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

№ 2 (лютий)

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. – №2 (лютий) . – 74 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 14
Міжнародне співробітництво у галузі кібербезпеки 17
Світові тенденції в галузі кібербезпеки 18
Сполучені Штати Америки 24
Країни ЄС 25
Китай 26
Російська Федерація та країни ЄАЕС 26
Інші країни 29
Протидія зовнішній кібернетичній агресії 31
Створення та функціонування кібервійськ 41
Кіберзахист критичної інфраструктури 42
Захист персональних даних 43
Кіберзлочинність та кібертероризм 47
Діяльність хакерів та хакерські угруповування 56
Вірусне та інше шкідливе програмне забезпечення 58
Операції правоохоронних органів та судові справи проти кіберзлочинців 61
Технічні аспекти кібербезпеки 62
Виявлені вразливості технічних засобів та програмного забезпечення 64
Технічні та програмні рішення для протидії кібернетичним загрозам 70
Нові надходження до Національної бібліотеки України імені В.І. Вернадського 72

«Украинскую социальную сеть «єСвоє», которую создатели позиционировали как первую в мире соцсеть с собственной криптовалютой и «реального конкурента Facebook», хакер-одиночка взломал на вторую неделю после её запуска в beta-версии.

Об этом говорится в постановлении Хмельницкого горрайонного суда Хмельницкой области…

Как стало известно, безработный гражданин Украины, уроженец Сургута (РФ), 8 октября 2017 года (сеть запустилась в режиме beta-версии 29 сентября 2017), обладая знаниями в области программирования и с помощью неустановленного досудебным расследованием программного обеспечения, осуществил доступ к административной панели Интернет ресурса esvoe.com, который принадлежит ООО «ИТЕРНЕТКЕШ», в результате чего получил доступ к конфиденциальной информации пользователей.

Согласно постановлению суда, злоумышленник получил полный доступ к текстовой и графической информации карточек пользователей указанной социальной сети, которые хранились во временных файлах для тестирования подключения Интернет-ресурса esvoe.com к электронным платежным системам.

– Таким образом, своими умышленными действиями мужчина совершил несанкционированное вмешательство в работу компьютерных сетей, а именно Интернет-ресурса esvoe.com, который принадлежит ООО «ИТЕРНЕТКЕШ», что привело к утечке информации, то есть уголовное преступление, предусмотренное ч. 1 ст. 361 УК Украины, – говорится в материалах дела….

В суде адвокат обвиняемого подал ходатайство о закрытии уголовного дела и освобождении обвиняемого от наказания. Защитник мотивировал ходатайство тем, что инкриминируемые обвиняемому деяния являются преