьютерами и скрытого наблюдения за их пользователями. Она обладает различными настройками, которые добавляются при создании конечного файла.

В дальнейшем, обвиняемый, имея специальные технические знания в области программирования, путем модификации существующего программного средства, создал с целью сбыта вредоносное программное обеспечение под названием «Revenge-RAT v.0.2 .exe» (инфицировано вирусом типа «Trojan») невидимое для антивирусов, предназначенное для несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров). После этого он для сокрытия созданного им вредоносного программного обеспечения с помощью архиватора «WinRAR» поместил файл с названием «Revenge-RAT v.0.2.exe» в архив «teamviewer.rar».

10 декабря 2018 года подозреваемый через электронное письмо сбыл покупателю вирус.

Кроме того, действуя таким же образом и замаскировав «Revenge-RAT v.0.2.exe» в архивы «32.rar» та «64.rar», 21 декабря того же года обвиняемый продал их с помощью мессенджера Telegram за 4200 гривен.

– Таким образом, суд приходит к выводу, что обвиняемый своими умышленными действиями, которые выразились в создании и сбыте вредоносных программных средств, предназначенных для несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров), совершил уголовное преступление, предусмотренное ч. 1 ст.361-1 УК Украины, а также своими умышленными действиями, которые выразились в создании и сбыте вредоносных программных средств, предназначенных для несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров), совершенными повторно, совершил уголовное преступление, предусмотренное ч.2 ст.361-1 УК Украины, – говорится в приговоре…» ***(Владимир Кондрашов. Украинец получил два года за модификацию и продажу ви руса // Internetua (http://internetua.com/ukrainec-polucsil-dva-goda-za-modifikaciua-i-prodaju-virusa). 11.03.2019).***

***

«Украинский хакер признан виновным в несанкционированном вмешательстве в работу компьютеров и приговорен к штрафу в 10 200 гривен. В суде мужчина объяснил, что собирал деньги на лечение бабушки…

Как говорится в приговоре, уроженец Смелы Черкасской области через Telegram в марте 2018 года приобрел вредоносное программное обеспечение для кражи персональных данных третьих лиц: три файла, видео-инструкцию и архив, в котором находился «джоинер», программное обеспечение для соединения нескольких файлов, файл «error» и инструкция о распространении вредоносного программного обеспечения, а также файл «ИНФО».

Используя «джоинер», к файлу-стилеру обвиняемый добавил информацию об ошибке из файла «error» для сокрытия его работы. Обвиняемый распространил вредоносное программное обеспечение, сообщив в видеоблоге «You Tube» заведомо ложную информацию о том, что данный файл – «хит мод» к игре, который помогает лучше играть. В файле скрывался «стилер» для получения персональных данных пользователей для последующей их продажи на форуме. В результате, говорится в материалах дела, был совершен несанкционированный доступ к электронно-вычислительным машинам (персональным компьютерам) пользователей всемирной сети Интернет, которые загружали файл, а именно: в апреле 2018 года, в неустановленное день и время, обвиняемый совершил с помощью файла несанкционированный доступ к логину и паролю двух банковских счетов в АТ КБ «ПриватБанк» и логину и паролю одной страницы социальной сети «Facebook».

В судебном заседании обвиняемый вину в совершении инкриминируемого уголовного преступления признал полностью и пояснил, что временно не работал, нужны были денежные средства на лечение бабушки, поэтому за 1400 грн в сети Интернет приобрел программное обеспечение, которое позволяло получить несанкционированный доступ к персональным данным других пользователей. В судебном заседании просил назначить наказание в виде штрафа.

Суд признал хакера виновным в совершении преступления, предусмотренного ч.1 ст.361 УК Украины и назначил ему наказание в виде 600 необлагаемых минимумов доходов граждан, что составляет 10200 гривен без лишения права занимать определенные должности или заниматься определенной деятельностью. Кроме того, с обвиняемого взыскали процессуальные расходы на проведение экспертизы в сумме 858 грн.» ***(Владимир Кондрашов. Украинский хакер воровал данные банковских карт, чтобы вылечить баб ушку // Internetua (http://internetua.com/ukrainskii-haker-voroval-dannye-bankovskih-kart-cstoby-vylecsit-babushku). 04.03.2019).***

***

«Бывший сотрудник Государственной фискальной службы заплатит около 15 тысяч гривен за кражу данных о компаниях из автоматизированной информационной системы «Налоговый блок»…

Обвиняемый, будучи бывшим работником Сторожинецкого отделения Выжницкой ГНИ ТУ ГФС в Черновицкой области, в период с 7 по 12 июня 2018 года, находясь в одном из служебных кабинетов местного отделения налоговой, пользуясь дружескими отношениями с работниками ДФС, без их ведома, умышленно совершил несанкционированное вмешательство в работу автоматизированной системы (электронной базы данных ДФС) - АИС «Налоговый блок», созданной и защищенной в соответствии с действующим законодательством.

По версии следствия, мужчина, под предлогом подзарядки своего мобильного телефона, с помощью USB-кабеля, подключив мобильный телефон к служебному компьютеру, на котором было установлено программное обеспечение для доступа к АИС «Налоговый блок», вошел в указанную автоматизированную

систему и, используя мобильный телефон в качестве накопителя, сохранил на нем полученную информацию с ограниченным доступом о хозяйственных операциях субъектов хозяйствования ООО «Бартош и Ко» и ООО «Экспорт-импорт транс «Феличита»». Мужчина скачал на телефон сведения о виде, размере, весе, объеме поставленных товаров, реквизитах контрагентов, валюте расчетов, странах назначения.

Обвиняемый, согласно предварительной договоренности, по электронной почте прислал заказчику письмо с прикрепленным к нему файлом формата (rtf) под названием «ООО» размером 403Кб, в котором содержалась информация с ограниченным доступом по хозяйственным операциям двух компаний.

4 февраля 2019 между прокурором и подозреваемым заключено соглашение о признании виновности, согласно которому последний полностью признал свою виновность в совершении уголовного преступления по ч.1 ст.361 УК Украины.

Суд соглашение утвердил и назначил обвиняемому согласованное наказание в виде штрафа в размере 600 необлагаемых минимумов доходов граждан, что составляет 10200 гривен, без лишения права занимать определенные должности или заниматься определенной деятельностью. Кроме того, мужчина также оплатит 4433 гривны на привлечение экспертов.» ***(Владимир Кондрашов. Суд: бывший сотрудник ГФС воровал из базы данных сведения о компаниях для их конкурентов // Internetua (http://internetua.com/sud-byvshii-sotrudnik-gfs-voroval-iz-bazy-dannyh-svedeniya-o-kompaniyah-dlya-ih-konkurentov). 15.03.2019).***

***

«…Працівники Поліського управління Департаменту кіберполіції спільно зі слідчими Рівненської поліції, за процесуального керівництва Рівненської місцевої прокуратури, викрили 32-річного мешканця Буковини у поширенні шкідливого програмного забезпечення.

Працівники кіберполіції встановили: 32-річний мешканець Буковини створив та адміністрував велику кількість інтернет-ресурсів. На створених ресурсах він розміщував шкідливе програмне забезпечення для майнінгу криптовалюти. Використовуючи обчислювальні можливості процесора та графічного адаптера, зловмисник втручався в роботу електронно-обчислювальної техніки відвідувачів вищевказаних Інтернет-ресурсів. Це призводило до порушення встановленого порядку маршрутизації інформації та подальшого погіршення роботи комп’ютерів відвідувачів…

Кримінальне провадження розпочато за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) КК України. Зловмиснику загрожує до шести років ув’язнення.» ***(Кіберполіція встановила молодика, який майнив криптовалюту за рахунок більш як мільйона українців // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vstanovila-molodika-yakij-majniv-kriptovalyutu-za-raxunok-bilsh-yak-miljona-ukrajinczіv/). 26.03.2019).***

***

«У штаб-квартирі НАТО підтвердили готовність активно співпрацювати з Україною для протидії кіберзагрозам

Про це повідомила голова постійної делегації у Парламентській асамблеї НАТО, народний депутат Оксана Юринець під час круглого столу «Інформаційна та кібербезпека в контексті євроатлантичної інтеграції»…

Нардеп наголошує, що співпраця України з НАТО в напрямку кіберзахисту ведеться з 2014 року…

"Це створення центру реагування на кіберінциденти, надання обладнання для лабораторій з розслідування кібератак, тренування та дорадча допомога. Все це ведеться з 2014 року, але особливо необхідним та активним це буде в цьому році", - зазначила депутат ВР.» ***(У НАТО розповіли, як допомагали Україні з кібербезпекою з 2014 року // Espreso.tv (https://espreso.tv/news/2019/03/11/u_nato_zayavyly_pro_gotovnist_do_spivpraci_z_ukrayinoyu_schodo_kiberbezpeky). 11.03.2019).***

***

«У Брюсселі 20 березня відбувся неформальний міні-саміт Україна – ЄС за участі президента України Петра Порошенка, президента Європейської ради Дональда Туска, президента Єврокомісії Жана-Клода Юнкера і президента Європарламенту Антоніо Таяні.

Як повідомляє прес-служба глави держави, в ході переговорів сторони погодили підходи до розвитку відносин між Україною та ЄС на найближчу перспективу і координацію спільної протидії викликам…

В ході міні-саміту сторони домовилися координувати зусилля з протидії зовнішньому втручанню в виборчі процеси як в Україні, так і в Європейському союзі, зокрема в сфері кібербезпеки і боротьби з дезінформацією…» ***(В ЄС запевнили Порошенка в беззастережній підтримці України // KyivTime – Київський час (https://kyivtime.co.ua/v-yes-zapevnyly-poroshenka-v-bezzasterezhnij-pidtrymtsi-ukrayiny-28760/). 21.03.2019).***

***

«Національна гвардія штату Пенсільванія (США) виявила інтерес до перспективи співпраці з регіональним центром комп'ютерної безпеки, який створюється Литвою в Каунасі.

Про це за підсумками зустрічі в штабі американського формування президент балтійської республіки Даля Грібаускайте, передає її прес-служба.

За її словами, американські експерти готові сприяти забезпеченню безпеки кібернетичного простору Литви…» ***(Нацгвардія США зацікавилася в регіональному кіберцентрі Литви, - президент // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (https://day.kyiv.ua/uk/news/130319-nacgvardiya-ssha-zacikavylasya-v-regionalnomu-kibercentri-lytvy-prezydent). 13.03.2019).***

***

«Компания Fortinet опубликовала результаты своего новейшего ежеквартального исследования глобальных угроз кибербезопасности Global Threat Landscape Report. Согласно опубликованным данным, киберпреступники прибегают ко все более изощренным методам атак, осуществляя их, например, через устройства Интернета вещей, которые в подавляющем большинстве случаев никак не защищены, или адаптируя вредоносные программы на базе открытых исходных кодов, чтобы превращать их в новые угрозы.

Согласно индексу угроз Fortinet Threat Landscape Index, киберпреступники продолжали без устали работать даже в праздники. После драматичного начала рост индекса Exploit Index во второй половине квартала остановился. Несмотря на то, что общая активность киберзлоумышленников несколько снизилась, количество уязвимостей на компанию (exploits per firm) увеличилось на 10%, а число зафиксированных уникальных уязвимостей выросло на 5%. В то же время, более сложными становятся ботнеты, и их теперь труднее обнаружить. Время инфицирования ботнетом выросло на 15%, примерно до 12 дней на фирму. Поскольку для распространения атак киберпреступники используют средства автоматизации и алгоритмы машинного обучения, департаментам безопасности необходимо использовать те же инструменты для противодействия столь современным и изощренным методам атак.

Конвергенция физических вещей и аспектов кибербезопасности приводит к расширению поверхности атаки, то есть приводит к увеличению числа атакуемых объектов. Шесть из двенадцати наиболее распространенных уязвимостей имели отношение к Интернету вещей, и четыре из шести наиболее распространенных уязвимостей были направлены на IP камеры наблюдения. Доступ к этим устройствам позволяет киберпреступникам следить за частной жизнью, планировать противоправную деятельность на физическом объекте, или получать доступ к сетевым системам для запуска DDoS атак или атак с целью вымогательства выкупа. Важно понимать, что атаки могут осуществляться даже посредством устройств, которые мы используем для контроля и обеспечения безопасности.

Вредоносные инструменты с открытым исходным кодом являются весьма полезными для сообщества профессионалов в области информационной безопасности: с их помощью специалисты могут тестировать защиту, исследователи могут изучать различные угрозы, а ведущие семинаров — использовать реальные примеры из практики. Исходные коды подобных инструментов опубликованы на многочисленных сайтах, например, на GitHub. Поскольку эти коды доступны для всех желающих, ими могут воспользоваться и злоумышленники для своих противоправных действий. В частности, они могут адаптировать и модернизировать эти вредоносные инструменты для реализации новых угроз, в значительной степени для создания так называемого ransomware, то есть вредоносных программ с целью вымогательства выкупа. В качестве примера

того, где подобный вредоносный код был использован для осуществления новых атак, можно назвать ботнет Mirai IoT. С момента его появления в 2016 году количество различных вариантов этого ботнета продолжает неуклонно расти. Для киберпреступников инновации открывают невероятные возможности.

Достижения в области стеганографии позволяют вдохнуть новую жизнь в старые типы атак. Стеганография обычно не используется в наиболее часто встречающихся атаках, однако в прошлом квартале топ-лист наиболее активных ботнетов возглавил Vawtrak. Это свидетельствует о том, что злоумышленники все пристальнее присматриваются к этому типу атак. Кроме того, в течение квартала исследователи обнаружили образцы вредоносных программ, использующие стеганографию для того, чтобы спрятать непосредственно вредоносный код в мемах, которые распространяются по социальным сетям. В ходе атаки после попытки связаться с командным сервером, код ищет изображения в соответствующей ленте в Twitter, загружает их и затем ищет в них спрятанные команды для дальнейшего распространения. Этот скрытый подход показывает, что злоумышленники продолжают экспериментировать с различными вариантами развития своего вредоносного кода.

Бесплатные программные продукты с размещенной в них рекламой по-прежнему не просто досаждают, а несут в себе угрозу. На глобальном уровне рекламное ПО является наиболее распространенным способом заражения вредоносными программами для большинства регионов — на его долю приходится более четверти всех заражений в Северной Америке и Океании, и почти четверть — в Европе. Поскольку рекламное ПО весьма распространено в магазинах мобильных приложений, этот тип атак представляет серьезную угрозу особенно для ничего не подозревающих пользователей мобильных устройств.

В связи с продолжающейся конвергенцией информационных технологий (ИТ) и операционных технологий (ОТ), в рассматриваемом периоде были отмечены относительные изменения распространения и частоты атак на эти окружения. К сожалению, в большинстве случаев увеличился и уровень распространения, и частота атак. В частности, возвращение вредоносной Shamoon в виде волны атак в декабре указывает на то, что эти разрушительные атаки могут повторяться с еще большей силой. Кибератака, нацеленная на ОТ-систему, или даже просто на подключенные к сети устройства, например, на клапаны, датчики или выключатели, может привести к разрушительным физическим последствиям, в том числе для критически важной инфраструктуры и сервисов, окружающей среды или даже угрожать жизням людей.

Данные об угрозах, представленные в исследовании за минувший квартал, в очередной раз подтверждают многие из тех тенденций, которые были спрогнозированы глобальной исследовательской фирмой FortiGuard Labs. Чтобы предвосхищать действия злоумышленников, организациям необходимо трансформировать свои стратегии безопасности в рамках своей общей работы по цифровой трансформации. Им необходима платформа безопасности, которая бы охватывала все сетевое окружение, от устройств Интернета вещей до облачных инфраструктур, и которая бы интегрировала все элементы безопасности для минимизации современных угроз и для защиты расширяющейся поверхности атак.

Этот подход позволит организациям оперативно и на должном уровне обмениваться информацией об угрозах, сокращает необходимые окна обнаружения (windows of detection), и обеспечивает автоматизированный инструмент для нейтрализации современных угроз.» ***(Fortinet исследовала глобальные угрозы кибербезопасности // ChannelForIT (http://channel4it.com/publications/Fortinet-issledovala-globalnye-ugrozy-kiberbezopasnosti-33432.html#). 11.03.2019).***

***

«Microsoft представила 24-й отчет об угрозах информационной безопасности Security Intelligence Report. Для его подготовки эксперты проанализировали 6,5 трлн сигналов, которые проходят через облачные ресурсы Microsoft каждый день. Данные были предоставлены корпоративными и частными пользователями, которые согласились поделиться ими с привязкой к геолокации.

В отчете выделены четыре основные типа атак: фишинг, программы-вымогатели, ПО для скрытого майнинга и атаки на цепочку поставок ПО. Согласно документу, самым быстрорастущим типом атак остается фишинг, количество атак вирусов-вымогателей снижается, но вместо них злоумышленники перешли к более скрытным методам, а именно, майнингу криптовалют.

Популярность фишинга стремительно растет, за 2018 г. среднемесячный показатель числа атак вырос более чем на 350%. Microsoft ежемесячно анализирует и сканирует более чем 470 млрд электронных писем на предмет фишинговых и вредоносных атак. За 2018 г. среднемесячный показатель фишинга вырос с 0,14% (644 млн писем в месяц) до 0,49% (2 млрд 254 млн) в месяц. В компании ожидают продолжения этой тенденции в обозримом будущем, поскольку действия злоумышленников направлены не на поиск технических уязвимостей, а на человеческие слабости.

Снижение количества атак вирусов-вымогателей в прошлом году демонстрирует, как меры компьютерной безопасности заставляют злоумышленников менять свои подходы. В 2017 г. вирусы-вымогатели представляли собой серьезную угрозу, именно поэтому так примечательно снижение числа их атак: среднемировой показатель снизился на 73%. Злоумышленники перешли от этого весьма заметного метода к более скрытным атакам, поскольку пользователи стали более грамотно реагировать на угрозы: отказываются платить злоумышленникам, применяют резервное копирование данных.

В некоторых странах, таких как Эфиопия (0,77%), Монголия (0,46%), Камерун (0,41%) эта угроза остается актуальной из-за низкой культуры кибербезопасности. Самая благоприятная ситуация с программами-вымогателями в Ирландии (0,01%), Японии (0,01%), США (0,02%), Великобритании (0,02%) и Швеции (0,02%).

По среднемесячному числу атак в 2018 г. программы-вымогатели уступили майнингу криптовалют (0,05% против 0,12%). Злоумышленники стали активно внедрять скрытый майнинг и начали использовать вычислительные мощности компьютеров своих жертв для генерации криптовалют. Вторжение не только

снижает производительность системы, но может нанести и более значительный вред.

Можно проследить зависимость числа подобных атак от стоимости криптовалют. Количество вирусов для майнинга выросло почти в 2,5 раза. Например, в марте зафиксирован резкий рост подобных атак по всему миру.

Самые опасные вирусы работают через браузеры, мошенникам не нужно заставлять жертву скачивать какое-либо дополнительное ПО. Некоторые сервисы рекламируют браузерные приложения для майнинга как способ монетизации трафика веб-сайтов. В этом случае владельцам ресурсов уже не нужно полагаться на доход с рекламы. Когда пользователь заходит на страницу со встроенным вирусом, у него сильно сокращается производительность компьютера и растет расход электричества. Мошенники таким образом получают доступ к мощностям тысяч компьютеров.

Страны, в которых специалисты чаще всего сталкивались с вирусами-майнерами, это Эфиопия (5,58%), Танзания (1,83%) и Пакистан (1,47%). Реже всего этот тип вредоносного ПО проявлялся в Ирландии (0,02%), Японии (0,02%) и США (0,02%).

Атаки на цепочку поставок ПО — это еще одна тенденция, которую Microsoft отслеживает последние несколько лет. Злоумышленники внедряют вирус в исходное приложение или пакет обновлений. Пользователи доверяют вендорам и самостоятельно устанавливают вредоносную программу на свои компьютеры, воспринимая ее за продукт известного поставщика.

В 2018 г. первой (и самой крупной) атакой данного типа стал троян Dofoil, за первые 12 часов действий которого Windows Defender Antivirus блокировал более 400 тысяч атак, направленных на пользователей России (73%), Турции (18%), Украины (4%) и других стран. Кроме того, было несколько атак, компрометирующих облачные сервисы, например, зараженные расширения Chrome, которые устанавливали вредоносный файл clickfraud, различные скомпрометированные репозитории Linux, вредоносные плагины WordPress, которые в том числе позволяли злоумышленникам публиковать контент на сайтах WordPress и т.д.

Среднемесячный показатель числа вредоносных программ в мире за 2018 г. снизился с 6,29% до 5,07%. Однако, в некоторых странах, например, в Эфиопии (26,3%) и Пакистане (18,94%), все еще наблюдается высокий показатель атак вредоносных программ, это является результатом низкого уровня цифровой культуры: осведомленности пользователей о принципах безопасности. Использование нелицензионного программного обеспечения также может быть источником вредоносного ПО. Кроме того, причиной часто выступают площадки, незаконно предлагающие бесплатное программное обеспечение или контент, например, потоковое видео.

Страны, в которых специалисты чаще всего сталкивались с вредоносным ПО, это Пакистан (18,94%), Палестина (17,5%), Бангладеш (16,95%) и Индонезия (16,59%). Реже всего вредоносное ПО проявлялось в Ирландии (1,26%), Японии (1,51%), Финляндии (1,74%), Норвегии (1,79%) и Нидерландах (1,82%).» ***(Число фишинговых атак в прошлом году выросло на 350% // «Компьютерное***

Обозрение»
(https://ko.com.ua/chislo_fishingovyh_atak_v_proshlom_godu_vyroslo_na_350_127984). 04.03.2019).

***

«Производитель решений для обеспечения информационной безопасности Trend Micro опубликовал исследование, посвященное ситуации с киберугрозами в 2018 году.

За рассматриваемый период количество атак с использованием вредоносных веб-адресов, доступ к которым удалось заблокировать, увеличилось на 269% относительно 2017 года. Число заблокированных попыток пользователей с уникальным IP-адресом перейти на фишинговый сайт подскочило на 82%.

Кроме того, злоумышленники продолжают компрометировать деловую переписку. Используя метод социальной инженерии, создавая знакомое визуальное оформление и контекст письма, хакерам удается обойти систему безопасности и обмануть пользователя. Так, за 2018 год был зафиксирован 28-процентный рост подобных атак.

Целью злоумышленников стали и офисные программы, которые применяются в компаниях. Среди уязвимостей, раскрытых в 2018 году, 60% случаев было классифицировано как "средний уровень" угроз, что на 3% больше, чем в 2017 году. А число уязвимостей с критическим уровнем опасности снизилось с 25% (2017 год) до 18% (2018 год).

В исследовании отмечается снижение волны вирусов-вымогателей: в компании Trend Micro указали на резкое падение их активности на 91%. Однако "вымогатель" WannaCry сохранил свои позиции и остался одной из основных угроз: в 2018 году было обнаружено более 600 тысяч кибератак.» ***(Фишинг стал одним из самых популярных методов кибератак в 2018 году // Goodnews.ua (http://goodnews.ua/technologies/fishing-stal-odnim-iz-samyx-populyarnyx-metodov-kiberatak-v-2018-godu/0. 03.03.2019).***

***

«BetterCloud выпустили свой первый отчет о внутренних угрозах: "State of Insider Threats in the Digital Workplace 2019"… Так, 91% ИТ-специалистов и экспертов в области безопасности чувствуют себя уязвимыми для внутренних угроз, а 75% считают, что самые большие риски связаны с такими облачными приложениями, как популярные решения для хранения файлов и электронной почты - Google Drive, Gmail, Dropbox и другие.

"Рост SaaS на цифровом рабочем месте сделал компании более уязвимыми внутренним угрозам, чем когда-либо. Основная причина в том, что SaaS предоставил пользователям все управление над данными в приложении, и, как следствие, ИТ-отдел и отдел безопасности потеряли контроль. Еще одной серьезной проблемой является сложность архитектуры приложений SaaS, которая затрудняет управление такими функциями, как совместное использование разрешений и конфигураций. Поскольку SaaS - это новая территория, компании не

готовы иметь дело со "слепыми зонами" безопасности, создаваемыми этими проблемами", - говорится в докладе.

В рамках исследования BetterCloud опросили около 500 специалистов по ИТ и сетевой безопасности из ведущих мировых организаций. Компания также изучила свои данные о собственных продуктах, чтобы прояснить, где профессионалы в области ИТ и безопасности наиболее уязвимы. Среди ключевых выводов:

Почти все опрошенные ИТ-специалисты и эксперты по безопасности (91%) чувствуют себя уязвимыми для внутренних угроз.

62% респондентов считают, что самая большая угроза безопасности исходит от благонамеренного, но небрежного конечного пользователя.

75% считают, что наибольшие риски связаны с облачным хранилищем, решениями для электронной почты (например, Google Drive, Dropbox, Box, OneDrive и т. д.) и самой электронной почтой (например, Gmail, Office 365).

46% ИТ-лидеров (руководители ИТ-подразделений и выше) считают, что рост числа приложений SaaS делает их наиболее уязвимыми.

40% респондентов считают, что они наиболее уязвимы для раскрытия конфиденциальной деловой информации (финансовой информации, списков клиентов).

Только 26% руководителей уровня С говорят, что вложили достаточно средств, чтобы снизить риск внутренних угроз, по сравнению с 44% ИТ-менеджеров.

"Исторически компании полагались на механизмы периметров безопасности, такие как брандмауэры и системы обнаружения вторжений, для хранения данных внутри стен компании, но эта парадигма просто не работает в облаке. Наши результаты дают понять, что для борьбы с этими растущими угрозами организации должны расширять свою защиту, отслеживая и управляя пользователем и всеми его взаимодействиями в приложении", - утверждают эксперты.» ***(Ирина Фоменко. Исследование: внутренние киберугрозы представляют наибольший риск для безопасности // Internetua (http://internetua.com/issledovanie-vnutrennie-kiberugrozy-predstavlyauat-naibolshii-risk-dlya-bezopasnosti). 21.03.2019).***

***

«По прогнозам IDC, мировые затраты на аппаратные средства, программное обеспечение и сервисы, предназначенные для обеспечения безопасности, достигнут в 2019 году $103,1 миллиардов. Таким образом, этот показатель обойдет на 9,4% показатель 2017 года. Такие данные IDC приводит в своем материале «Worldwide Semiannual Security Spending Guide». Ожидается, что пик расходов на защитные решения придется на 2022 год, когда сумма достигнет $133,8 миллиардов. В 2019 самые большие суммы на кибербезопасность потратят три сферы: банки, дискретное производство и госучреждения. В общей сумме они потратят более $30 миллиардов. Три другие сферы — обрабатывающая промышленность, профессиональные услуги и телекоммуникации — потратят в этом году более $6 миллиардов. Однако самый большой рост расходов все же придется на государственные учреждения.

«В процессе анализа самых быстрорастущих сегментов безопасности мы наблюдали целый спектр сфер вроде кредитных организаций и госучреждений, которым надлежит обеспечить безопасность конфиденциальной информации», — комментирует вице-президент IDC по программным продуктам Джессика Гепферт. «Помимо этого, телекоммуникационным компаниям также придется увеличить свои расходы на безопасность. Однако в целом можно сделать вывод, что независимо от индустрии такие технологии останутся в приоритете в процессе распределения бюджета». ***(Олег Иванов. IDC: Мировые расходы на безопасность достигнут $103,1 млрд в 2019 году // ООО «АМ-МЕДИА» (https://www.anti-malware.ru/news/2019-03-21-1447/29209). 21.03.2019).***

***

«Большинство компаний во всех странах мира осознают ценность данных, однако все еще сталкиваются со сложностями в их надлежащей защите.

Компания Dell EMC объявляет результаты третьего исследования Global Data Protection Index, демонстрирующего быстрый темп роста данных, который составил 569%, а также внушительный скачок в количестве «компаний-первопроходцев» (Adopters) по защите данных почти на 50 процентных пунктов по сравнению с 2016 годом.

В исследовании приняли участие 2200 руководителей, принимающих решения в области ИТ, как из государственных, так и из частных организаций с количеством сотрудников от 250 человек и выше в 18 странах и 11 отраслях промышленности. Исследование обеспечивает всестороннее понимание состояния защиты данных и зрелости их стратегий. В частности, в ходе опроса было выявлено увеличение среднего объема обработки данных — с 1,45 петабайта (ПБ) в 2016 году до 9,70 ПБ в 2018 году, а также высокий уровень осведомленности о ценности данных. Фактически, 92% респондентов осознают потенциальную ценность данных, а 36% уже их монетизируют. Несмотря на признание положительных факторов, большинство респондентов пытаются должным образом защитить свои данные. Тревожным фактом является растущий объем необратимой потери данных. Сочетание данных факторов лежит в основе многих выводов исследования…

Инциденты сбоев в работе случаются часто, но более тревожным фактом является растущий объем необратимой потери данных. Более чем три четверти (76%) респондентов во всем мире сталкивались с определенными видами сбоев в течение 12-месячного периода, а 27% не смогли восстановить данные с помощью имеющегося решения для их защиты, что превышает показатели 2016 года почти вдвое (14%).

В то же самое время, 76% респондентов во всем мире также пользуются услугами по меньшей мере двух поставщиков систем защиты данных, что увеличивает угрозу возникновения сбоев в течение того же 12-месячного периода на 35% по сравнению с теми, кто пользуется услугами одного вендора. Незапланированные простои систем стали наиболее распространенным видами сбоев (43%) для тех, кто пользуется системами двух или более вендоров. За этим

следовали атаки в целях вымогательства, которые становились препятствием к доступу данных (32%) и их потере (29%).

Хотя незапланированные простои систем носят всё более массовый характер, потеря данных обходится намного дороже. Например, те, кто столкнулся с простоями, наблюдали в среднем 20 часов простоя за последние 12 месяцев, что стоило им 526 845 долларов, в то время как те, кто столкнулся с потерей данных, потеряли в среднем 2,13 терабайта на общую сумму около 1 миллиона долларов. Кроме того, многие из тех, кто столкнулся со сбоями, также отмечали, что они имели далеко идущие последствия для предпринимательской деятельности, начиная от доверия клиентов к торговой марке и заканчивая производительностью труда работников, а также многие другие.

Стоимость зависела не только от количества потерянных данных, но и от ценности самих данных. Очевидно, что предприятия осознают это, так как 81% опрошенных признали, что более серьезно относятся к защите тех категорий данных, которые имеют наибольшую денежную ценность…

В то время как те компании, которые отнесены к категории «первопроходцев» (Adopters) защиты данных, увеличились в количестве почти на 50 процентных пунктов (с 9% в 2016 до 57% в 2018 году), а количество «компаний-лидеров» (Leaders) увеличилось на 10 процентных пунктов (с 2% в 2016 до 12% в 2018 году), большинство предприятий все еще изо всех сил пытаются найти то решение, которое бы должным образом соответствовало их потребностям. Большинство респондентов (95%) сталкивались по меньшей мере с одной проблемой в области защиты данных. На глобальном уровне выделяют три основные проблемы:

Сложность настройки и эксплуатации программного и аппаратного обеспечения защиты данных, а также растущие затраты на хранение и управление резервными копиями из-за быстрого увеличения количества данных занимают первое место и составляют 46%.

Отсутствие решений по защите данных в отношении новых технологий занимает второе место и составляет 45%.

Обеспечение соответствия таким нормативам, как GDPR, занимает третье место и составляет 41%.

Среди тех, кто пытается найти решение для защиты данных в отношении новых технологий, более половины (51%) заявили, что не могут найти подходящего решения для защиты данных искусственного интеллекта и данных машинного обучения; за ними следуют облачные приложения (47%) и Интернет вещей (IoT) (40%).

Проблемы, связанные с новыми технологиями и быстрым увеличением количества данных, только начинают принимать форму. Таким образом, только 16% респондентов считают, что выбранные решения по защите данных смогут решить все будущие задачи…

Согласно «Глобальному индексу защиты данных», от общей ИТ-среды на предприятиях респондентов использование публичного облака в среднем увеличилось с 28% в 2016 до 40% в 2018 году. Почти все предприятия (98%), использующие публичное облако, также применяют его для защиты данных.

Выделяют следующие основные варианты использования публичного облака для защиты данных:

Сервисы резервного копирования и создания моментальных снимков для защиты рабочих нагрузок, создающихся в облачном сервере с использованием новых программных архитектур (41%).

Резервное копирование локальных рабочих нагрузок/данных (41%).

Защита отдельных приложений SaaS (40%).

Облачные версии локального программного обеспечения для защиты рабочих нагрузок публичного облака (40%).

Сервисы резервного копирования и создания моментальных снимков для защиты рабочих нагрузок, создающихся в публичном облаке с использованием устаревших программных архитектур (38%).

При анализе решений по защите данных в публичном облаке совокупность увеличивающегося количества данных играет особо важную роль, на что указали 64% респондентов, назвавшие опции масштабируемости крайне важными. В частности, 41% респондентов привели в качестве примера влияние инфраструктуры или сервисов защиты данных, необходимых для защиты в широких масштабах, а 40% — возможность расширять сервисы по мере увеличения нагрузок на публичное облако…

Нормативные положения о защите данных, такие как «Общий регламент ЕС по защите данных» (GDPR), являются относительно новыми, и их реальное воздействие на индустрию данных еще предстоит осознать. Тем не менее, они быстро стали центральным элементом, поскольку соблюдение нормативных требований вошло в тройку лидеров в списке проблем, связанных с защитой данных, которые были отмечены 41% респондентов.

Более того, только 35% опрашиваемых были уверены в том, что имеющаяся в их компании база и процессы защиты данных соответствуют региональным нормам. Этот настрой начинает воплощаться в жизнь, поскольку 12% респондентов, чьи компании столкнулась с потерей данных или незапланированным простоем в течение последних 12 месяцев, сообщили, что в результате они уплатили штрафные санкции.

«Новым технологиям, таким как искусственный интеллект и Интернет вещей, часто уделяется особое внимание при цифровой трансформации компании, однако данные, которые генерируют эти технологии, играют ключевую роль на пути к переменам», — сказала Бет Фален (Beth Phalen), президент и генеральный директор отдела по защите данных Dell EMC. «Почти 50-процентный рост количества приверженцев защиты данных и тот факт, что в настоящее время большинство предприятий осознают ценность данных, доказывают, что мы находимся на правильном пути к защите и использованию данных, которые стимулируют прогресс человечества».

«Банковская отрасль существенно изменилась за последнее десятилетие», прокомментировал Боб Бендер (Bob Bender), технический директор компании Founders Federal Credit Union. — «До цифровой трансформации самым ценным активом банков были наличные деньги в их хранилищах. Сегодня же данные так же ценны, как и наличность, и нужно их тщательно оберегать и охранять, применяя

системы резервного копирования и восстановления данных, системы обеспечения устойчивости к угрозам кибербезопасности, а также обеспечивая соответствие нормам регуляторов. Сотрудничая с одним партнером, мы уверены, что каждый килобайт данных является ценнейшим ресурсом как для нас, так и для наших клиентов». ***(В мире растет объем необратимой потери данных // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5572461-V-nastoyashhee-vremya-bolshinstvo.html). 22.03.2019).***

***

«Фарид Синх, управляющий директор программы CyberNorth эстонского акселератора Startup Wise Guys, рассказывает, почему сейчас кибербезопасность — перспективное направление для стартапов, как на этом могут заработать украинские команды, и чем им может помочь акселератор.

Мы так глубоко погрузились в кибермир, что наша «жизнь» в нем начала оставлять заметный след на людях и реальном мире. К сожалению, не всегда положительный. Каков масштаб ущерба? Судите сами: по оценкам экспертов, к 2021 году мировые потери от киберпреступлений могут достигнуть $6 трлн. Самое время сосредоточиться на развитии потенциала в области кибербезопасности…

Преимущество стартапов по сравнению с гигантами отрасли – гибкость, быстрота реагирования и относительно скромные бюджеты на разработку продукта. Благодаря этому у них есть все шансы стать локомотивом развития инноваций и очень узкоспециализированных решений, в которых все – и люди, и бизнес, и даже целые государства – сейчас остро нуждаются.

Посмотрите на рост инвестиций. За последние 4 года их объем утроился, и в 2018 году компании, которые занимаются кибербезопасностью, получили рекордные $5,3 млрд венчурного финансирования. Такой колоссальный спрос говорит о том, что у стартапов есть все шансы не только хорошо «выстрелить», но и отлично заработать…

По оценкам экспертов, только от вируса Petya украинская экономика потеряла $466 млн, или 0,5% ВВП в 2018 году. Не говоря уже о киберугрозах, связанных с текущими взаимоотношениями с Россией. Мы отчетливо понимаем, что нынешняя политико-экономическая ситуация в Украине и значительное усиление киберугроз в ближайшем будущем будут только увеличивать запрос на развитие отрасли кибербезопасности.

В то же время мы наблюдаем здесь интересную ситуацию: все эти потрясения и вызовы активизировали украинское киберсообщество в их работе с различными технологиями, но из-за недостатка финансирования эта активность крайне редко перерастает в создание реального продукта.

По собственному опыту работы здесь мы знаем, что в Украине немало технических талантов, способных быстро и качественно создать продукт, который будет пользоваться спросом не только здесь, но и в других странах Европы…

Вот направления кибербезопасности, которые сейчас наиболее перспективны на наш взгляд:

Защита данных. Утечка данных может стоить бизнесу миллионы и даже привести к банкротству. По данным IBM, в среднем ущерб от утечки данных

оценивается в $3,62 млн. А с учетом того, что изобретательность взломщиков и, соответственно, частота взломов растет, продукты, решающие проблемы в этой сфере, будут пользоваться огромным спросом.

Глобальная цифровизация бизнеса и обеспечение конфиденциальности. Вне зависимости от того, использует ли компания частный сервер или облачную платформу для ведения своего бизнеса, большинству предприятий требуются протоколы безопасности для обеспечения сохранения конфиденциальности коммуникаций, передачи данных и так далее. Чем глубже бизнес уходит в интернет, тем больше будет расти потребность в решениях по кибербезопасности.

Работа с Big Data. Актуально как для бизнеса, так и для госсектора, городской инфраструктуры. Атаки на подобные системы чреваты не только финансовыми потерями, государственными угрозами, а и фактической парализацией всей жизни.

Фишинг и пропаганда. Возникновение и непрерывное развитие виртуального пространства дает людям много новых возможностей – для общения, работы, обучения и отдыха. В то же время киберпреступники тоже нашли свою нишу и успешно ее используют: кибершпионаж, кибератаки, пропаганда экстремистских идей и движений – только часть преступлений, совершаемых с использованием технологий, количество и многообразие которых возрастает с каждым годом. Создание новых методов противодействия и борьбы со всем этим актуально, как никогда, и нуждается в инновационном подходе.

CivicTech для образования в области кибербезопасности. Утечка данных, взлом систем и краж персональных данных часто связаны не с высоким уровнем взломщиков систем, а с человеческим фактором и низким уровнем осведомленности в основах кибербезопасности. А значит, какие бы высокотехнологичные решения ни были в распоряжении компаний и госорганизаций, их эффективность будет сводиться к нулю, если люди не будут ими пользоваться и соблюдать правила безопасности. Поэтому самое время обратить внимание на просвещение рядового пользователя в области цифровой безопасности и угроз. Возможности применения современных технологий в этом направлении достаточно широки и все еще не реализованы…» ***(Фарид Синх. Кибербезопасность набирает обороты: как украинским стартапам заработать на этом // AIN.UA (https://ain.ua/2019/03/18/ukrainskie-startapy-kiberbezopasnost/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ainua+%28AIN.UA%29). 18.03.2019).***

***

«Компания Trend Micro обнародовала некоторые результаты опроса, посвященного проблеме дефицита квалифицированных ИБ-кадров, в котором приняли участие ИТ-специалисты из США и десятка стран Европы. 69% опрошенных считают, что использование искусственного интеллекта (ИИ) поможет снизить влияние нехватки профессионалов на качество обеспечения безопасности.

Кроме того, 63% респондентов заявили, что планируют использовать ИИ-технологии, чтобы автоматизировать процессы поддержания и обеспечения

безопасности. Вместе с тем, ИИ не сможет закрыть абсолютно все «пробелы». Например, для таких задач как анализ результатов и управление общей стратегией безопасности, необходимы квалифицированные специалисты по кибербезопасности.

Среди прочего, участники опроса отметили, что нехватка кадров заставляет их расширять программы обучения и использовать аутсорсинговые услуги для выявления и предотвращении угроз.

В прошлом году рост киберугроз ощутили на себе 64% организаций. Сегодня организации имеют общую проблему: отделы по ИТ-безопасности не полностью укомплектованы и занимаются широким кругом вопросов. А согласно исследованию Gartner, нехватка квалифицированных специалистов по безопасности стала постоянной проблемой. Ожидается, что спрос на сотрудников по кибербезопасности будет быстро расти и к 2020 г. рынок столкнется с 1,5 млн открытых вакансий.» ***(Бизнес уповает на ИИ в деле укрепления кибербезопасности // «Компьютерное Обозрение» (https://ko.com.ua/biznes_upovaet_na_ii_v_dele_ukrepleniya_kiberbezopasnosti_128136). 19.03.2019).***

***

«Компания Positive Technologies обнародовала развёрнутый отчёт, посвящённый анализу ситуации с безопасностью во Всемирной сети в прошлом году.

В течение 2018-го зафиксировано на 27 % больше уникальных киберинцидентов, чем годом ранее. Пики атак наблюдались в феврале, мае, июле и в конце года, что связано со всплесками активности злоумышленников в преддверии и во время крупных спортивных соревнований и праздников.

Большинство атак в 2018 году были совершены с целью хищения персональных данных — 42 %. Практически такое же количество кибернападений — 41 % — осуществлено ради финансовой выгоды.

Примерно четверть атак (23 %) затронули частных лиц. Среди юридических лиц в 19 % инцидентов жертвами хакеров стали государственные учреждения, ещё в 11 % случаев пострадали медицинские учреждения, а в 10 % — финансовые организации.

Эксперты Positive Technologies пришли к выводу, что в прошлом году более половины всех кибернападений (55 %) имели целенаправленный характер.

Соотношение атакуемых объектов практически не изменилось. Чаще всего злоумышленники пытались взломать инфраструктуру и веб-ресурсы компаний: это 49 % и 26 % атак соответственно. Доля нападений на банкоматы и POS-терминалы за год сократилась с 3 % до 1 %.

В целом, в 56 % всех атак применялось вредоносное программное обеспечение. Вместе с тем действия злоумышленников становятся всё более хитроумными: атаки осуществляются в несколько этапов, в ходе которых применяются разные методы.

Специалисты прогнозируют, что в текущем году тенденция к росту атак, направленных на хищение данных, скорее всего, сохранится. Мощность DDoS-атак

будет увеличиваться как в связи с продолжающимся ростом ботнетов, так и в связи с использованием новых техник и уязвимостей. Кроме того, ожидаются новые атаки шифровальщиков-вымогателей.» ***(Каждая вторая кибератака имеет целенаправленный характер // Goodnews.ua (http://goodnews.ua/technologies/kazhdaya-vtoraya-kiberataka-imeet-celenapravlennyj-xarakter/). 17.03.2019).***

***

«…Згідно з результатами досліджень, майже всі юридичні фірми мають відкриті критичні прогалини на ПК і серверах, половина — на мережевому обладнанні. 65% юрфірм не мають навіть мінімальної системи захисту, 60% уразливі для дій інсайдерів, а 70% — не захищені від зовнішніх загроз. Причинами цього є відсутність шифрування даних, процесів забезпечення безпеки і реагування на інциденти; відкриті права доступу; з усіх засобів захисту в основному присутні тільки антивірус і слабкі паролі.

На практиці для юридичної фірми або адвокатського об'єднання це означає ряд дуже неприємних речей, а саме… юридична компанія може не лише втратити особисті дані клієнтів та продукти своєї інтелектуальної праці, а й навіть не зуміти вчасно зреагувати на те, що трапилось. І наслідки такої інформаційної недбалості можуть бути глобальні. Порушення конфіденційності даних юридичної фірми та її клієнтів часто призводить до вимагання та шантажу, інсайдерської торгівлі та недобросовісної конкуренції. І це може не лише завдати шкоди репутації — юридична фірма понесе відповідальність, починаючи від фінансової та закінчуючи кримінальною…

Є дві міжнародні, офіційно визнані експертами плани-стратегії, які потрібно розробити кожній юридичній компанії, що турбується про свою кібербезпеку. Перша — це стратегія безперервності бізнесу (англ. Business Continuity Planning), друга — стратегія аварійного відновлення (англ. Disaster Recovery Plan).

Перша — це комплексний стратегічний ряд організаційних заходів, спрямованих на зниження ризиків переривання бізнес-процесів і мінімізацію негативних наслідків у разі збоїв IT-інфраструктури. Друга — стратегія повного розуміння, як потрібно реагувати на стихійне лихо або іншу надзвичайну подію, які можуть вплинути на інформаційні системи, та мінімізувати негативний вплив на діяльність компанії…

Важливим фактором є те, що у випадку атаки на юридичний софт 65% інформації, до якої отримують доступ хакери, належить клієнтам компанії. Юристам слід врахувати, як вирішувати проблему з персональними даними, та прописати ці моменти у договорі про надання юридичних послуг. Звісно, багатьом перспектива атаки здається примарною та навіть неможливою, проте прописавши у договорі можливі ризики, ви убезпечите і клієнтів, і себе…» ***(Питання кібербезпеки у світі юриспруденції // "Судово-юридична газета" (https://sud.ua/ru/news/publication/138379-pitannya-kiberbezpeki-u-sviti-yurisprudentsiyi). 27.03.2019).***

***

«Мировые расходы на кибербезопасность впервые преодолели рубеж в 10 млрд долл. по итогам финальной четверти 2018 г., сообщают исследователи из Canalys. В целом за прошлый год инвестиции в средства кибербезопасности увеличились на 9% «YoY», до 37 млрд долл. По итогам 2020 г. аналитики ожидают преодоление рубежа в 42 млрд долл.

Несмотря на высокий приоритет для многих организаций и постоянно растущее количество различных угроз, в общегодовых ИТ-расходах на кибербезопасность по-прежнему уходит не более 2%.

В 2018 г. на долю традиционного аппаратного и программного обеспечения приходилось не менее 82% общих расходов. Оставшиеся 18% были связаны с тратами на виртуальные устройства и агентов, услуги «cybersecurity is a service». Однако уже по итогам 2020 г. доля традиционного сегмента сократится до 70%.» ***(В прошлом году расходы на кибербезопасность выросли на 9% // «Компьютерное Обозрение» (https://ko.com.ua/v_proshlom_godu_rashody_na_kiberbezopasnost_vyrosli_na_9_128272). 29.03.2019).***

***

«Безопасность была главной темой однодневной конференции AWS Summit, в эту среду собравшей в г. Санта-Клара (штат Калифорния) 6,5 тыс. клиентов и партнёров AWS.

В своей двухчасовой вступительной речи технический директор AWS, Вернер Фогельс (Werner Vogels), говорил об ответственности, которую они, как провайдеры технологий, несут за защиту своих заказчиков и их бизнеса от всё более изощрённых фишинговых атак.

«Сейчас практически не встречаются фронтальные атаки методом грубой силы, — заявил Фогельс. — Только социальная инженерия. Всегда найдётся идиот, который нажмёт на ссылку».

Он напомнил посетителям конференции о широком ассортименте инструментов AWS, с помощью которых её клиенты могут организовать себе автоматическую защиту от киберугроз. Это такие решения, как Amazon Inspector, непрерывно сканирующее код и обеспечивающее соответствие, или AWS CloudTrail, служащее для мониторинга использования облачных ресурсов и записи вызовов API. «А учитывая, что мы встроили шифрование практически во все сервисы AWS, есть прямой смысл им воспользоваться», — добавил Фогельс.

Ещё больше возможностей киберзащиты предоставляют работающие с AWS партнёры. Многие из них создают и распространяют свои средства безопасности с использованием сервисов AWS. Например, стартап Aporeto, изначально использовавший свою версию Kubernetes, сейчас находится в процессе миграции на управляемый сервис Kubernetes, EKS от Amazon. Ещё один стартап сетевой безопасности, Hexagon, использует для тренировки нейросетей глубокого обучения вычислительный движок AWS, а для автоматического предоставления облачных инстансов — бессерверную технологию AWS, Lambda.

AWS сообщила подробности о новом средстве автоматизации Concurrency Scaling, на порядок ускоряющем работу репозитория данных Redshift, и

представила сервис Deep Learning Containers с искусственным интеллектом и инструментарием для развёртывания на различных вычислительных инстансах.

Компания также объявила о доступности ряда продуктов, анонсированных в ноябре, на конференции re: Invent. Среди них App Mesh, Toolkit for IntelliJ и Glacier Deep Archive.» ***(Amazon Web Services акцентирует внимание на кибербезопасности // «Компьютерное Обозрение» (https://ko.com.ua/amazon_web_services_akcentiruet_vnimanie_na_kiberbezopasnosti_128263). 29.03.2019).***

***

«Фонд Карнеги (Carnegie Endowment for International Peace) подготовил отчет о характере кибернетических атак в финансовой сфере и причастности к ним государственных структур.

Интернет ресурсу УкрСтрахование из материалов отчета известно, что с 2007 года произошло 94 кибератаки, которые признаны финансовыми преступлениями. 23 кибератаки или 24% от общего числа, согласно отчету, были совершены при государственной поддержке. В частности, называются Иран, Россия, Китай и Северная Корея, на долю которых приходится большинство подобного рода кибератак.

В отчете содержится вывод о высокой уязвимости финансовых рынков от действий злоумышленников, которые могут действовать в интересах какого-либо государства…» ***(Кибератаки при поддержке государства создают отраслевые системные риски // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/kiberataki-pri-podderzhke-gosudarstva-sozdayut-otraslevyie-sistemnyie-riski). 27.03.2019).***

***

Сполучені Штати Америки

«…Президент США Дональд Трамп в бюджетном запросе в Конгресс США предлагает направить $9,6 млрд для содействия миссиям Минобороны США в киберпространстве, говорится в тексте документа, опубликованном в понедельник на сайте Белого дома…

Тремя ключевыми миссиями Пентагона в киберпространстве в документе называются защита собственных информационных систем, поддержка целей военного командования и защита государства.

Эти инвестиции, говорится в документе, предоставят необходимые ресурсы для наращивания потенциала США в киберпространстве, инвестиций в трудовые ресурсы в этой сфере и сохранения высоких стандартов кибербезопасности в США…» ***(Трамп предлагает выделить Пентагону $9,6 млрд на работу в киберпространстве // Телеграф (https://telegraf.com.ua/mir/usa/4912346-tramp-predlagaet-vyidelit-pentagonu-9-6-mlrd-na-rabotu-v-kiberprostranstve.html). 11.03.2019).***

***

«Президент США Дональд Трамп продлил на год введенное еще Бараком Обамой в 2015 году чрезвычайное положение в связи с угрозой кибератак.

В своем послании Конгрессу Трамп отметил, что вредоносные действия в киберпространстве продолжают представлять чрезвычайную угрозу для США…

По словам Трампа, киберугрозы во многом исходят из-за рубежа и угрожают национальной безопасности, политике и экономике США…» ***(Из-за киберугроз Трамп продлил действие режима ЧП // «Слово и Дело» (https://ru.slovoidilo.ua/2019/03/27/novost/politika/kiberugroz-tramp-prodlil-dejstvie-rezhima-chp). 27.03.2019).***

***

«Руководство Microsoft утверждает, что корпорация ежегодно тратит огромное количество средств на защиту от киберпреступников и поддержание приемлемого уровня информационной безопасности. Если быть точным, как заявил вице-президент Джейсон Зандер, техногиганту обходится все вышеозначенное в $1 миллиард ежегодно. Зандер выразил позицию руководства корпорации, которое считает, что обеспечение безопасности является крайне важным направлением, по которому работать надо постоянно. Также в компании прекрасно понимают, что киберпреступники совершенствуются с каждым годом, изобретая все новые способы проникновения в сети. Следовательно, нельзя расслабляться, приходится постоянно поддерживать грамотный уровень оппозиции. «Поскольку программами от Microsoft пользуются миллионы людей по всему миру, наша задача — обеспечить должный уровень безопасности и надежности этих приложений», — отметил вице-президент американского техногиганта. Именно поэтому корпорация готова вливать такое огромное количество денег в поддержание безопасности всего, что касается продукции, подытожил Зандер…» ***(Олег Иванов. Microsoft ежегодно вливает $1 млрд в безопасность // ООО «АМ-МЕДИА» (https://www.anti-malware.ru/news/2019-03-13-1447/29124). 13.03.2019).***

***

«Управление генерального инспектора осталось недовольным результатами проверки программы кибербезопасности NASA.

Информационная безопасность Национального управления по аэронавтике и исследованию космического пространства США оставляет желать лучшего. К такому выводу пришли специалисты Управления генерального инспектора NASA по результатам недавней проверки.

Аудиторы раскритиковали персонал NASA за «несвоевременное проведение контрольной оценки информационной безопасности». По их словам, это может свидетельствовать о «недостатке контроля и потенциальных угрозах операциям NASA, способных подорвать возможность управления защищать конфиденциальность, целостность и доступность своих данных, систем и сетей»…

Аудиторы выразили обеспокоенность по двум аспектам. Во-первых, планы NASA по обеспечению безопасности информационных систем содержат неполные и неточные данные, а во-вторых, контрольная оценка не проводится на регулярной основе.

По системе оценивания программы кибербезопасности Управления генерального инспектора, Уровень 2 означает, что «политики, процедуры и стратегии формализованы и документированы, но не всегда реализуются». В свою очередь, уровень 4 означает, что правительственное учреждение имеет «количественные и качественные показатели эффективности политик, процедур и стратегий, собираемые по всей организации и используемые для оценки и внесения необходимых коррективов»…» ***(Информационной безопасности NASA поставили «двойку» // SecurityLab.ru (https://www.securitylab.ru/news/498310.php). 12.03.2019).***

***

«Итог «российского дела» специального прокурора США Роберта Мюллера не решит главную проблему, лежащую в основе него, — угрозу злонамеренных кибератак против политических партий, корпораций и всех, кто пользуется интернетом, пишет в колонке The Washington Post Дэвид Игнатиус.

…главное беспокойство связано с американской уязвимостью перед атаками. По его словам, американское правительство до сих не может сделать многое для защиты большинства частных лиц или организаций от нападений хакеров.

Между тем, киберкомандование США и Агентство национальной безопасности уже перешли в наступление на Москву, подчеркивает автор. Во время промежуточных выборов США киберкомандование отключило доступ в интернет для российского «Агентства интернет-исследований». Позже сообщалось, что кибератаку против России одобрил президент США Дональд Трамп.

В настоящее время улучшена безопасность избирательной системы и важнейшей инфраструктуры, но защита банков, хедж-фондов, юридических организаций и других компаний ложится на их собственные плечи, добавляет автор.

Тем не менее, у итога расследования Мюллера будет собственная жизнь на Капитолийском холме, и ее невозможно предсказать. Однако конгресс должен обратить внимание на выявленную уязвимость данных перед атаками иностранных хакеров и шпионов, заключает обозреватель.» ***(Washington Post: киберкомандование США начало наступление на Москву // Goodnews.ua (http://goodnews.ua/technologies/washington-post-kiberkomandovanie-ssha-nachalo-nastuplenie-na-moskvu/). 22.03.2019).***

***

«Истребители F-35 совершенно не защищены от кибератак – к такому выводу пришли специалисты американской некоммерческой организации «Проект государственного надзора» (Project on Government Oversight, POGO).

F-35 считается самой дорогостоящей военной системой в истории, однако перед вредоносным ПО истребитель абсолютно беспомощен.

Кибербезопасность в F-35 играет чрезвычайно важную роль, поскольку его работа во многом зависит от сети автоматизированных систем, пояснили в POGO. «Из-за полностью интегрированной природы всех систем в F-35 кибербезопасность для него имеет гораздо большее значение, чем для других самолетов», – отметил специалист POGO Дэн Гразьер (Dan Grazier).

Как пояснил Гразьер, использующиеся в настоящее время устаревшие модели самолетов оснащены подсистемами, работающими на базе ПО. Хакеры могут взломать его и получить доступ к системам навигации. Тем не менее, поскольку в устаревших самолетах подсистемы не являются полностью интегрированными, злоумышленники не смогут получить доступ, скажем, к системе связи. С другой стороны, подсистемы в F-35 являются полностью интегрированными, что делает истребитель чрезвычайно уязвимым.

Взаимосвязанная природа компьютерных систем F-35 уже сама по себе является серьезной уязвимостью. Все отдельные подсистемы самолета, такие как электронные радары, система распределенной апертуры и система связи, навигации и идентификации, обмениваются данными между собой. То есть, скомпрометировав лишь одну из них, злоумышленники смогут получить доступ ко всем остальным.

«Успешная атака на одну из систем оружия может потенциально снизить его эффективность, помешать выполнению миссии и даже стать причиной физического повреждения и человеческих потерь», – отметили в POGO.» ***(Истребители F-35 уязвимы к кибератакам // Goodnews.ua (http://goodnews.ua/technologies/istrebiteli-f-35-uyazvimy-k-kiberatakam/). 31.03.2019).***

***

«В Федеральном бюро расследований (ФБР) США объявили о начале масштабных учений, цель которых – обновить базу знаний и методы противодействия киберпреступности… это крупнейшее обучение с 2001 года.

Оно охватило тысячи спецагентов. В результате обучения ожидается, что удастся провести переориентацию специалистов бюро расследований на борьбу с преступлениями в киберпространстве.

В ФБР отметили, что организовать масштабное обучение сотрудников решили по причине того, что значительно расширился спектр кибератак, которые спонсировали зарубежные противники развития американского бизнеса…

"Будущее в киберпространстве — это будущее организации, будущее мира. Мы должны думать о том, как наши специалисты разбираются в киберпространстве — будь это отдельная преступная атака коммерческого характера или нападение национального масштаба", — заявила представитель ФБР Эми Хесс.» ***(В ФБР начали масштабное обучение по борьбе с киберпреступностью // Goodnews.ua (http://goodnews.ua/technologies/v-fbr-nachali-masshtabnoe-obuchenie-po-borbe-s-kiberprestupnostyu/). 31.03.2019).***

***

«У Парижі розпочала діяльність мережа Колегії розвідки (інформації) в Європі.

У церемонії інавгурації взяв участь президент Франції Еммануель Макрон…

«Наша безпека базується на інформації. Щоб ми бути захищеними від терористичних загроз, кібератак або шпіонажу, я запропонував у вересні 2017 року створити мережу, на базі якої розвідувальні служби європейських країн могли б вести діалог», - заявив Макрон.

Метою діяльності мережі є посилення співробітництва та координації між розвідувальним органами 28 країн Євросоюзу, а також не членами Спільноти Швейцарією та Норвегією, включаючи обмін інформацією, попередження про загрози протидія іноземним спецслужбам…» ***(У Франції розпочала діяльність мережа Колегії розвідки в Європі // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (https://day.kyiv.ua/uk/news/070319-u-franciyi-rozpochala-diyalnist-merezha-kolegiyi-rozvidky-v-yevropi). 07.03.2019).***

***

«Европол в понедельник объявил о принятии нового протокола о том, как правоохранительные органы в Европейском Союзе и за его пределами будут реагировать на крупные трансграничные кибератаки…

Новый протокол ЕС по реагированию правоохранительных органов на чрезвычайные ситуации должен оказаться полезным (EU Law Enforcement Emergency Response Protocol) в случае крупных атак, таких как WannaCry и NotPetya, которые в 2017 году поразили сотни тысяч систем по всему миру и принесли значительные потери многим организациям.

Протокол, принятый Советом ЕС, является частью проекта ЕС по скоординированному реагированию на крупномасштабные трансграничные инциденты и кризисы в области кибербезопасности, и он будет реализован Европейским центром киберпреступности (EC3) Европола. Основное внимание уделяется быстрой оценке, обмену информацией и координации международных аспектов расследования.

Протокол охватывает только злонамеренные и криминальные инциденты в киберпространстве - Европол подчеркнул, что он не охватывает ситуации, вызванные стихийными бедствиями, человеческой ошибкой или сбоем системы. Его цель - дополнить существующие механизмы управления кризисами.

Протокол состоит из семи основных компонентов: раннее обнаружение и идентификация крупной кибератаки, классификация угрозы, создание координационного центра для реагирования на чрезвычайные ситуации, ранние предупреждения, план оперативных действий для правоохранительных органов, расследование инцидента и закрытие протокола аварийного реагирования…» ***(Ирина Фоменко. ЕС принял новый протокол реагирования на крупные кибератаки // Internetua (http://internetua.com/es-prinyal-novyi-protokol-reagirovaniya-na-krupnye-kiberataki). 19.03.2019).***

***

«Европейский Союз намерен призвать правительства стран-участниц к обмену информацией для управления рисками безопасности беспроводных сетей 5G… во вторник, 26 марта, ЕС опубликует рекомендации, согласно которым странам-участницам будет дано несколько месяцев на выявление и сообщение ЕС потенциальных угроз безопасности сетей 5G на их рынках. На базе этой информации будут разработаны минимальные стандарты безопасности, действительные на всей территории ЕС.

Данный шаг направлен на координацию европейского подхода к управлению киберрисками на фоне обвинений в шпионаже, выдвинутых правительством США против Huawei и других китайских технологических компаний. Следует отметить, что в настоящее время Вашингтон активно призывает своих союзников отказаться от услуг Huawei по строительству сетей 5G. Американские власти даже угрожают Германии прекратить сотрудничество в обмене разведданными, если она будет иметь дело с китайской компанией.

Тем не менее, ЕС готовит гораздо более мягкие меры, чем хотелось бы США. Европейские страны пытаются найти баланс между обеспечением кибербезопасности на фоне растущего влияния Китая и выгодным сотрудничеством со вторым крупнейшим торговым партнером на этом рынке. К примеру, Германия и Франция предлагают не отказываться от сотрудничества с Huawei, а ужесточить требования для сетей передачи данных. Еще раньше глава Секретной разведывательной службы Великобритании (MI6) Алекс Янгер (Alex Younger) отмечал маловероятность отказа от сотрудничества с китайской компанией.» ***(ЕС разработает стандарты безопасности для сетей 5G // Goodnews.ua (http://goodnews.ua/technologies/es-razrabotaet-standarty-bezopasnosti-dlya-setej-5g/). 25.03.2019).***

***

«Країни ЄС повинні будуть обмінюватися даними щодо ризиків кібербезпеки мереж 5G, а також розробити заходи для їх подолання до кінця 2019 року.

Про це заявила у вівторок Європейська комісія, пише Reuters.

Мета полягає в тому, щоб використовувати інструменти, наявні в рамках існуючих правил безпеки, а також транскордонне співробітництво.

Віце-президент Єврокомісії Андрус Ансіп заявив, що заходи, оголошені у вівторок, спрямовані на вирішення занепокоєння з приводу діяльності іноземних урядів, які використовують технологічні компанії для шпигунства.

Минулого тижня президент Франції Еммануель Макрон заявив, що Європа пробуджується щодо потенційного китайського домінування в регіоні.

Ансіп сказав, що технологія 5G принесе значні зміни в економіку і суспільство, але це не може відбутися без запровадження повної безпеки.

"Тому дуже важливо, щоб інфраструктури 5G в ЄС були стійкими і повністю захищеними від технічних або юридичних бекдорів", - сказав Ансіп.

Країни ЄС мають до кінця червня оцінити ризики кібербезпеки, пов'язані з 5G. Загальна оцінка блоку буде зроблена до 1 жовтня. За допомогою цього, країни

ЄС повинні будуть домовитися про заходи щодо пом'якшення ризиків до кінця року.

Такі заходи можуть передбачати вимоги до сертифікації та випробування продукції або постачальників, які вважаються потенційно небезпечними. ЄС вирішить до 1 жовтня 2020 року, чи слід вживати подальших заходів.

Комісія заявила, що країни ЄС самі повинні вирішувати, чи хочуть вони виключити компанії зі своїх ринків на підставах національної безпеки.» ***(Країни ЄС обмінюватимуться розвідданими щодо загроз безпеки 5G // Європейська правда (https://www.eurointegration.com.ua/news/2019/03/26/7094421/). 26.03.2019).***

***

«ANSSI підзвітний Генеральному секретаріату з питань національної оборони і безпеки (SGDSN) і сприяє французькому прем'єр-міністру в питаннях оборони і національної безпеки. Згідно зі списком досліджуваних ANSSI продуктів, з 1 червня 2018 року, були сертифіковані 122 з 261 прийнятих до розгляду продуктів.

Всі продукти, які претендують на отримання сертифікату CPSN, проходять серію випробувань в лабораторії ANSSI з тестуванням декількох сценаріїв атак, які ставлять під загрозу безпеку. Агентство оцінює «міжмережевий захист, ідентифікацію, аутентифікацію і доступ, безпеку зв'язку і вбудоване програмне забезпечення».

Ledger підкреслює важливість отримання сертифіката незалежної третьої сторони для підтвердження безпеки свого гаманця і зазначає, що CPSN для Ledger Nano S – це початок зусиль з сертифікації всіх продуктів компанії. У записі в блозі також йдеться, що Ledger проводить власну внутрішню оцінку безпеки під назвою Ledger Donjon, яка перевіряє стійкість продуктів до різних сценаріїв загроз.

Крім того, компанія розробила спеціальну операційну систему BOLOS (Blockchain Open Ledger Operating System) для об'єднання програмних і апаратних стратегій, які підвищують безпеку.» ***(Гаманець Ledger Nano S отримав сертифікат Національного агентства кібербезпеки Франції // Finance.ua (https://news.finance.ua/ua/news/-/445929/gamanets-ledger-nano-s-otrymav-sertyfikat-natsionalnogo-agentstva-kiberbezpeky-frantsiyi). 20.03.2019).***

***

Китай

«Китайская технологическая компания Huawei открыла в Брюсселе Европейский центр по кибербезопасности.

"Во вторник китайская технологическая компания Huawei открыла лабораторию по кибербезопасности в Брюсселе, сердце ЕС, в то время как компания пытается убедить правительственных лидеров и борется с американскими обвинениями, что ее оборудование представляет риск для национальной безопасности", – говорится в сообщении…

В этом Центре клиенты Huawei смогут проверять источник кодирования в сети китайской компании.

Таким образом в Huawei надеются успокоить европейских чиновников, что компания не занимается шпионажем в пользу Пекина…» ***(Huawei открыл Центр по кибербезопасности в "сердце ЕС" // «Новости онлайн 24» (https://newsonline24.com.ua/huawei-otkryl-centr-po-kiberbezopasnosti-v-serdce-es/). 05.03.2019).***

***

Інші країни

«Таїланд одностайно схвалив Закон про кібербезпеку, який дає уряду контроль над Інтернетом…

Законодавчий акт дозволяє Національному комітету кібербезпеки, який очолюють військові, «викликати осіб на допит і мати доступ до приватної власності без дозволу суду у випадку реальної або очікуваних серйозних «кібер-загроз».

Інша гілка влади тепер може, зіткнувшись з такою загрозою, шукати і вилучати дані і обладнання без ордеру.

Таїланд також схвалив Закон про захист персональних даних, який регулює всі компанії, які збирають дані фізичних осіб у країні.

Закони набудуть чинності після їх схвалення королем Таїланду.

Зазначимо, Закон про кібербезпеку жорстко розкритикували як активісти, так і підприємці, причому деякі опоненти назвали його «кібер-військовим Законом».

Директор Азіатської інтернет-коаліції Джефф Пейн заявив, що Закон «надасть режиму широкі повноваження з моніторингу онлайн-трафіку, що потенційно може ставити під загрозу конфіденційні і корпоративні дані». ***(Таїланд схвалив Закон, який надає Уряду контроль над Інтернетом // "Українське право" (http://ukrainepravo.com/news/international/tayiland-skhvalyv-zakon-yakyy-nadaye-uryadu-kontrol-nad-internetom-/). 04.03.2019).***

***

«Більше третини кібератак на Японію в 2018 році здійснювалися з території Росії і Китаю. Про це повідомило агентство Kyodo з посиланням на інформацію японської поліції.

За даними поліції, в минулому році щодня здійснювали в середньому 2 752,8 спроб несанкціонованого доступу. Атаки були підтверджені і зафіксовані системами безпеки. З території Росії проходило 20,8% кібератак, ще 14,8% — з Китаю.

Повідомляється, що в 2018 році 126 тисяч 815 осіб, постраждалих від кібератак, звернулися в поліцію. Через кіберзлочини в Японії завели більше 9 тисяч кримінальних справ…» ***(Кібератаки на Японію в 2018 році найчастіше здійснювалися з Росії і Китаю // «Дзеркало тижня. Україна» (https://dt.ua/WORLD/kiberataki-na-yaponiyu-v-2018-roci-naychastishe-zdiysnyuvalisya-z-rosiyi-i-kitayu-304904_.html). 07.03.2019).***

***

«Сумма инвестиций в израильский стартап CyberX, занимающийся кибербезопасностью, достигла 48 миллионов долларов.

Сегодня, 25 марта израильская компания объявила, что привлекла еще 18 миллионов долларов США в рамках финансирования в раунде B, который провели инвестиционные компании Qualcomm Ventures LLC и Inven Capital.

Мы считаем, что у CyberX есть подходящая управленческая команда, глубокие знания в области и масштабируемая технология для удовлетворения потребностей крупнейших и наиболее сложных предприятий в мире.

— сказал Боаз Пеер, директор Qualcomm Israel Ltd. и директор по инвестициям Qualcomm Ventures.

CyberX сообщили, что дополнительное финансирование позволит компании укрепить свои позиции на рынке, а также внедрить разработку инновационных продуктов.» ***(Израильский кибер-стартап привлек 48 миллионов долларов // Jewishnews (https://jewishnews.com.ua/economics-and-business/izrailskij-kiber-startap-privlek-48-millionov-dollarov). 25.03.2019).***

***

«Президент Венесуэлы Николас Мадуро заявил, что в стране есть внутренние силы, атакующие энергосистемы изнутри.

Он заявил, что после кибератаки система электроснабжения была восстановлена на 70%, но в полдень произошла «еще одна кибератака», вновь сломавшая систему, передает «Интерфакс».

Мадуро добавил, что вышел из строя и один из генераторов электроэнергии. Виновны в этом, по его словам, внутренние силы, «проникшие в энергетическую компанию изнутри».

«Мы ведем расследование и исправляем сбой, потому что есть много тех, кто нападает на электрическую компанию изнутри», – сказал он.

Ранее Мадуро заявил, что американские власти обладают технологиями, которые могли спровоцировать отключение электричества по всей Боливарианской Республике.» ***(Сергей Гурьянов. Мадуро заявил об атаках на энергосистему Венесуэлы изнутри // Деловая газета «Взгляд» (https://vz.ru/news/2019/3/10/967702.html). 10.03.2019).***

***

«Парламент Венесуели підтримав пропозицію опозиційного лідера Хуана Гуайдо та оголосив у країні режим надзвичайного стану через масштабне відключення електроенергії, яке триває вже шостий день.

З такою пропозицією раніше виступив лідер опозиції Хуан Гуайдо, якого більшість західних країн визнають законним президентом Венесуели…

Режим надзвичайного стану оголошено на 30 днів.

У понеділок більша частина Боліваріанської республіки залишалася без електропостчання, світло дали лише в столиці Каракасі…

Влада країни назвала причиною масштабного блекауту саботаж на ГЕС "Гурі" в штаті Болівар, яка є найбільшою у Венесуелі. Чиновники заявляли, що її робота була порушена внаслідок кібератаки. У понеділок за підозрою в організації "саботажу" було заарештовано дві людини…» ***(У Венесуелі оголосили надзвичайний стан // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (https://day.kyiv.ua/uk/news/120319-u-venesueli-ogolosyly-nadzvychaynyy-stan). 12.03.2019).***

***

«Американское правительство прямо руководило действиями, направленными на вывод из строя венесуэльской системы электроснабжения, заявил президент Боливарианской Республики Николас Мадуро.

В ходе выступления, которое транслировалось в приложении Periscope, Мадуро подчеркнул, что атака, которая привела к отключению в республике электричества, осуществлялась из двух американских городов – Хьюстон (штат Техас) и Чикаго (штат Иллинойс), передает ТАСС.

По словам президента Боливарианской Республики, за атакой стоял советник президента США по национальной безопасности Джон Болтон.

«Это была самая крупная кибератака, о которой известно на планете Земля», – приводит его слова РИА «Новости».

Мадуро также сообщил, что власти Венесуэлы решили создать военное командование по защите стратегических объектов…» ***(Ольга Никитина. Мадуро назвал блэкаут в Венесуэле терактом со стороны США // Деловая газета «Взгляд» (https://vz.ru/news/2019/3/16/968643.html). 16.03.2019).***

***

«В уряді Венесуели назвали причину чергового відключення електроенегрії на території країни.

Як повідомляє El Nacional, на енергосистему країни була здійснена кібератака.

Як сказав міністр зв'язку й інформації країни Хорхе Родрігес, ситуація із відключенням світла 25 березня 2019 аналогічна тій, яка сталась у Венесуелі вперше - 7 березня.

"Сьогоднішня атака аналогічна атаці 7 березня: вони атакували "мозок" Національної енергосистеми на гідроелектростанції імені Симона Болівара в Ель-Гурі", - сказав Родрігес.

Наразі, за словами міністра, подача електроенергії практично повністю відновлена…» ***(У Венесуелі назвали причину масових відключень світла // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (https://day.kyiv.ua/uk/news/260319-u-venesueli-nazvali-prichinu-masovih-vidklyuchen-svitla). 26.03.2019).***

***

«Тролі вже не створюють пропагандистський контент самостійно, а масово запускають фейкові акаунти

Російські інтернет-тролі змінюють свою стратегію, аби втрутитися у вибори президента США в 2020 році.

«Ми бачимо, як вони розповсюджують контент замість того, щоб просто самостійно його створювати», - заявив Джон Халтквіст, експерт американської фірми FireEye, котра спеціалізується на кібербезпеці, в інтерв'ю виданню Bloomberg, опублікованому в суботу, 9 березня.

Таким чином, контент «не обов'язково недостовірний», а отже, це створює тролям можливість «сховатися за кимось».

Хакери можуть зламувати комп'ютери і використовувати їх для створення величезної кількості фейкових акаунтів у соцмережах і керування ними, зазначив у свою чергу представник американської компанії Symantec Кандід Вуеест. За спостереженнями експерта, у 2018 році за допомогою фейкових акаунтів створювалося менше контенту, ніж роком раніше. Водночас кількість самих фейковий акаунтів стала збільшуватися. Тролі можуть використовувати цей прийом задля поширення повідомлень, що сіють розбіжності, зазначає експерт.

Соціальні мережі залишаються основним каналом закордонного впливу на американські вибори, заявив раніше директор Федерального бюро розслідувань США Крістофер Рей, виступаючи на конференції з питань кібербезпеки. За його словами, «зловмисна кампанія з іноземної експансії» лише посилюється під час виборчих циклів.» ***(Російські інтернет-тролі змінюють стратегію з втручання у вибори в США // "Українські медійні системи" (https://glavcom.ua/world/observe/rosiyski-internet-troli-zminyuyut-strategiyu-z-vtruchannya-u-vibori-v-ssha-575983.html). 10.03.2019).***

***

«…Китай здійснив кібератаки на університети в США, Канаді та країнах Південно-Східної Азії для викрадення досліджень в області військово-морських технологій…

Хакери атакували Гавайський університет, Університет штату Вашингтон, Массачусетський технологічний інститут, Університет штату Пенсильванія і інші. Більшість з них, за даними видання, так чи інакше пов'язані з Океанографічним інститутом у Вудс-Хол (штат Массачусетс), який також піддався кібератаці. У ряду цих вузів укладені контракти з ВМС США

Інформаційний підрозділ з кібербезпеки iDefense компанії Accenture Security засік у внутрішніх мережах згаданих вузів кіберактивність, витікаючу з боку серверів, розташованих на території Китаю і контрольовану групою хакерів, відомої експертам під різними назвами – Temp.Periscope, Leviathan або Mudcarp…» ***(Китай здійснив кібератаку на США, Канаду і країни Південно-Східної Азії // Рубрика (https://rubryka.com/2019/03/05/kytaj-zdijsnyv-kiberataku-na-ssha-kanadu-i-krayiny-pivdenno-shidnoyi-aziyi/). 05.03.2019).***

***

«Хакерська група Fancy Bear, пов'язана з російською військовою розвідкою, підозрюється в нападах 2015 року на сайти Центральної виборчої комісії, МВС та деяких інших інституцій Болгарії під час виборів у країні.

Про це заявив керівник відділу кібезлочинності Головної дирекції з боротьби з організованою злочинністю Болгарії Явор Колев…

"Група пов'язана з російською військовою розвідкою і підозрюється в нападах на болгарські сайти в 2015 році під час виборчого процесу, а також у маніпуляціях з виборчим процесом в США. Інша група - це представники Китайської народної армії, яких ФБР звинувачує в різних кіберзлочинах", - заявив Колев, додавши, що в більшості випадків цей вид злочинів є транскордонним.

Посольство Росії в Болгарії заперечило твердження про хакерську атаку на болгарські державні органи та втручання в місцеві вибори 2015 року, повідомляє ТАСС…» ***(Російських хакерів підозрюють в атаці на держустанови Болгарії // Європейська правда (https://www.eurointegration.com.ua/news/2019/03/12/7093824/). 12.03.2019).***

***

«Міністерство оборони Іспанії виявило ймовірну атаку на свою внутрішню комп'ютерну мережу…

"Виявлено можливе вторгнення в мережу загального призначення. Інцидент перебуває на початковому етапі розслідування. Над ним працюють Командування з кіберзахисту і Центр інформаційних та комунікаційних систем і технологій", - йдеться у повідомленні.

Уточнюється, що прокуратура країни повідомлена про те, що трапилося…» ***(Ангеліна Літінська. Міноборони Іспанії виявило сліди кібератаки на внутрішню мережу // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1785542-minoboroni-ispaniyi-viyavilo-slidi-kiberataki-na-vnutrishnyu-merezhu). 11.03.2019).***

***

«…За кражей данных британской неправительственной организации "Институт государственного управления" может быть военная разведка России…

По словам источника, эту атаку считают "значительной" потому, что если информация о причастности ГРУ подтвердится, то это будет первый случай, когда РФ совершила взлом в Великобритании.

Один из учредителей "Института государственного управления", чиновник министерства обороны Великобритании Кристофер Донелли считает, что за взломом стоит ГРУ.

Расследованием взлома занимается Национальное криминальное агентство Великобритании…» ***(СМИ сообщили, кто может стоять за взломом британской организации // Информационное агентство ЛІГАБізнесІнформ (https://news.liga.net/world/news/smi-soobschili-kto-mojet-stoyat-za-vzlomom-britanskoy-organizatsii). 07.03.2019).***

***

«Пресс-секретарь президента Дмитрий Песков оставил без комментариев заявления главы комиссии Индонезии по всеобщим выборам о якобы выявленных атаках «российских хакеров» на базу данных избирателей перед выборами 17 апреля.

«Никак не могу прокомментировать (эти сообщения). Мы неоднократно заявляли, что Россия не занималась, не занимается и не имеет никаких намерений вмешиваться в какие-то внутренние дела других государств, тем более в электоральные процессы», – сказал Песков, передает ТАСС.

«Мы не любим, когда это делают с нами, и никогда сами этим не занимаемся», – добавил пресс-секретарь…» ***(Алексей Дегтярев. Кремль отказался комментировать сообщения о «российских кибератаках» в Индонезии // Деловая газета «Взгляд» (https://vz.ru/news/2019/3/13/968144.html). 13.03.2019).***

***

«Сенаторы США требуют от парламентского пристава раскрыть детали кибератак, совершенных на Сенат и его членов. Это требование было озвучено в письме, которое подписали Рон Уайден и Том Коттон — оба являются членами комитета Сента по разведке. «Компаниям и их руководителям, согласно федеральному закону, надлежит сообщать об утечках. На этом фоне явно чувствуется контраст с Конгрессом, который освобожден от обязанности раскрывать информацию об утечках и других киберинцидентах», — гласит письмо. «Парламентский пристав должен вести полностью прозрачную политику в отношении предоставления членам Сената всей информации, касающейся кибератак на Сенат. Каждый сенатор имеет право знать были ли взломаны компьютеры Сената, и как часто они были взломаны». При этом оба сенатора отметили: они прекрасно понимают, что некоторую информацию о кибератаках важно оставлять в тайне пока идет расследование. Также некоторые данные нельзя раскрыть из соображений конфиденциальности. Тем не менее они требуют предоставлять в обязательном порядке хотя бы общую статистику по кибератакам.» ***(Олег Иванов. Сенаторы США требуют статистику и детали атак на их компьютеры // ООО «АМ-МЕДИА» (https://www.anti-malware.ru/news/2019-03-14-1447/29147). 14.03.2019).***

***

«У Празі працював великий російський центр кібератак, - про це пише чеське видання "Респект", яке провело власне розслідування.

Журналісти з'ясували, що російські спецслужби влаштовували хакерські атаки через дві комп'ютерні фірми, які начебто продавали обладнання та програмне забезпечення. Частину техніки для цих фірм привезли з Росії автівкою тамтешнього посольства з дипломатичними номерами. Зловмисників викрили ще на початку 2018 року.» ***(Ольга Торнер. У Чехії викрили кібер-центр російських спецслужб - ЗМІ // ООО "Национальные информационные системы"***

(https://podrobnosti.ua/2288866-u-cheh-vikrili-kber-tsentr-rosjskih-spetssluzhb-zm.html). 19.03.2019).

***

«Финляндия приготовилась к защите от российских интернет-троллей перед парламентскими выборами 14 апреля…

Россия стремится к разжиганию недоверия властям, усилению местных антиевропейских движений и расколу европейского единства всеми возможными способами, считает министр юстиции страны Антти Хяккянен…

По словам министра, Финляндии нужны средства быстрого реагирования, чтобы вычислять и удалять ботов в соцсетях до того, как с подозрительных аккаунтов начнется распространение дезинформирующих данных.

Финское правительство уже проводит обучение тому, как противостоять дезинформации и взлому аккаунтов. Журналистов обучают защищать свои данные и отвечать на подозрительные сообщения и угрозы. Политикам также напоминают о том, как противостоять хакерам с помощью двухфазной аутентификации, сложных паролей и обновлении программного обеспечения компьютера.

В то же время отмечается, что пока подозрительной киберактивности в финском интернете зафиксировано не было, а президентские выборы в 2018 году прошли без эксцессов.» ***(Финляндия приготовилась к предвыборной кибератаке россиян // DsNews (http://www.dsnews.ua/world/finlyandiya-prigotovilas-k-predvybornoy-kiberatake-rossiyan-28032019121900). 28.03.2019).***

***

Захист персональних даних

«Витоки приватних даних уже псують життя людям, але вони не квапляться посилювати своє ставлення до кібербезпеки. Нове дослідження лабораторії Malwarebytes Labs показує розбіжність у сприйнятті власної безпеки та практик, які вони використовують для втілення цієї безпеки у реальність.

Експерти Malwarebytes опитали понад 4000 користувачів. Вони з'ясували, що люди турбуються про свої приватні дані, і не довіряють компаніям у тому, що вони здатні вберегти їхню інформацію. При цьому в реальності більшість користувачів самі не хочуть особливо перейматися кібербезпекою, воліючи використовувати швидкі, але часто не дієві практики та відкидаючи надійні, але складні для їхнього сприйняття дії.

Опитування показує, що 96 респондентів усіх поколінь турбуються про свою приватність, а 93% – використовують програмне забезпечення для підвищення безпеки. Однак при цьому лише 32% читають угоди користування (EULA), тільки 47% знають, які дозволи мають їхні додатки, та тільки 53% використовують менеджери паролів.

Загалом 29% опитаних визнають використання одного пароля на багатьох сайтах. Більшість респондентів (87%) також кажуть, що вони не впевнені у безпеці своїх приватних даних в онлайні.

Коли респондентів запитали, наскільки сильно вони довіряють тому, що соцмережі можуть захистити їхні дані, середнє значення склало 0,6 бала з 5 максимальних.

Автори дослідження підсумовують, що за останні роки було багато випадків, коли надмірна впевненість у захищеності даних призводила до важких наслідків. Але, відзначають вони, люди все одно не хочуть змінювати свої звички.» ***(Євген Корольов. Інтернет-користувачі надмірно впевнені у своїй захищеності // Tech Today (https://techtoday.in.ua/news/internet-koristuvachi-nadmirno-vpevneni-u-svoyiy-zahishhenosti-111220.html). 05.03.2019).***

***

«Эксперт по кибербезопасности из Нидерландов Виктор Геверс обнаружил базу данных с открытым кодом, в которой находится переписка 364 млн жителей Китая…

Постоянно обновляющаяся база данных с перепиской 364 млн жителей Китая в шести самых популярных в стране мессенджерах — с паспортными данными и текущими контактами — хранится на 18 серверах. Для получения доступа к ним необходимо знать всего лишь адрес, который хранится в открытом коде.

Эти данные автоматически отправляются в полицейские участки, в которых в ручном режиме просматриваются около 3 тыс. приоритетных. Алгоритм автоматически — по ключевым словам — ищет необходимые слова в сообщениях и маркирует их как особо важные…» ***(В открытом доступе оказалась переписка 364 млн жителей Китая // Goodnews.ua (http://goodnews.ua/technologies/v-otkrytom-dostupe-okazalas-perepiska-364-mln-zhitelej-kitaya/). 05.03.2019).***

***

«Facebook зберігав мільйони паролів користувачів соціальної мережі у відкритому доступі для своїх співробітників протягом багатьох років. Про це компанія заявила в четвер після того, як дослідник безпеки написав в Інтернеті про цю проблему…

Зберігаючи паролі в читабельному текстовому форматі, Facebook порушив основні практики комп'ютерної безпеки. Вони вимагають, щоб організації та веб-сайти зберігали паролі в зашифрованій формі, що не дозволяє відновити оригінальний текст…

Facebook заявив, що немає доказів, що його співробітники зловживали доступом до цих даних. Але тисячі співробітників могли їх шукати. Компанія заявила, що паролі зберігаються на внутрішніх серверах компанії, де жоден сторонній користувач не має доступу до них.

Інцидент виявляє ще один величезний недогляд у компанії, яка наполягає, що вона відповідально стоїть на варті особистих даних своїх 2,2 мільярда користувачів по всьому світу.

У блозі з безпеки KrebsOnSecurity сказано, що Facebook міг залишити паролі близько 600 мільйонів користувачів Facebook уразливими. У дописі в блозі Facebook повідомив, що він, ймовірно, повідомить “сотні мільйонів” користувачів Facebook Lite (легка версія сайту), мільйони користувачів Facebook і десятки тисяч користувачів Instagram, що їхні паролі зберігаються у звичайному тексті.» ***(Ілля Нежигай. Facebook зберігав мільйони паролів користувачів у відкритому для своїх співробітників доступі // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1788009-facebook-zberigav-milyoni-paroliv-koristuvachiv-u-vidkritomu-dlya-svoyikh-spivrobitnikiv-dostupi). 22.03.2019).***

***

«Взломщик Gnosticplayers, который ранее уже трижды выставлял на продажу базы персональной информации, предложил покупателям новую порцию данных. С учетом этой подборки объем скомпрометированных злоумышленником файлов приблизился к 866 млн, а список жертв насчитывает 32 организации.

Выставленные на черный рынок базы содержат более 26 млн записей, за которые преступник хочет получить около $5000 в биткойнах. В число пострадавших вошли шесть компаний, предлагающих различные программные продукты:

Bukalapak (13 млн записей оцениваются в 0,34 BTC) — индонезийский агрегатор интернет-магазинов;

Estante Virtual (5,45 млн записей, 0,2618 BTC) — бразильский книжный интернет-магазин;

LifeBear (3,86 млн записей, 0,2618 BTC) — японское приложение для ведения расписания;

Coubic (1,5 млн записей, 0,157 BTC) — онлайн-календарь;

Gamesalad (1,5 млн записей, 0,0785 BTC) — платформа-конструктор для разработчиков игр;

YouthManual.com (1,12 млн записей, 0,144 BTC) — индонезийский портал для студентов с вакансиями начального уровня.

В этих базах есть электронные адреса, хешированные пароли, IP-адреса и прочие данные, связанные с деятельностью компаний, — например, персональные увлечения пользователей YouthManual или подробности о покупках, совершенных через Bukalapak. Четыре из пяти баз были похищены в феврале 2019 года, а Bukalapak взломали еще в 2017 году.

Журналисты отмечают, что некоторые из предыдущих жертв Gnosticplayers ранее действительно объявляли об утечках. Это позволяет предположить, что выставленные на продажу данные реальны. Из шести компаний, которые попали в нынешнюю серию, к настоящему моменту комментарии поступили только от Coubic и LifeBear — они сообщили об идущем расследовании возможного взлома.

Сам Gnosticplayers объясняет свои действия желанием наказать организации за пренебрежение безопасностью. По его словам, все опубликованные пароли можно взломать, поскольку компании не применяют сильные алгоритмы

шифрования…» ***(Egor Nashilov. Взломщик выложил данные шести компаний в назидание другим // Threatpost (https://threatpost.ru/gnosticplayers-goes-for-round-4-with-six-companies-data/31911/). 19.03.2019).***

***

«Компания InfoWatch представляет основные данные по утечкам конфиденциальной информации из учреждений здравоохранения в 2018 г.

В 2018 г. аналитический центр компании InfoWatch зарегистрировал 429 утечек из различных учреждений медицинской сферы по всему миру: больницы, поликлиники, военные госпитали, лаборатории, аптеки, медицинское страхование и т.д. Это почти на 16% больше, чем в 2017 г. Число скомпрометированных записей персональных данных по сравнению с 2017 г. выросло почти вдвое и составило 27 млн.

Более 80% записей ПДн утекло в результате внешнего воздействия. Так, в начале 2018 г. киберпреступники атаковали информационную систему Юго-Восточной медицинской службы Норвегии. Украдены данные около 3 млн человек, то есть примерно половины жителей этой скандинавской страны. В норвежском управлении по информационной безопасности не исключают, что хакеры действовали по заказу иностранного государства.

Каждая третья утечка в прошлом году произошла в результате хакерских атак. Но основными виновниками утечек в данной отрасли остаются сотрудники. На их долю приходится 53,7% зарегистрированных инцидентов. Например, в Канаде бывший сотрудник сети Alberta Health Systems незаконно получил доступ к защищенным медицинским данным порядка 13 тыс. пациентов.

Соотношение умышленных и случайных утечек в медицине составило 47,5% и 52,5%. При этом среди утечек, совершенных по вине сотрудников, доля умышленных инцидентов составляет немногим более 20%. В основном данные ограниченного доступа компрометируются в результате ошибок, недосмотра, халатности. В США данные более 200 тыс. пациентов были оставлены на незащищенном FTP-сервере. Виновником утечки названа компания MedEvolve – поставщик управленческого ПО для медучреждений.

Доля персональных данных в утечках по сравнению с 2017 г. сократилась с 90,2% до 84,4%. При этом в 2018 г. выросла доля утечек платежной информации – с 8,6% до 13,5%. Это может быть связано с развитием коммерческой медицины и новых форм оплаты. В американском штате Сент-Луис медсестра из дома престарелых в личных интересах использовала данные банковских карт своих пациентов. На деньги стариков женщина покупала одежду и другие вещи для своей семьи.

Более 45% утечек в 2018 г. случились через сетевой канал. Далее располагаются электронная почта (21,1%) и бумажные документы (20,2%). В Великобритании аптечная сеть Well Pharmacy в результате ошибочной рассылки по e-mail скомпрометировала личные данные более 24 тыс. сотрудников и местных жителей. Утекла такая информация, как имена, адреса, номера телефонов, адреса электронной почты, данные о заработной плате.» ***(Число утечек из медицинских учреждений выросло на 16% // ООО "ИКС-МЕДИА"***

(http://www.iksmedia.ru/news/5571321-Chislo-utechek-iz-medicinskix-uchre.html). 18.03.2019).

***

«Нещодавно у сімейному застосунку Family Locator виявили збій. Застосунок розробила австралійська компанія React Apps. Завдяки йому, члени сім'ї можуть відстежувати один одного в режимі реального часу. Батькам програма надсилає повідомлення в той час, коли дитина залишає певну геозону. В результаті проблеми, інформація про місцезнаходження користувачів та інші особисті дані витекли в мережу і опинилися у відкритому доступі.

Витік виявив фахівець з кібербезпеки Саньям Джейн і повідомив про неї сайту TechCrunch. За його словами, внутрішня база даних стала загальнодоступною. В результаті збою з'явилася можливість роздобути облікові записи 238 тис користувачів. В них містяться такі особисті дані, як ім'я користувача, фотографії, адреса електронної пошти та незашифрований пароль. У базі, крім іншого, зберігалася інформація про місцезнаходження людей в режимі реального часу.

Family Locator насправді залишає всі ці дані незахищеними, оскільки застосунок працює з серверами, які не володіють достатнім рівнем шифрування. Повідомляється, що проблеми не вирішували до тих пір, поки керівництво TechCrunch не звернулася до Microsoft з проханням зв'язатися з розробниками, які як і раніше ніяк не прокоментували витік даних. Доступ до бази був закритий.» ***(Дейнека Анастасія. Family Locator порушував конфіденційність користувачів // Pingvin.pro (https://pingvin.pro/gadgets/news-gadgets/family-locator-porushuvav-konfidentsijnist.html). 25.03.2019).***

***

«…Представители японского автопроизводителя Toyota Motor Corp в Японии рассказали о возможной масштабной утечке персональных данных. Об этом сообщили в пресс-релизе компании.

Злоумышленники могли взломать систему компании в ряде торговых подразделений и пяти компаниях на территории Японии. Они, предварительно, заполучили до 3,1 миллиона наименований персональной информации.

«Персональная информация, утечка которой могла произойти, не касается информации по кредитным картам», — сообщили в пресс-службе.

Систему взломали 21 марта.

Руководство Toyota Motor пообещало предпринять все меры, необходимые для обеспечения сохранности информации у своих дилеров и внутри всей корпорации…

Компания всерьез обеспокоилась этой ситуацией. Поэтому руководство пообещало клиентам внедрить меры информационной безопасности в дилерские центры и все отделения Toyota Group.

Незадолго до этого, 19 февраля, австралийские дилеры Toyota также подверглись кибератаке. Из-за действия хакеров отказали многие корпоративные IT-системы.

Эксперты по безопасности подозревают, что за атаками на дочерние и дилерские компании Toyota стоит хакерская группа APT32, еще известная как OceanLotus и Cobalt Kitty. Ее поддерживает Вьетнам. А все эти взломы — часть крупномасштабной скоординированной операции.» ***(Миллионы клиентов Toyota стали жертвами хакеров // Goodnews.ua (http://goodnews.ua/technologies/milliony-klientov-toyota-stali-zhertvami-xakerov/). 31.03.2019).***

***

«Ежедневно интернет-пользователи генерируют эксабайты данных: поисковые запросы и почтовые сервисы, мобильные банкинги, видео- и фотохостинги, чаты в социальных сетях. В результате каждый оставляет цифровой след, а вдобавок и цифровую тень.

О том, какое это имеет последствие для бизнеса и рядовых пользователей, рассказывает Алексей Смирнов, менеджер по развитию бизнеса Orange Business Services.

Цифровой след

Из двух терминов – цифровой след и цифровая тень – чаще всего пользователи знают только первый.

Под цифровым следом понимают все создаваемые юзером данные, которые так или иначе остаются в цифровом пространстве. Процесс создания, распространения и использования таких данных можно контролировать – полностью или частично.

Каждое устройство оставляет след вне зависимости от того, подключено оно к сети постоянно или только время от времени. К примеру, некоторые компании для сбора маркетинговой информации устанавливают в торговых точках или местах большого скопления людей специальные датчики, которые отслеживают активные Wi-Fi- и Bluetooth-модули смартфонов прохожих и записывают MAC-адреса устройств…

Цифровая тень – менее известный термин, который тоже означает данные пользователя в цифровой среде.

Разница со «следом» состоит в том, что теневые отпечатки юзер никак не контролирует. Часто он даже не знает, что вообще где-то оставил информацию о себе.

Пример – попадание в поле зрения камеры наблюдения…

Яркий пример цифровой тени и связанных с ней последствий – попадание женщины с бойфрендом в объективы камер автомобилей Google, а после – размещение фотографии этой пары на Google Maps…

Избавиться от цифровой тени практически невозможно. Остается лишь минимизировать риски и делать все возможное, чтобы даже часть следа не была использована злоумышленниками…

Сама по себе эта информация не представляет значительного интереса, но вкупе с предиктивной аналитикой система сможет предсказать местонахождение человека в определенное время, ориентируясь на его паттерны поведения и любимые локации.

В некоторых странах сбор персональных данных граждан поставлен на поток. В Китае, например, имеется несколько различных систем видеонаблюдения.

В рамках одной из них, Skynet Project, установлено более 20 миллионов камер. К 2020 году к этому числу планируется добавить еще несколько сотен миллионов устройств. Граждан идентифицируют на улице – например, для того, чтобы наказать за нарушение правил дорожного движения.

В ряде регионов Поднебесной и цифровой отпечаток, и цифровая тень гражданина значат гораздо больше, чем в любой другой стране…

Существует три сценария использования собранной о пользователях информации:

коммерческий,

государственный,

преступный…

Резюмируя, необходимо подчеркнуть, что сбор пользовательских данных сам по себе не несет негатива, если происходит без нарушения прав граждан.

Главное – необходимо понимать, кто и как планирует впоследствии использовать полученную информацию. Чем «умнее» будут становиться устройства, дома и целые города, тем больше данных будет неминуемо агрегироваться и впоследствии собираться.

Не надо бояться этого процесса, главное – не оставляйте информацию, знание которой может стать оружием против частного лица или компании. Используйте принципы «сетевой гигиены» и анализируйте свои действия, особенно в публичных сетях – это позволит минимизировать риски.» ***(Алексей Смирнов . Новая реальность: какие угрозы несет сбор пользовательских даннях // Rusbase (https://rb.ru/opinion/sbor-dannyh/). 29.03.2019).***

***

Кіберзлочинність та кібертерроризм

«Історія із загубленим у барі прототипом iPhone 4 для більшості користувачів залишилася цікавим маркетинговим трюком. Але для хакерів втрачені інженерні прототипи є дуже цінними гаджетами. Усе тому, що з їхньою допомогою вони можуть проникнути глибше в захист Apple.

Сьогодні прототипи смартфонів Apple є дуже цінним товаром – подібний гаджет можна продати за $1800. Причина в тому, що в таких пристроях Apple не використовує свою систему захисту на повну потужність. Наприклад, завдяки цьому вдалося дослідити вбудований у iPhone процесор Secure Enclave Processor (SEP). У комерційних зразках він активний, і його шифрування важко зламати. Але дослідити роботу SEP вдалося за допомогою тестового прототипа iPhone. Ці прототипи мають активні права розробника, що дозволяє на них робити більше, ніж дозволено звичайному користувачеві.

Рідкісні прототипи iPhones допомагають хакерам з меншими зусиллями шукати суттєві вразливості в смартфонах Apple. Знайдені діри можна потім перепродати дослідникам з кібербезпеки чи іншим хакерам за десятки тисяч

доларів. Наприклад, саме так фірма Cellebrite розробила пристрої, які «ламають» iPhone.

Хакери кажуть, що хоча інженерні прототипи iPhone є рідкісними, зацікавленій людині, яка має достатню суму грошей, нескладно стати власником одного з них. Наприклад, інженерний варіант iPhone X продають за $1800.» ***(Євген Корольов. Прототипи iPhone допомагають хакерам ламати захист Apple // Tech Today (https://techtoday.in.ua/news/prototypy-iphone-dopomagayut-hakeram-lamaty-zahyst-apple-111441.html). 11.03.2019).***

***

«Число фішингових атак в останні місяці зросло більш ніж удвічі. При цьому один із 61 листа, що надходять на корпоративні поштові скриньки, містить шкідливу URL-адресу…

Аналіз, проведений фахівцями з безпеки в Mimecast показав, що в період з серпня по листопад і з грудня по лютий кількість відправлених електронних листів із шкідливими URL-адресами збільшилася на 126%.

Ці шкідливі посилання є одним з ключових методів, використовуваних кіберзлочинцями для проведення злочинних кампаній: шляхом поширення фішингових листів, які спонукають користувачів переходити по посиланню…

В цілому фахівці проаналізували 28 407 664 електронних листів, доставлених в корпоративні поштові скриньки, які були визнані "безпечними" автоматичними системами безпеки, і з'ясували, що 463 546 з них містили шкідливі URL-адреси. Тобто, кожне 61 повідомлення несе в собі потенційну небезпеку користувачам…» ***(Кожне 61 повідомлення у поштовій скринці містить шкідливе посилання. Чим це загрожує // Espreso.tv (https://espreso.tv/news/2019/03/05/kozhne_61_povidomlennya_u_poshtoviy_skrynci_mistyt_shkidlyve_posylannya_chym_ce_zagrozhuye). 05.03.2019).***

***

«Через соцсеть для бизнеса LinkedIn киберпреступники высылают потенциальным жертвам фейковые предложения о работе и ссылки на подставные ресурсы, при переходе на которые на целевой компьютер загружаются вредоносные программы…

По словам исследователей компании Proofpoint, специализирующейся на кибербезопасности, цель хакеров — внедрить на скомпрометированный компьютер бэкдор More_eggs, который позволяет атакующему удалённо развёртывать на нём другое вредоносное ПО.

Хакеры создают профили в LinkedIn и отправляют жертве небольшое сообщение с предложением вакансии. Спустя несколько дней злоумышленники уже на рабочую почту, указанную в соцсети, высылают email, в котором получателю предлагается перейти на определённый веб-сайт за дальнейшими деталями о вакансии.

URL-адреса ведут на подставные страницы, замаскированные под легитимные компании по подбору персонала. После открытия сайт начинает скачивать зловредный Word-документ с маросом, который активирует загрузку

бэкдора More_eggs. Иногда URL ведут на PDF-файлы с фальшивой информацией о работе и вредоносными ссылками. Атаки могут быть более изощрёнными и использовать краткие ссылки, вредоносные вложения в письмах, защищённые паролями Word-документы и даже просто невинные email-ы без вложений или ссылок с попыткой установить…» ***(Хакеры высылают фейковые предложения о работе в LinkedIn // Goodnews.ua (http://goodnews.ua/technologies/xakery-vysylayut-fejkovye-predlozheniya-o-rabote-v-linkedin/). 02.03.2019).***

***

«…Несколько дней назад злоумышленники провели DNS-атаку на ряд крупных российских ресурсов, одним из них является «Яндекс»… Для этого использовалась уязвимость в действующей в России системе блокировки сайтов, которую контролирует Роскомнадзор. В ходе атаки злоумышленник, владеющий доменом из реестра запрещенных сайтов, может связать его с IP-адресом любого другого сайта и добиться его блокировки.

Об уязвимости в системе блокировки сайтов Роскомнадзора стало известно в 2017 году, когда злоумышленники с ее помощью на протяжении нескольких дней периодически блокировали доступ к сайтам крупных российских банков. Участники рынка говорят, что за два года Роскомнадзор так и не устранил уязвимость. В «Яндексе», напротив, утверждают, что Роскомнадзор уже выработал несколько инструментов защиты компаний, в том числе «Яндекса»: ведомство предложило применять белые списки сайтов, которые ни при каких обстоятельствах нельзя блокировать.

Кто устроил атаку, неизвестно. Собеседники издания обращают внимание на то, что нападение совпало по времени с митингом против изоляции Рунета 10 марта.» ***(Уязвимость в реестре Роскомнадзора позволила атаковать «Яндекс» // «Открытые системы» (https://www.computerworld.ru/news/Uyazvimost-v-reestre-Roskomnadzora-pozvolil-atakovat-Yandex). 14.03.2019).***

***

«Специалисты ИБ-компании Proofpoint сообщили о массовых атаках на корпоративных пользователей облачных сервисов Office 365 и G Suite. Злоумышленники обходят двухфакторную аутентификацию и получают доступ к учетным записям через незащищенный протокол IMAP. За шесть месяцев они проникли в отслеживаемые экспертами аккаунты более 100 тыс. раз.

По мнению специалистов, обеспечить должную степень безопасности разработчикам мешают устаревшие протоколы. Двухфакторная аутентификация не позволяет защитить аккаунты в Office 365 и G Suite в нужной мере, поскольку общие и сервисные почтовые ящики арендаторов остаются уязвимыми. Доступ к ним злоумышленники получают в ходе кампаний типа password-spraying через протокол IMAP, когда учетные записи взламывают посредством перебора часто используемых паролей либо используют базы, составленные по результатам фишинга, взломов и утечек.

По данным специалистов, в период с сентября 2018 года по февраль 2019-го мошенники использовали IMAP-атаки для угона аккаунтов руководителей и

административного персонала. Помимо прочего, после захвата профилей они распространяли вредоносное ПО во внутренних сетях, меняли правила переадресации email-сообщений, рассылали фишинговые письма в другие организации, а также использовали доступ к корпоративной инфраструктуре для поиска конфиденциальной информации, пригодной для продажи, или перенаправления зарплат и платежей на свои счета.

Проанализировав миллионы профилей, исследователи установили:

72% арендаторов облачных сервисов подвергались по меньшей мере одной атаке.

В средах 40% клиентов G Suite и Office 365 обнаружилась хотя бы одна взломанная учетная запись.

В среднем из 10 тыс. активных аккаунтов злоумышленникам удавалось захватить 15.

За последние полгода атакам через IMAP подверглись 60% арендаторов G Suite и Office 365. В каждом четвертом случае злоумышленники успешно проникали в корпоративные среды…» ***(Egor Nashilov. Взломщики похищают аккаунты Office 365 и G Suite через IMAP // Threatpost (https://threatpost.ru/office-365-and-g-suite-tenants-attacked-through-imap/31880/). 17.03.2019).***

***

«Кібератака на одного з найбільших у світі виробників алюмінію, компанію Norsk Hydro, розпочалася у понеділок увечері і посилилася протягом ночі.

Про це заявило у вівторок норвезьке державне агентство, відповідальне за кібербезпеку…

"Ми допомагаємо Norsk Hydro у вирішенні ситуації, обмінюючись цією інформацією з іншими секторами в Норвегії та з нашими міжнародними партнерами", - заявила прес-секретар Норвезького органу національної безпеки (NSM).

Вона сказала, що обсяг збитків все ще оцінюють, і відмовилася коментувати тип атаки.

Кібератака призвела до збоїв у роботі компанії в Європі і США, пише Bloomberg. Частину робочих процесів на виробництві перевели в ручний режим, деякі інші процеси взагалі призупинили, розповів прес-секретар Norsk Hydro Халвор Молланд…» ***(Норвезький алюмінієвий гігант Norsk Hydro зазнав кібератаки // Європейська правда (https://www.eurointegration.com.ua/news/2019/03/19/7094128/). 19.03.2019).***

***

«По данным NETSCOUT Systems, в 2016 году на облачные сервисы пришлось 25% DDoS-атак, в 2017-м — 33%, в 2018-м — 47%. Рост внимания дидосеров к облачным услугам эксперты подразделения ASERT/Arbor объясняют расширением использования цифровых технологий, способных повысить эффективность деловых операций.

Согласно итогам опроса, ежегодно проводимого среди пользователей продуктов компании, за год доля SaaS-сервисов (ПО как услуга) как мишени дидосеров возросла с 13 до 41%, сторонних ЦОД и облачной обработки данных — с 11 до 34%.

Растет также число DDoS-атак, обусловленных политическими мотивами. В 2018 году с такой формой протеста столкнулись 60% участников опроса — против 37% годом ранее.

Анализ данных, собранных за год на платформе ATLAS (в настоящее время мониторит около трети интернет-трафика) показал, что общее количество DDoS-инцидентов в прошлом году уменьшилось — 6,13 млн против 7,5 млн в 2017-м. В то же время мощность атак возросла почти в 2,5 раза, с 270,6 до 600 Гбит/с — и это не предел для дидосеров, как показала февральская DDoS с memcached-плечом, достигшая отметки 1,7 Тбит/с.

Подобные потоки способны обрушить любой сайт — 91% респондентов, переживших DDoS в 2018 году, подчеркнули, что в ходе атаки пропускная способность интернет-каналов предприятия была полностью исчерпана.

Исследователи также отметили, что по мере расширения использования облачных услуг по защите от DDoS злоумышленники начали проводить проверку наличия такой обороны. Согласно статистике NETSCOUT, за год доля атак на межсетевые экраны и системы предотвращения вторжений (к сожалению, на них все еще уповают некоторые бизнес-структуры) возросла почти в 2 раза, с 16 до 31%. При этом 43% пострадавших отметили, что отказ традиционного средства защиты в результате атаки увеличил время простоя, грозящего снижением дохода.

Сложные, многовекторные DDoS-атаки, судя по результатам опроса, пока сохраняют актуальность: с подобными инцидентами столкнулись 36% компаний.

В рамках годового отчета специалисты NETSCOUT впервые провели также целевой опрос руководителей корпоративных ИБ- и IT-служб в семи странах: США, Канаде, Бразилии, Великобритании, Франции, Германии и Японии. Результаты показали, что за год предпочтения дидосеров изменились в пользу Азиатско-Тихоокеанского региона (2,3 млн атак), тогда как ранее их больше привлекали страны EMEA. Рост DDoS-активности наблюдался также в Латинской Америке (на 14%, до 41 938 атак ежемесячно).

В прошлом году каждый час простоя из-за DDoS в среднем обходился предприятиям названных стран в 221 837 долларов. В Германии эта сумма оказалась самой высокой (почти $352 тыс.), в Японии — самой низкой (немногим более $123 тыс.).

Основным вызовом, связанным с DDoS-атаками, половина респондентов назвала нехватку специалистов по защите, которых трудно не только заполучить, но и удержать.» ***(Maxim Zaitsev. Эксперты фиксируют рост числа DDoS-атак на облачных сервисах // Threatpost (https://threatpost.ru/netscout-reports-ddos-attacks-increasingly-targeting-cloud-services-in-2018/31971/). 25.03.2019).***

***

«Специалисты Trend Micro выявили фишинговую кампанию, направленную на похищение учетных данных посетителей нескольких южнокорейских сайтов.

Злоумышленники внедрили скрипт, загружающий фальшивую форму авторизации, на главные страницы скомпрометированных ресурсов, что позволило им проводить атаки по методу «водопоя» (watering hole). Эксперты предполагают, что вредоносное ПО, которое используют киберпреступники, пока находится в стадии тестирования и отладки.

Вредоносный штамм, получивший кодовое название Soula, был найден на четырех южнокорейских сайтах, один из которых входит в число самых посещаемых бизнес-ресурсов в стране. Как выяснили специалисты, главные страницы всех онлайн-площадок содержали JavaScript-сценарий, который загружал со стороннего сервера фишинговый скрипт и поддельную страницу регистрации. Зловред анализировал HTTP-заголовки передаваемых пакетов, чтобы отсеять боты и определить тип устройства остальных посетителей — им он выводил соответствующую форму для ввода учетных данных.

Зловред не проявлял активности до тех пор, пока жертва не заходила на скомпрометированный сайт шестой раз, после чего предлагал ей «авторизоваться». Введенные в фишинговом окне логин и пароль отправлялись киберпреступникам без какой-либо проверки корректности данных. По мнению ИБ-специалистов, это свидетельствует о том, что злоумышленники еще настраивают и дорабатывают свое программное обеспечение, и в дальнейшем можно ожидать новых атак.

Код Soula содержит комментарии на китайском языке, что позволяет сделать вывод о национальной принадлежности автора зловреда. Как выяснили эксперты, злоумышленники использовали CDN-сеть Cloudflare, чтобы скрыть домен и реальный IP-адрес своего сервера. Узнав о злоупотреблении, операторы сети доставки контента заблокировали аккаунт фишеров, однако инициаторы атак watering-hole перенесли свои скрипты и страницы на другой сервер — на сей раз взломанный…» ***(Maxim Zaitsev. Фишеры поджидают жертв у «водопоя» // Threatpost (https://threatpost.ru/phishers-use-watering-hole-attack-to-steal-website-credentials/32048/). 29.03.2019).***

***

Діяльність хакерів та хакерські угруповування

«Хакери з Північної Кореї в період з 2017 по 2018 рік в обхід санкцій здійснювали кібератаки на зарубіжні фінансові установи і криптовалютні біржі.

Про це повідомляє Nikkei з посиланням на звіт, схвалений членами Ради Безпеки ООН для публікації на наступному тижні…

«Північна Корея проводила кібератаки на зарубіжні фінансові установи з 2015 по 2018 рік», - йдеться в повідомленні.

Відповідно до щорічного звіту групи експертів РБ ООН з санкцій щодо Північної Кореї, Пхеньян накопичив близько 670 мільйонів доларів в іноземній і

віртуальній валюті за допомогою кібер-крадіжок. Щоб обійти режим санкцій і приховати свої сліди, північнокорейські хакери використовували технологію блокчейна.

Як зазначає видання, інформацію про те, як саме Північна Корея отримує іноземну валюту за допомогою кібератак, експерти надали вперше з початку режиму санкції.

Експерти рекомендували державам-членам Альянсу «розширити свої можливості щодо сприяння активному обміну інформацією про кібератаки з боку КНДР» для виявлення і запобігання спробам Північної Кореї ухилятися від санкцій…» ***(Хакери з КНДР за два роки викрали $ 670 мільйонів, - ЗМІ // Західна інформаційна корпорація (https://zik.ua/news/2019/03/09/hakery_z_kndr_za_dva_roky_vykraly__670_milyoniv__zmi_1525669). 09.03.2019).***

***

«Американська компанія Microsoft виявила, що за останні два роки були здійснені кібератаки, пов'язані з іранськими хакерами, на тисячі співробітників понад 200 світових компаній…

"Microsoft виявив, що за останні два роки були здійснені кібератаки, пов'язані з іранськими хакерами, на тисячі співробітників понад 200 світових компаній", - йдеться у повідомленні.

У Microsoft пояснили, що хакери, з групи Holmium (інша назва APT33), надіслали 2300 особам фішингові листи, які можуть самостійно встановлювати шкідливі коди на комп'ютерах.

За даними WSJ, таким чином хакери викрали конфіденційні дані компаній та видаляли дані з самих комп'ютерів співробітників.

У Microsoft також заявили, що кібератаки були здійснені на нафтогазові компанії, та виробників важкої техніки в декількох країнах, включаючи Саудівську Аравію, Велику Британію, Індію та США.

Своїми діями хакери завдали збитків на сотні мільйонів доларів США.

Представництво Ірану в ООН ще не прокоментувало новину.» ***(Microsoft виявив атаки іранських хакерів на понад 200 компаній // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (https://day.kyiv.ua/uk/news/070319-microsoft-vyyavyv-ataky-iranskyh-hakeriv-na-ponad-200-kompaniy). 07.03.2019).***

***

«Северокорейские хакеры стали одной из ключевых угроз кибербезопасности Соединенных Штатов, заявил помощник генпрокурора США по нацбезопасности Джон Демерс…

В числе их первоочередных целей — американские банки, рассказал он.

«Кибератаки с кражей средств — это значительная часть того, чем они занимаются в киберпространстве», — сообщил Демерс. Это отличает их от прочих стран, таких как Иран, Китай и Россия, которые в большей степени заинтересованы в шпионаже.

Целью КНДР становятся не только американские банки. Как установили следователи ФБР, в 2016 году именно северокорейские хакеры стояли за кибератакой на Центральный банк Бангладеш.

По мнению опрошенных CNN экспертов, это связано с попытками Пхеньяна добыть деньги на фоне жестких санкций, ухудшивших финансовое положение страны.

Демерс подтверждает эту точку зрения.» ***(Хакеры из КНДР атаковали американские банки // "УКРОП" (Україна: Об'єктивний погляд) (http://укроп.org/%d1%85%d0%b0%d0%ba%d0%b5%d1%80%d1%8b-%d0%b8%d0%b7-%d0%ba%d0%bd%d0%b4%d1%80-%d0%b0%d1%82%d0%b0%d0%ba%d0%be%d0%b2%d0%b0%d0%bb%d0%b8-%d0%b0%d0%bc%d0%b5%d1%80%d0%b8%d0%ba%d0%b0%d0%bd%d1%81%d0%ba%d0%b8/). 02.03.2019).***

***

«…Компания Citrix сообщает о взломе своей внутрикорпоративной сети неизвестной группой хакеров. 6 марта, говорится в заявлении, компания получила уведомление от ФБР, после чего были немедленно предприняты действия для нейтрализации угрозы. Помощь Citrix оказывают специалисты одной из ведущих фирм в области компьютерной безопасности, а также сотрудники ФБР.

Для первоначального проникновения в сеть злоумышленники, по всей видимости, использовали подбор ненадежных паролей. После получения определенного уровня доступа они смогли с помощью других методов обойти остальные средства защиты. Возможно, что в итоге им удалось получить доступ к корпоративной документации, говорится в заявлении, но какие именно документы оказались у злоумышленников, пока сказать трудно. Не найдено пока также признаков того, что в результате взлома может пострадать безопасность продуктов или сервисов Citrix, подчеркивают в компании. Расследование происшествия еще не закончено, и в компании обещают публиковать новые сообщения по мере поступления информации.» ***(Хакеры пробрались во внутреннюю сеть Citrix // «Открытые системы» (https://www.computerworld.ru/news/Hakery-probralis-vo-vnutrennyuyu-set-Citrix). 13.03.2019).***

***

«Будучи подростком, Бето О'Рурк состоял в старейшей группе компьютерных хакеров в истории США…

Чрезвычайно влиятельная Cult of the Dead Cow (CDC, Культ Мертвой Коровы), в шутку названная в честь заброшенной бойни в Техасе, печально известна тем, что выпускает инструменты, позволяющие обычным людям взламывать компьютеры под управлением Microsoft Windows. Группа хакеров также известна благодаря изобретению слова "хактивизм" для описания работы по обеспечению безопасности, основанной на правах человека.

Члены группы хранили секрет О'Рурка на протяжении десятилетий, не желая ставить под угрозу его политическую деятельность. Однако в серии интервью члены CDC признали О'Рурка одним из своих. В целом, более дюжины участников

согласились фигурировать в книге о хакерской группе. У О'Рурка взяли интервью в самом начале его кампании в Сенат…» ***(Ирина Фоменко. Кандидат в президенты США оказался бывшим хакером // Internetua (http://internetua.com/kandidat-v-prezidenty-ssha-okazalsya-byvshim-hakerom). 17.03.2019).***

***

«Эксперты Flashpoint обнаружили новые атаки группировки Fin7, которая вернулась к активным действиям после ареста нескольких ее участников. Злоумышленники используют два новых зловреда и панель администратора, которые помогают им красть ценные данные, практически не оставляя следов.

Американские полицейские задержали трех граждан Украины — членов Fin7 в августе прошлого года. Правоохранители обвинили их в похищении платежной информации у клиентов более 100 компаний в нескольких странах. Группировка применяет бесфайловые зловреды, чтобы атаковать рестораны, отели, игорные дома и другие заведения.

Как сообщили специалисты, нынешние атаки Fin7 продолжают кампании, стартовавшие еще в январе 2018 года. Они построены на вредоносных документах, которые распространяются через email-рассылки. Эксперты отмечают, что составители писем учитывают специфику отраслей, в которых работают их жертвы, и всячески подталкивают их к открытию вложения. Полезную нагрузку составляют две вредоносные программы — SQLRat и DNSBot.

Первый файл запускается через форму Visual Basic, встроенную в документ-приманку. Для успешной атаки жертва должна кликнуть по картинке, в которую и встроен вредоносный модуль. Он запускает обфусцированный JavaScript-сценарий и загружает на компьютер дополнительные файлы.

Далее зловред выполняет серию SQL-скриптов, которые и обеспечили ему название. Эти сценарии связывают компьютер с сервером Fin7, позволяя провести необходимые действия с зараженной машиной, а потом удалить следы вторжения.

Второй тип полезной нагрузки, DNSBot, выполняет функции бэкдора. С его помощью преступники отправляют команды компьютерам жертв и получают с них необходимые данные. Вся коммуникация происходит по протоколу DNS, но эксперты нашли в коде возможность перейти на защищенные каналы HTTP или SSL.

Для управления текущими кампаниями преступники используют еще одну новинку — панель администратора Astra, построенную на базе Windows-сервера с применением Microsoft SQL. Эта написанная на PHP консоль позволяет быстро устанавливать скрипты на компьютеры жертв.

Специалисты рекомендуют пользователям проверить Планировщик Windows — зловреды создают под себя две ежедневные задачи, закрепляясь таким образом на зараженной машине. Кроме того, для усиления защиты стоит настроить свое антивирусное решение на регулярное сканирование папок %appdata%\Roaming\Microsoft\Templates\ и %appdata%\local\Storage\.» ***(Egor Nashilov. Группировка Fin7 возобновила атаки // Threatpost***

(https://threatpost.ru/fin7-phishing-emerges-yet-again-with-new-malware/31942/). 21.03.2019).

***

«Російські хакерські групи останніми місяцями посилили атаки на держустанови, політичні організації та медіа в Німеччині та інших країнах ЄС.

Про це заявила американська компанія з кібербезпеки FireEye…

Від середини 2018 року експерти виявили "значне збільшення" діяльності хакерських груп APT28 (також відома як Fancy Bear) і Sandworm, заявила компанія. Західні уряди вважають ці хакерські групи підпорядкованими російському уряду і військовій розвідці ГРУ.

Як заявив старший менеджер FireEye з аналізу кібершпигунства Бенджамін Рід, хакери можуть "публікувати дані, які завдають шкоди окремим політичним партіям або кандидатам перед виборами в Європі".

Експерти японської компанії Trend Micro також помітили "підвищену активність" від APT28 за останні півроку, повідомляє газета. Постраждали політичні фонди та неприбуткові організації з метою просування демократії в Бельгії та Німеччині.

У минулому APT28 звинувачували в нападах на Бундестаг, МЗС і Міноборони Німеччини, Фонд Конрада Аденауера, Фонд Фрідріха Еберта, Демократичну партію в американській президентській виборчій кампанії, НАТО і виборчу кампанію президента Франції Еммануеля Макрона. Корпорація Microsoft повідомила, що протягом 2018 року хакери, ймовірно з тієї ж групи, здійснили атаки на аналітичні центри, пов'язані з політикою ЄС, зокрема на Німецьку раду з міжнародних відносин, Інститут Аспена та Німецький фонд Маршалла.

На думку аналітиків, мета хакерської групи - шпигунство. На противагу цьому, група Sandworm, за їхніми словами, здійснює акти саботажу. Серед іншого, група несе відповідальність за хакерські атаки на електростанції в Україні, а також на українські засоби масової інформації, які мали на меті не шпигунство, а знищити інфраструктуру.» ***(Російські хакери активізували атаки в Німеччині – ЗМІ // Європейська правда (https://www.eurointegration.com.ua/news/2019/03/22/7094278/). 22.03.2019).***

***

«За словами експертів з кібербезпеки, хакери зламали інструменти для автоматичного оновлення програмного забезпечення компанії ASUS, завдяки чому вдалося поширити шкідливе програмне забезпечення на сотнях тисяч комп'ютерів бренду. Варто відзначити, що віруси поширювалися як на нові пристрої, так і на старі.

За заявами (сайт заблокований на території України) експертів, тайванська компанія ненавмисно встановила “злоякісний” бекдор на тисячі комп'ютерів своїх клієнтів. У шкідливих файлів був законний цифровий сертифікат ASUS, що дозволяло їм майже безперешкодно поширюватися, і ніхто навіть і не зміг помітити підступу. Уразливість помітили лише через 5 місяців, що робить всі гаджети від ASUS потенційно небезпечними для клієнтів. ASUS поки не коментує ситуацію,

але користувачі хочуть дізнатися думку корпорації на цей рахунок…» ***(ASUS 5 місяців поширювала віруси на ноутбуки: мільйони користувачів під загрозою // znaj.ua (https://znaj.ua/techno/221794-asus-5-misyaciv-poshiryuvala-virusi-na-noutbuki-milyoni-koristuvachiv-pid-zagrozoyu). 27.03.2019).***

***

«Эксперты антивирусной компании ESET изучили недавние кибератаки хакерской группировки OceanLotus (также известной как APT32 и APT-C-00) и пришли к выводу, что злоумышленники существенно расширили список используемых техник в попытках скрыться от антивирусного ПО.

OceanLotus преимущественно действует в странах Юго-Восточной Азии — Лаосе, Камбодже, Вьетнаме и на Филиппинах. Их целью является шпионаж за госструктурами, политическими партиями и крупными компаниями этих государств.

В новой вредоносной кампании киберпреступники использовали уязвимость в Microsoft Office (CVE-2017-11882) с целью фишинговых атак. Для заражения пользователей применялись файлы с двойным расширением и самораспаковывающиеся архивы.

Жертвы OceanLotus получали фишинговые письма, замаскированные под сообщения СМИ о текущих политических событиях. В письмах использовались интригующие имена вложений, связанные с актуальной новостной повесткой.

Открыв вредоносное вложение в виде документа с поддержкой макросов или запустив самораспаковывающийся SFX-архив, замаскированный под обычное изображение, пользователь инициировал установку бэкдора. Получив доступ к системной информации, бэкдор отправлял ее на управляющий C&C-сервер.

Эксперты ESET полагают, что группировка продолжит совершенствовать свои методы, уменьшая шансы обнаружения продуктами безопасности…» ***(Эксперты изучили новые ловушки группировки OceanLotus // IKSMEDIA.RU (http://www.iksmedia.ru/news/5573714-Eksperty-izuchili-novye-lovushki.html). 28.03.2019).***

***

Вірусне та інше шкідливе програмне забезпечення

«Мир привык к вредоносным программам, которые крадут информацию о кредитной карте или требуют биткоины, чтобы вернуть доступ к файлам. Однако, согласно новому исследованию в MIT, главной угрозой в этом году станет программа, которая нацелена на системы безопасности промышленных предприятий по всему миру.

Согласно исследованию, проведенному в MIT, программа очень похожа на систему безопасности, которая защищают атомные электростанции и водоочистные сооружения.

«В худшем случае, неавторизованный код может привести к выбросу токсичного сероводородного газа или вызвать взрывы, поставив под угрозу жизни

людей как на объекте, так и в его окрестностях», — отметил Мартин Джайлз из MIT Tech, после атаки программы на нефтехимический завод в Саудовской Аравии.

Исследователи называют вредоносное ПО Triton. Оно распространяется с 2014 года, но исследователи узнали об этом только в 2017 году. Самое тревожное, как сообщил MIT Tech неназванный источник, заключается в том, что вредоносное ПО пересекает этическую черту…». ***(Вредоносная программа выводит из строя системы безопасности на промышленных предприятиях // Goodnews.ua (http://goodnews.ua/technologies/vredonosnaya-programma-vyvodit-iz-stroya-sistemy-bezopasnosti-na-promyshlennyx-predpriyatiyax/). 11.03.2019).***

***

«Исследователи безопасности компании Morphisec сообщили о новой вредоносной кампании, в ходе которой злоумышленники атакуют PoS-терминалы по всему миру с целью кражи данных банковских карт. Жертвами киберпреступников стали финансовые, страховые, медицинские и прочие организации в Индии, Японии, США и других странах.

По словам исследователей, имеющихся у них сведений недостаточно для того, чтобы с точностью определить, кто стоит за атаками. «Почерк» киберпреступников наводит на мысль о группировке FIN6, но некоторые моменты указывают на возможную связь с группировкой EmpireMonkey.

По мнению исследователей, одним из векторов атак являются файлы HTA (HTML Application), выполняющие скрипты PowerShell как часть встроенного VBScript.

Используемое злоумышленниками вредоносное ПО для похищения данных из памяти PoS-терминалов отличается от случая к случаю. В одних случаях они прибегают к инструменту FrameworkPOS, а в других – к PowerShell/WMI для загрузки ПО Cobalt Strike с расширением PowerShell непосредственно в память. Cobalt Strike позволяет атакующим получить контроль над зараженной системой и проникать в другие системы в одной с ней сети. С его помощью злоумышленники могут похищать учетные данные жертв, выполнять код и осуществлять другие вредоносные операции.» ***(Новая волна кибератак обрушилась на PoS-терминалы // Goodnews.ua (http://goodnews.ua/technologies/novaya-volna-kiberatak-obrushilas-na-pos-terminaly/). 04.03.2019).***

***

«Fortinet представила результаты последнего отчета о кибератаках. Исследования показывают, что кибер-преступники в своей деятельности прибегают даже к мемам.

Вредоносные программы, замаскированные в мемах — это стеганография — метод, который заключается в сокрытии вредоносных сообщений, таким образом невозможно обнаружить, где находится сам факт проведения связи. Киберпреступники часто используют этот механизм. В прошлом квартале аналитики Fortinet обнаружили вредоносные программы, использующие команды, скрытые в мемах, размещенных в социальных сетях. С целью безопасности нужно

соблюдать осторожность и лучше не загружать файлы с мемами. Появились также предложения, чтобы во внутренних корпоративных сетях, блокировать доступ к материалам с картинками, которые называются мемами. Это ограничило бы риск заражения корпоративной сети.» ***(Алекс Max. Мемы используются для проведения кибератаки // Bad Android (https://bad-android.com/news/45886-memy-ispolzuyutsya-dlya-provedeniya-kiberataki). 04.03.2019).***

***

«Финансовое вредоносное ПО Qbot, которому уже десять лет, вновь появилось в улучшенной версии в новой атаке на предприятия, заразив тысячи систем…

Исследователи Varonis раскрыли атаку после предупреждения клиента о подозрительной активности на компьютере. Виновником оказалась заражение новым штаммом Qbot, также известным как Qakbot, который пытался распространиться на другие системы в сети.

Qbot является одной из самых успешных вредоносных программ за последнее десятилетие, отчасти потому, что ее исходный код доступен для киберпреступников, поэтому Qbot можно легко модифицировать и расширять. Изначально Qbot был трояном, предназначенным для кражи учетных данных онлайн-банкинга, но с годами получил множество улучшений.

Qbot представляет собой полуполиморфную угрозу, поскольку его серверы управления и контроля периодически перешифровывают код и конфигурацию, чтобы избежать обнаружения антивирусными программами. ПО также может перемещаться по корпоративным сетям с помощью учетных данных Windows…» ***(Зафиксирована новая кибератака на бизнес-ресурсы // Goodnews.ua (http://goodnews.ua/technologies/zafiksirovana-novaya-kiberataka-na-biznes-resursy/). 02.03.2019).***

***

«13 марта была осуществлена массовая рассылка вредоносных документов (MS Word Document), «вооруженных» макросом. Атака была направлена на украинские органы государственной власти и финансовые учреждения…

В качестве приманки использовалось письмо от имени Национального агентства по вопросам предотвращения коррупции…

В случае активации содержимого (запуска макроса) на атакуемом ПК будет выполнена команда powershell, которая повлечет за собой цепочку связанных событий, в конечном счете ведущую к заражению ПК вредоносной программой.

Для коммуникации с сервером управления используется HTTPS-соединение (с самоподписанным (от 12.03.2019) сертификатом). Основную логику работы первой фазы заражения выполняют powershell и MSIL байт-код (оригинальное имя: "tools.dll"; дата компиляции: 2019-03-12 06:16:05; класс "R3Rq4b8"). Изначально обеспечивается сбор информации об атакуемом объекте (systeminfo, ipconfig, netstat и др., а также снимок экрана). Вторая фаза предполагает загрузку на ПК другого EXE/DLL файла (на момент исследования не установлен)…

Также эксперты отмечают, что злоумышленники, возможно, заинтересованы в атаках на организации среднего и большого размера. В пользу этого предположения говорит тот факт, что одна из выполняемых проверок определяет принадлежность атакованного компьютера к домену (как правило, применяется в корпоративных сетях)…

Применительно к конкретному инциденту, эксперты рекомендуют:

Ограничить возможность запуска документов с макросами.

Предотвратить возможность запуска powershell.exe из-под WINWORD.EXE (в данном случае powershell даже не был переименован).

Обращать внимание на необходимость мониторинга (например, с помощью штатных средств журналирования ОС и/или sysmon) фактов запуска легитимных утилит (процессов), используемых на этапе разведки объекта атаки.

Обеспечить мониторинг сетевых подключений, осуществляемых с помощью самоподписанных сертификатов.

В случае выявления фактов коммуникации с упомянутым IP-адресом осуществить исследование инцидента…» ***(Владимир Кондрашов. Эксперты: хакеры проводят «разведку боем» от имени НАПК // Internetua (http://internetua.com/eksperty-hakery-provodyat-razvedku-boem-ot-imeni-napk). 14.03.2019).***

***

«Group-IB зафиксировала активность нового JS-сниффера, предназначенного для перехвата пользовательских данных: номеров банковских карт, имен, адресов, логинов, паролей.

Первым ресурсом, на котором эксперты Group-IB обнаружили JS-сниффер, стал сайт, принадлежащий спортивному гиганту FILA, fila.co[.]uk, как минимум 5 600 клиентов которого могли стать жертвой кражи платежных данных за последние 4 месяца. В общей сложности новый JS-сниффер заразил 7 сайтов, включая шесть онлайн-магазинов в США, которые суммарно посещают около 350 000 уникальных посетителей в месяц…

О новом инциденте стало известно в феврале 2019 года благодаря команде Group-IB Threat Intelligence. Британский сайт FILA (fila.co[.]uk) стал одной из мишеней киберпреступников, внедривших вредоносный код JS-сниффера, получившего название GMO. Этот же вредонос был обнаружен на 6 сайтах американских компаний. Команда Group-IB предприняла несколько попыток предупредить сайты о том, что они оказались зараженными этим JS-сниффером. Специалисты компании Group-IB также передали информацию в профильные организации в Великобритании и США.

В Group-IB пояснили: «Вредоносный код загружает JavaScript-сниффер как только клиент попадает на страницу оформления заказа. Сниффер, внедренный на сайт, перехватывает данные кредитной карты и персональную информацию жертвы, после чего отправляет их на сервер злоумышленников — гейт. В цепочке передачи данных со сниффера может быть использовано несколько уровней гейтов, расположенных на разных серверах или взломанных сайтах, что усложняет задачу обнаружить конечный сервер злоумышленников. Однако в некоторых случаях

административная панель расположена на том же хосте, что и гейт для сбора украденных данных. Киберпреступники могли внедрить вредоносный код несколькими способами: используя уязвимость Magento CMS (системы управления контентом), используемой FILA.co.uk, или скомпрометировав учетные данные администратора сайта, используя программу-шпион или взломав пароль методом простого перебора паролей».

Специалисты направления Threat Intelligence Group-IB впервые зафиксировали активность нового JS-сниффера именно на британском сайте компании FILA. Вредоносный код был обнаружен в начале марта 2019 года. В ходе расследования выяснилось, что GMO предположительно собирает данные о платежах клиентов с ноября 2018 года. Используя данные сайта Alexa.com, можно посчитать, что сайт посещает около 140 000 уникальных пользователей. Минимальная конверсия в покупку для интернет-магазинов одежды составляет 1%, по данным IRP. Следовательно, киберпреступники по самым скромным подсчётам могли похитить платежные и личные данные как минимум 5600 клиентов: каждый, кто приобретал товары на сайте fila.co.uk с ноября 2018 года, может находиться в «группе риска».

Позже специалисты Group-IB обнаружили другие сайты, зараженные JS-сниффером GMO. Список жертв включает шесть онлайн-магазинов в США, которые в общей сложности посещают около 350 000 уникальных посетителей в месяц (согласно рейтингу Alexa.com): http://jungleeny[.]com (магазин домашнего дизайна), https://forshaw[.]com/ (магазин продукции для борьбы с насекомыми), https://www.absolutenewyork[.]com/ (магазин косметики), https://www.cajungrocer[.]com/ (продуктовый онлайн-магазин), https://www.getrxd[.]com/ (магазин тренажёров), https://www.sharbor[.]com/ (магазин оборудования для видеомонтажа)…» ***(Платежные данные тысяч клиентов онлайн-магазинов США и Великобритании могли быть скомпрометированы // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5570998-Platezhnye-dannye-tysyach-klientov.html). 15.03.2019).***

***

«Опасный вирус DMSniff атаковал терминалы оплаты и крал данные банковских карт. Вредоносную программу обнаружили сотрудники компании Flashpoint, их исследование опубликовано на портале BleepingComputer.

Вирус попадает в устройство либо путем подбора пароля, либо через эксплуатацию уязвимостей. В ходе мониторинга зараженного устройства программа ищет данные о банковских картах и передает их в руки злоумышленников.

Вредоносное ПО также скрывает передаваемые данные, чтобы зашифровать свои действия. Жертвами хакеров чаще всего становились развлекательные предприятия и кафе.

Преступники используют DMSniff с 2016 года. С тех пор исследователи в области кибербезопасности обнаружили более десятка различных вариаций вируса…» ***(В терминалах оплаты нашли ворующий деньги вирус // Goodnews.ua***

(http://goodnews.ua/technologies/v-terminalax-oplaty-nashli-voruyushhij-dengi-virus/). 17.03.2019).

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Нидерландский суд оставил на свободе организатора DDoS-атак, от которых пострадали BBC, Yahoo News, криптобиржа Moneypot и прочие интернет-ресурсы. Злоумышленник, которому на момент суда исполнилось 20 лет, признал вину и попросил о снисхождении, что позволило ему отделаться 120 часами общественных работ.

Следствие не раскрывает имя преступника — в судебных материалах он обозначен как S. Эксперты полагают, что это один из 20 операторов крупнейших IoT-ботнетов 2018 года.

…преступник построил сеть на базе варианта Mirai. Обвинение оценило ее размер в 2697 хостов, другие источники сообщают о 10 тыс. зараженных устройств. В октябре 2016 года злоумышленник стал атаковать с их помощью различные сайты, требуя с некоторых компаний выкуп. DDoS-атаки с этого ботнета прекратились лишь через год, когда полиция арестовала организатора.

Сам S. объяснил свои действия тем, что родители ограничивали его карманные расходы. Когда злоумышленник узнал, что Mirai принес своему создателю $100 тыс., он решил также воспользоваться ботнетом — зловред к тому времени уже попал в открытый доступ. Как установило следствие, преступная деятельность принесла преступнику $150 тыс. в биткойнах.

Представители обвинения просили назначить молодому человеку два года тюремного заключения вместе со штрафом в €12 тыс., которые он должен заплатить некоторым жертвам. Итоговый приговор оказался мягче — подсудимого ждут 120 часов общественных работ и условный срок в 360 дней. Суд учел тот факт, что S. нарушил закон до совершеннолетия и полностью признал свою вину. Вторую часть наказания, 377 дней заключения в центре для несовершеннолетних, списали в счет времени, которое преступник провел в ожидании приговора…» ***(Egor Nashilov. В Нидерландах 20-летний организатор DDoS-атак избежал тюрьмы // Threatpost (https://threatpost.ru/dutch-ddos-mirai-botmaster-evades-jail/31897/). 19.03.2019).***

***

«Австралийская федеральная полиция (AFP) при содействии ФБР США арестовала 21-летнего юношу, который промышлял торговлей краденными учетными данными. Житель Сиднея в течение почти двух лет управлял сайтом WickedGen[]com, где выставил на продажу около миллиона имен и паролей пользователей Netflix, Spotify, Hulu и других сервисов. Вплоть до закрытия объявления на сайте уверяли, что на ресурсе зарегистрированы 120 тыс. человек.

Правоохранители полагают, что преступник заработал с помощью WickedGen и подобных ему сайтов, продававших чужие подписки, не менее $212 тыс.

Специалисты пришли к выводу, что данные пользователей со всего мира, выложенные на преступных ресурсах, добыли с помощью атак credential stuffing. Расследование началось в мае 2018 года, когда ФБР США обратило внимание австралийской полиции на сайт, а задержание произошло 12 марта в пригороде Сиднея Ди Вай. У мошенника, имя которого не разглашается, при обыске изъяли «электронные материалы и различные криптовалюты»…

Молодого человека обвиняют по пяти статьям. Наиболее серьезная из них — доход, полученный преступным путем, в размере свыше $100 тыс., — предусматривает максимальное наказание в виде тюремного заключения сроком до 20 лет…» ***(Egor Nashilov. В Австралии арестовали торговца краденными учетными данными // Threatpost (https://threatpost.ru/stolen-data-dealer-busted-by-australian-police-and-fbi/31876/). 15.03.2019).***

***

Технічні аспекти кібербезпеки

Виявлені вразливості технічних засобів та програмного забезпечення

«В воскресенье, 10 марта, в официальном блоге Google появилась информация о том, что компании удалось обнаружить в Windows 7 сразу две критических уязвимости, которые уже используются хакерами для внедрения вредоносного кода в ОС…

Так как речь идет об уязвимости нулевого дня, которая состоит из двух брешей в системе защиты, из сообщения следует, что все компьютеры на Windows 7 неожиданно взломали, ибо никакого способа защиты от обнаруженной «дыры» в безопасности пока что нет.

В свою очередь, Microsoft уже признала, что такая проблема действительно имеет место быть, но над ее решение уже работают специалисты, однако на полную ликвидацию бреши уйдет порядка 10 дней, а возможно и больше.

Чтобы уже сейчас защититься от критической бреши, которую обнаружила Google, компания Microsoft советует обновить Windows 7 до Windows 10, где подобной проблемы попросту нет. Сейчас же все компьютеры и иные электронные устройства, работающие на седьмой «винде», могут быть взломаны, потому как брешь позволяет выполнять произвольный вредоносный код без каких-либо ограничений и с правами суперадминистратора, поэтому пользователи не смогут даже понять, что их электронное устройство чем-то заразили.

Издание отмечает, что подобная информация не лучшим образом сказывается на репутации Microsoft, в программном обеспечении которой снова и снова обнаруживают какие-то недочеты. Хорошего во всем этом ничего нет, потому как почти наверняка за многие годы существования уязвимости в Windows 7, о которой

сообщила Google, ее успели обнаружить десятки хакеров, используя для заражения компьютеры обычных пользователей. Она позволяет украсть личные данные, перехватывать данные, показывать рекламу, а также выполнять любые другие действия, вплоть до полного удаления ОС и всех файлов…» ***(Сразу две критических уязвимости: все компьютеры на Windows 7 неожиданно взломали // «Факты и комментарии®» (https://fakty.ua/298700-srazu-dve-kriticheskih-uyazvimosti-vse-kompyutery-na-windows-7-neozhidanno-vzlomali). 11.03.2019).***

***

«Специалисты из Университета Левена заявили об уязвимости, которую содержат в себе все Wi-Fi-роутеры.

Они отметили, что из-за этого в зоне риска находится любой гаджет, который может таким образом выходить в интернет, пишет NewsOboz.org со ссылкой на Корреспондент.net.

Эксперты отмечают, что роутер защищен от кибератак благодаря технологии сетевой безопасности под названием Wireless Protected Access 2 (WPA-2). Данная технология является неотъемлемой в любом сертифицированном оборудовании с 2006 года.

Однако, как оказалось, все роутеры с данной системой уязвимы для взлома. Для атаки кибермошенники используют программу Key Reinstallation Attacks (KRACK).

Совершая атаку, злоумышленник может получить доступ к личным контактам пользователей на гаджетах, паролям и данным банковских карт.

При этом, по словам специалистов, проблема кроется в самой WPA-2, содержащей уязвимость. Такие компании, как Google и Apple, уже выпустили обновления для устранения такой уязвимости.» ***(Раскрыт универсальный способ взлома Wi-Fi // NewsOboz (http://newsoboz.org/it_tehnologii/raskryt-universalnyy-sposob-vzloma-wi-fi-11032019132200). 12.03.2019).***

***

«Уязвимости в подключенных медицинских устройствах могут иметь серьезные последствия для пациентов и отрасли здравоохранения в целом…

Эксперты Check Point утверждают, что Интернет медицинских вещей (IoMT) призван расширить поверхность атаки для организаций здравоохранения. Ожидается, что к концу 2019 года 87% медицинских учреждений будут использовать технологии IoT, а к 2020 году будет использовано почти 650 миллионов устройств IoMT.

Устройства IoT собирают огромное количество данных и обычно основаны на устаревшем программном обеспечении и операционных системах. Это делает их уязвимыми для киберпреступников, которые могут их легко взломать и перемещаться по сети.

Рассмотрим ультразвуковые технологии. Исследователи объясняют, как были достигнуты "огромные успехи" для предоставления подробных данных о здоровье врачам и пациентам. К сожалению, новшество не привело к безопасности IT-среды,

в которой работают ультразвуковые аппараты. Чтобы доказать это, исследователи проанализировали устройство.

Оказалось, что ультразвуковая машина работает на Windows 2000. Как и многие устройства IoMT, аппарат больше не получает обновлений или исправлений и оставляет как компьютер, так и его данные открытыми для злоумышленников. По словам экспертов, использовать уязвимости несложно, чтобы получить доступ к базе данных ультразвуковых изображений.

Злоумышленник с таким доступом может запустить вирусы-вымогатели в системе больницы или подменить изображения пациентов. "Подумайте, сколько хаоса может принести это медучреждению", - заявил руководитель исследования уязвимости продукта Check Point Одед Вануну.

Киберпреступники могут использовать медицинские записи для получения дорогостоящих услуг и отпускаемых по рецепту лекарств; они также могут получить доступ к государственным льготам. Ponemon Institute обнаружил, что нарушения в сфере здравоохранения самые дорогие, по 408 долларов за запись.

Вануну объяснил, что у организаций здравоохранения часто не хватает средств для обеспечения IT и безопасности. "Больницы - это однородные сети. Мы думаем, что киберпреступность начнет распространяться на самые слабые сети. Это уже происходит", - утверждает Одед.

IoMT-устройства находятся в серийном производстве, но ничего не делается для их защиты. Поскольку анализируемое устройство Check Point работало под Windows 2000, его было легко использовать. "Нет уязвимости нулевого дня, нет уязвимости обратного проектирования. Любой новичок может воспользоваться ею", - заявил Вануну». ***(Ирина Фоменко. Эксперты: медицинские IoT-устройства могут легко взломать хакеры // Internetua (http://internetua.com/eksperty-medicinskie-iot-ustroistva-mogut-legko-vzlomat-hakery). 11.03.2019).***

***

«Уязвимость в веб-версии Google Фото позволяет киберпреступникам узнать подробности истории фотографий пользователя…

Через браузерные тайминг-атаки хакеры могут анализировать данные изображения, чтобы узнать, когда человек посещал определенное место. Это не обычная угроза, и она наиболее эффективна в целевом сценарии, но вредоносный веб-сайт можно использовать и для доступа к фотографиям.

"Google Фото много знает о людях, которые его используют. Служба автоматически помечает каждое изображение с помощью метаданных (дата, координаты местоположения), а механизм искусственного интеллекта обнаруживает объекты и события, которые могут указывать на свадьбу, водопад, закат или ряд других мест. Теги распознавания лиц также присутствуют на фотографиях", - объяснил исследователь Imperva Рон Масас. – "Эта подробная информация может многое рассказать о том, когда, где и с кем был человек".

Масас обнаружил, что конечная точка поиска службы уязвима для атаки, называемой межсайтовым скриптингом или XSS. В подтверждение своей концепции он использовал тег HTML-ссылки для создания нескольких

перекрестных запросов к конечной точке поиска. Используя JavaScript, он измерил время, необходимое для запроса к серверу Google Фото и получения в качестве ответа нулевых результатов.

Вот как работает эта уязвимость: преступник должен сначала отправить цели злонамеренную ссылку, пока этот человек находится в Google Фото, путем встраивания вредоносного JavaScript в веб-рекламу, отправки прямого сообщения по электронной почте или через онлайн-мессенджер. Вредоносный код JavaScript создает запросы к конечной точке поиска в Google Фото и извлекает ответы.

Однако, как только жертва закрывает вредоносную страницу, поиск прекращается. "В тот момент, когда вы закрываете сайт, я больше не могу этого делать. Но могу обмануть вас, чтобы вы зашли на другой ресурс в будущем, и продолжу оттуда. Нужно, чтобы вы каждый раз открывали сайт", - пояснил Масас.

По мнению исследователя, это не очень сложная атака, но она имеет наибольшую ценность, если хакер специально нацелен на одного человека. Например, кто-то мог использовать уязвимость, чтобы определить местонахождение высокопоставленного человека или узнать, с кем он проводил время.» ***(Ирина Фоменко. Уязвимость в Google Фото позволяет преступникам узнать местоположение жертвы // Internetua (http://internetua.com/uyazvimost-v-google-foto-pozvolyaet-prestupnikam-uznat-mestopolojenie-jertvy). 21.03.2019).***

***

«За два первых дня соревнования Pwn2Own-2019 в Ванкувере этичные хакеры нашли и продемонстрировали 14 уязвимостей в браузерах и платформах виртуализации. Это принесло им в общей сложности $510 тыс.

Pwn2Own проводится в рамках конференции по информационной безопасности CanSecWest начиная с 2007 года. В этот раз призовой фонд составил $1 млн.

Компании-партнеры предложили исследователям список целей в нескольких категориях. Среди виртуальных машин их больше всего интересовали бреши в Oracle VirtualBox, VMware Workstation, VMware ESXi и клиенте Microsoft Hyper-V. Востребованным остается и обнаружение уязвимостей в браузерах Chrome, Microsoft Edge, Safari и Firefox, а также корпоративных приложениях — Adobe Reader, Microsoft Outlook и пакете MS Office 365. Кроме того, представители Microsoft выдвинули заявку на поиск багов в протоколе RDP, предназначенном для удаленной работы с сервером.

В этом году в числе партнеров соревнования появилась компания Tesla. Ее представителей больше всего интересует безопасность IoT-устройств, поскольку все обновления для своих автомобилей Tesla доставляет по воздуху. В последний день конкурса, участники попробуют себя в новой, автомобильной категории и попытаются взломать Tesla Model 3…» ***(Egor Nashilov. За два дня «белые» хакеры заработали на Pwn2Own $510 тысяч // Threatpost (https://threatpost.ru/pwn2own-2019-participants-earned-510k-dollars/31961/). 22.03.2019).***

***

«Компанія “Check Point”, котра спеціалізується на кібербезпеці, виявила уразливість в WinRAR, яка існувала понад 19 років. Помилка закралася в підтримку архіватором застарілого формату ACE, коли зловмисники можуть привласнювати файлу ACE розширення (rar), після чого, потім, використовувати його для виконання шкідливого коду з теки автозапуску після перезавантаження системи.

Rarlab вже випустили патч, але ті, хто не використовує останню версію програми, все ще знаходяться в небезпеці, оскільки хакери вже щосили використовують дану уразливість. Дослідження компанії “McAfee” виявило понад 100 унікальних експлойтів.

У WinRAR близько 500 мільйонів користувачів, більшість з яких, ймовірно, не знають про цю уразливість, що ще більше приманює хакерів. Ймовірно, дана атака спричинить серйозні наслідки в майбутньому, тому, будь ласка, поділіться новиною з друзями й сім’єю, якщо ви знаєте, що у них встановлений WinRAR, і звантажте останню версію програмного забезпечення.» ***(В архіваторі WinRAR знайдена критична уразливість // hpib.life (http://hpib.life/v-arxivatori-winrar-znajdena-kritichna-urazlivist/). 19.03.2019).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Ghidra представил на конференции RSA в Сан-Франциско Роб Джойс, старший советник агентства по кибербезопасности. Программа умеет декомпилировать, осуществлять обратное проектирование и анализировать вредоносное ПО…

Долгие годы Ghidra была внутренним инструментом АНБ.

Даже о факте ее существования до 2017 года — когда WikiLeaks опубликовала секретные документы ЦРУ — было неизвестно.

Разумеется, это не единственный инструмент обратного инжиниринга в сети. Есть несколько альтернатив, вроде IDA европейской компании Hex Rays, созданного добровольцами Radare или Binary Ninja от Vector 35. Однако большинство из них платные, тогда как Ghidra распространяется свободно — скачать ее можно со страницы на GitHub…

Специалисты высоко оценили Ghidra и ее функции: например, возможность работать сообща над одним проектом, поддержку различных процессоров, настраиваемый пользовательский интерфейс, использование шаблонов, расширений и плагинов…» ***(АНБ открыло доступ к засекреченному приложению // Goodnews.ua (http://goodnews.ua/technologies/anb-otkrylo-dostup-k-zasekrechennomu-prilozheniyu/). 09.03.2019).***

***

«На торговой площадке eBay… был выставлен лот, в котором продаётся… устройство для дешифровки и взлома смартфонов… всего за жалкие, относительно полной стоимости, 100 долларов. Такие государственные службы как к примеру Федеральное бюро расследований (ФБР) США, а так же различные министерства внутренней безопасности, приобретают данные универсальные, многофункциональные приборы компании Cellebrite, использующиеся для судебной экспертизы за сумму, порой достигающую 15000 долларов. Отмечается, что на вторичном рынке можно приобрести более ранние образцы этих устройств по более низкой цене, но это сути дела не меняет.

Эта ситуация походит на факт того, что правоохранительные органы решили продать, либо же просто выкинуть подобные, уже устаревшие модели устройств. В связи с этим устройства скорей всего и попали на торговую площадку eBay. Обеспокоенный этим фактом, Мэтью Хики — исследователь кибербезопасности приобрёл на вышеуказанной площадке несколько штук устройств UFED, вскоре после чего узнал, для взлома каких устройств использовалось оборудование, и какие данные с его помощью удалось достать. Конечно Мэтью Хики не указывает, какие именные данные он смог обнаружить: различные личные данные, фотографии, или же доступ к перепискам…

В ходе исследования Мэтью обнаружил, что устройства были использованы для получения доступа к таким телефонам как Motorola, LG, Samsung и ZTE. Так же отмечается, что это устройство могло бы запросто взломать IPod и IPhone старых поколений со старыми версиями операционных систем. Это является доказательством того, что старые модели устройств взлома UFED продаются или выкидываются за ненадобностью. Вызвано это тем, что современные устройства постоянно получают новые версии прошивок и операционных систем, что в свою очередь делает некоторые модели устройств взлома полностью бесполезными. Устройство от Cellebrite для взлома использует различные «дыры» и уязвимости в операционных системах от Google и Apple. Но приходится постоянно обновлять протоколы взлома, так как компании постоянно исправляют ошибки, и латают дыры. На данный момент самое новое устройство способно взломать IPhone на базе ОС IOS 11.

Cellebrite обеспокоилась тем, что их устройства попадают в руки обычных граждан, в связи с чем компания попросила не продавать устаревшие модели, а уничтожать их, или отправлять обратно фирме, для дальнейшей утилизации.» ***(На eBay можно приобрести устройства для взлома смартфонов // Goodnews.ua (http://goodnews.ua/technologies/na-ebay-mozhno-priobresti-ustrojstva-dlya-vzloma-smartfonov/). 02.03.2019).***

***

«Источники заявили, что знаменитый антивирусный гигант «Лаборатория Касперского» готовит новую мобильную операционную систему, за основу которой будет взята уже существующая KasperskyOS. Упор в новой ОС будет сделан на безопасность пользователей. Согласно данным, полученным RNS от неназванного топ-менеджера одной из ИТ-компаний, новая мобильная система может выйти до конца этого года. На данный момент ОС, судя

по всему, находится в стадии тестирования. «Лаборатория Касперского» планирует продавать новое решение государственным организациям и крупным компаниям. Однако есть информация о том, что вендор может выпустить и версию для граждан. Логично предположить, что версия для госструктур позволит произвести импортозамещение, чего уже давно пытаются добиться власти. «У компании будет два позиционирования операционной системы: одно для госструктур в рамках импортозамещения и информационной безопасности, а второе для домашних пользователей в рамках борьбы за приватность персональных данных», — рассказал источник. В настоящее время уже существующее решение KasperskyOS планируется включить в реестр отечественного программного обеспечения. «Лаборатория Касперского» подала соответствующую заявку.» ***(Олег Иванов. RNS: Лаборатория Касперского готовит мобильную ОС для импортозамещения // ООО «АМ-МЕДИА» (https://www.anti-malware.ru/news/2019-03-05-1447/29061). 05.03.2019).***

***

«…Вместо вымогательства киберпреступники в последнее время предпочитают внедрять на компьютеры жертв программы для майнинга криптовалют, отмечают специалисты фирмы Darktrace. Майнинг занимает много времени, но приносит гарантированную прибыль, в отличие от вымогательства, считают специалисты. Преступники придумывают разные способы скрыть работу майнинговых программ от пользователя: например, запуская их не на полную мощность, чтобы не допустить перегрева и чрезмерного шума вентилятора. Хотя на первый взгляд майнинг не наносит значительного ущерба пользователю (за исключением траты электричества и сетевого трафика), компьютер при этом все равно находится под контролем злоумышленника и он может от майнинга перейти, например, к краже финансовых данных.

Darktrace рекламирует собственную систему мониторинга компьютерных систем (включая облачные) под названием Antigena, применяющую технологии искусственного интеллекта для выявления необычного поведения устройств. В одной японской инвестиционной фирме Antigena помогла обнаружить вирус в системе видеонаблюдения, благодаря которому злоумышленники могли наблюдать за всей работой фирмы.» ***(Darktrace: киберпреступники предпочитают воровать вычислительные ресурсы для криптомайнинга // «Открытые системы» (https://www.computerworld.ru/news/Darktrace-kiberprestupniki-predpochitayut-vorovat-vychislitelnye-resursy-dlya-kriptomayninga). 19.03.2019).***

***

«Первое место среди производителей аппаратно-программных комплексов безопасности занимает Cisco. На втором, третьем и четвертом — Palo Alto Networks, Fortinet и Check Point соответственно.

Количество проданных в мире аппаратно-программных комплексов для обеспечения компьютерной безопасности: систем объединенного управления угрозами (Unified Threat Management, UTM), обнаружения и предотвращения вторжений (IDP), межсетевых экранов и прочих устройств, в четвертом квартале

2018 года выросло на 20% по сравнению с предыдущим годом и достигло почти 1,1 млн. В денежном выражении продажи поднялись на 16,7% до 4,5 млрд долл.

Самый большой вклад в рост выручки внес сегмент UTM-систем. Он вырос на 220 млн долл., что на 19,7% больше прошлогоднего, и теперь занимает 50,9% рынка. Быстро растут также сегменты устройств для обеспечения веб-безопасности (на 5,5%) и при обмене мгновенными сообщениями (18,1%). Сегменты гибридных средств и средств VPN на основе протоколов IPsec, напротив, уменьшились: на 10,4% и 20,1%.

Первое место среди производителей аппаратно-программных комплексов для обеспечения компьютерной безопасности занимает Cisco (14,1%). Palo Alto Networks все еще пытается догнать лидера (12,8% рынка). Fortinet и Check Point — третье и четвертое (9,9% и 5,5%).» ***(IDC: спрос на UTM-системы поднял рынок устройств компьютерной безопасности // «Открытые системы» (https://www.computerworld.ru/news/IDC-spros-na-UTM-sistemy-podnyal-rynok-ustroystv-kompyuternoy-bezopasnosti). 19.03.2019).***

***

«Компания Mozilla выпустила очередную версию своего браузера — Firefox 66. Помимо прочего, в релиз вошли патчи для 21 уязвимости, пять из которых — критические.

Разработчики обновили оформление и содержание страниц с предупреждениями об ошибках сертификатов. Теперь браузер сообщает пользователю о попытках злоумышленников удаленно перехватить зашифрованный трафик — уведомление отображается, если Firefox посчитает новый TLS-сертификат ненадежным или усомнится в его принадлежности к хосту, с которым установлено соединение.

Также в версии 66 добавлена поддержка технологии Windows Hello, позволяющей пользователям Windows 10 авторизоваться на сайтах через внешние ключи или функцию распознавания лиц и отпечатков пальцев.

Разработчики устранили 21 уязвимость в браузере, из которых пять — критические, семь — высокой степени опасности. В их число попала брешь CVE-2019-9790, связанная с ошибкой use-after-free, а также баги в JIT-компиляторе IonMonkey — CVE-2019-9791 и CVE-2019-9792.

Помимо того, в новой версии Firefox появилась блокировка автоматического воспроизведения звука. Эту функцию можно либо включить для всех сайтов по умолчанию, либо установить исключения для часто посещаемых ресурсов. Разработчики пообещали постепенно расширять круг пользователей, которым доступна эта настройка.

В прошлом месяце в Firefox для iOS появился постоянный приватный режим. Теперь при запуске браузера пользователи могут продолжить работу с сайтами, открытыми в ходе предыдущей сессии. Это нововведение должно упростить работу со страницами, которые им не хотелось бы хранить в истории просмотров.» ***(Egor Nashilov. В Firefox 66 устранили 21 уязвимость // Threatpost (https://threatpost.ru/execute-order-firefox-66/31946/). 22.03.2019).***

***

«Группа компаний БАКОТЕК сообщает о начале сотрудничества с CyberX, разработчиком решения в сфере промышленной кибербезопасности, а также о начале поставок продукции вендора на рынки Украины, Латвии, Литвы, Эстонии, Азербайджана, Республики Беларусь, Грузии, Армении, Казахстана, Кыргызстана, Таджикистана, Узбекистана и Туркменистана.

CyberX создала платформу по промышленной кибербезопасности от киберэкспертов с внушительным опытом защиты объектов критической инфраструктуры в сфере энергетики, систем водоснабжения, производственных предприятий, компаний транспортных перевозок, заказчиков в химической отрасли и др.

С помощью флагманского решения вендора – модуля XSense – клиенты сокращают дорогостоящие простои производства, предотвращают сбои безопасности и экологические инциденты, используют технологии машинного обучения и моделирования для обнаружения атак в реальном времени в основе продукта.

Для обеспечения целостного отображения и унифицированного управления безопасностью IT/OT заказчика, CyberX зачастую становится частью существующего оперативного центра безопасности (SOC) путем интеграции с решениями IBM Security, Splunk, Palo Alto Networks, Optiv Security, DXC Technologies и Deutsche-Telekom/ T-Systems.» ***(«Бакотек» предлагает решение CyberX для защиты критической инфраструктуры // «Компьютерное Обозрение» (https://ko.com.ua/bakotek_predlagaet_reshenie_syberx_dlya_zashhity_kriticheskoj_infrastruktury_128199). 25.03.2019).***

***

«Государственная служба специальной связи и защиты информации Украины» сертифицировала линейку решений McAfee для построения комплексных систем киберзащиты, сообщает официальный дистрибьютор решений вендора на территории Украины группа компаний БАКОТЕК.

Сертификация «Госспецсвязи» означает, что украинские государственные организации, которые уже внедрили или планируют использовать решения McAfee для повышения уровня кибербезопасности ИТ-инфраструктуры, будут полностью соответствовать требованиям госрегулятора к безопасности.

Комплекс продуктов, прошедших сертификацию, позволяет решить следующие задачи:

Защита рабочих станций (Endpoint Security);

Защита серверов (Server Security)

Оперативное обнаружение и реагирование на инциденты кибербезопасности (Endpoint Detection and Response);

Защита от скрытых и сложных угроз (Sandbox);

Защита баз данных (Database Security);

Защита от утечки конфиденциальной информации (Data Loss Prevention);

Защита от сетевых вторжений (Intrusion Prevention System);

Защита интернет-трафика (Web Gateway);

Управление событиями информационной безопасности (SIEM);

Обмен информацией об угрозах (Threat Intelligence Exchange) и пр…» ***(Комплекс решений McAfee прошел сертификацию Госспецсвязи // «Компьютерное Обозрение» (https://ko.com.ua/kompleks_reshenij_mcafee_proshel_sertifikaciyu_gosspecsvyazi_128135). 19.03.2019).***

***

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

Актуальні проблеми протидії злочинності : матеріали XVIII студент. наук. конф. з кримінології (м.Харків, 28 листоп. 2018 р.). - Харків : Право, 2018. - 194 с.

Зі змісту:

- Бойко В.О. Проблема віктимності неповнолітніх, як детермінаційна складова кіберзлочинності;
- Василенко К.О. Кримінологічна характеристика особистості кіберзлочинця;
- Вишневська І.А. Окремі аспекти латентності кіберзлочинності;
- Якубовський В.О. Проблемні аспекти протидії кіберзлочинам;
- Яскорська І. Кіберзлочинність як загроза національній безпеці України.

Шифр зберігання НБУВ: ВА828619.

***

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

Досліджено виникнення та розвиток феномену Інтернету речей. На численних прикладах з’ясовано його унікальну роль у розвитку соціуму. Наведено методологічні підходи щодо аналізу, з’ясування та формулювання правових проблем, пов’язаних із розвитком інформаційної інфраструктури Інтернету речей, застосування 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, із визначенням юридичної відповідальності тощо.

Шифр зберігання НБУВ: В357518/1.

***

Глобальні імперативи розвитку бізнесу та права : тези доп. Міжнар. наук.-практ. конф. (Київ, 15-16 листоп. 2018 р.). - Київ, 2018. - 377 с.

Зі змісту:

- Тімашов В.О., Юрченко З.-Н.А. Протидія кіберзлочинності в Україні;
- Шведова Г.Л. Інституціональні загрози об'єктам критичної інфраструктури в Україні.

Шифр зберігання НБУВ: СО36250.

***

Досудове розслідування: актуальні проблеми та шляхи їх вирішення : матеріали постійно діючого наук.-практ. семінару (м. Харків, 26 жовтня 2018 року. - Харків : Право, 2018. - Вип. 10 (ювілейний). - 304 с.

Зі змісту:

- Тарасюк А.В. Актуальні питання протидії кіберзлочинності в сучасних умовах.

Шифр зберігання НБУВ: В355392/10

***

Економіка, менеджмент і право у XXI столітті: стратегічні пріоритети розвитку : матеріали міжрегіон. наук.-практ. конф. молодих учених (Харків, 27 листоп. 2018 р.). - Харків : Право, 2018. - 158 с.

Зі змісту:

- Більченко А.Г. Кіберзлочинність: причини та форми існування.

Шифр зберігання НБУВ: ВА828617

***

Економічний і соціальний розвиток України в XXI столітті: національна візія та виклики глобалізації : зб. тез доп. 15-ї Ювіл. Міжнар. наук.-практ. конф. молодих вчених. - Тернопіль, 2018. - 276 с.

Зі змісту:

- Шевчук О.А. Аналіз загроз у комп'ютерних інформаційних системах бухгалтерського обліку (КІСБО).

Шифр зберігання НБУВ: ВА828278

***

Информационные технологии и безопасность: мат. XVIII Международной научно-практической конференции ИТБ-2019.- Киев, 2018.- 359 с.

Зі змісту:

- Яковів І., Циганюк В. Аналіз процедури оцінювання стану кібервразливості систем електропостачання;
- Цуркан О.В., Р.П.Герасимов Різновиди маніпулятивних форм використання соціальної інженерії в кіберпросторі.

Шифр зберігання НБУВ: Ж743360

***

Кальченко В.В. Огляд методів проведення тестування на проникнення для оцінки захищеності комп'ютерних систем / В.В.Кальченко // Системи управління, навігації та зв'язку. - 2018. - Вип. 4. - С. 109-114.

Проаналізовано міжнародні стандарти і керівництва з інформаційної безпеки. Розвинуто методології проведення тестування на проникнення. Наведено перелік найбільш розповсюджених міжнародних методологій проведення пентестінгу, надано їх короткий опис. Запропоновано класифікацію методологій тестування на проникнення для оцінки захищеності комп'ютерних систем.

Шифр зберігання НБУВ: Ж73223

***

Комаров М.Ю. Аналіз і дослідження моделу порушника безпеки інформації для захищеного вузла Інтернет доступу / Комаров М.Ю., Ониськова А.В., Гончар С.Ф. // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Технічні науки. - 2018. - Т. 29(68), № 5(1). - С. 138-142.

Подано загальну класифікацію порушників безпеки інформації, яка циркулює в захищеному вузлі Інтернет доступу. Приведено специфікації моделі порушника за мотивами здійснення порушень, за рівнем кваліфікації та обізнаності, за показником можливостей використання засобів для реалізації загроз, за часом дії, за місцем дії.

Шифр зберігання НБУВ: Ж70795/техн. н.

***

Право і безпека у контексті європейської та євроатлантичної інтеграції = Law and security in the context of European and Euro-Atlantic integration : зб. ст. та тез наук. повідомл. за матеріалами дискус. панелі II Харків. міжнар. юрид. форуму, м. Харків, 28 верес. 2018 р. - Харків : Право, 2018. - 188 с.

Зі змісту:

- Войціховський А.В. Кібербезпека як напрям євроатлантичної інтеграції України.

Шифр зберігання НБУВ: ВА828075

***

Сучасні напрями, засоби та методи протидії злочинності : матеріали Міжнар. конф., присвяч. 105-річчю від дня народж. видат. вченого-криміналіста, д-ра юрид. наук, проф. Віктора Павловича Колмакова, 23 листоп. 2018 р. - Одеса, 2018. - 225 с.

Зі змісту:

- Самойленко О.А. Види злочинних спільнот, що вчиняють кримінальні правопорушення з використанням кіберпростору.

Шифр зберігання НБУВ: ВА828828

***

Яковів І. Кібернетична модель APT атаки / Ігор Яковів // Information Technology and Security. - 2018. - Vol. 6, Iss. 1. - С. 46-58.

Запропоновано нову модель APT на основі кібернетичного підходу. У рамках моделі поведінку кібернетичної системи зловмисника представлено через математичний опис інформаційних процесів управляння та ітеративний взаємозв'язок між суміжними фазами кібернетичної моделі. Модель дозволяє представити кожну атаку у вигляді набору взаємопов'язаних характеристик елементарних подій на вузлах мережі інформаційно-телекомунікаційних систем.

Шифр зберігання НБУВ: Ж74190

***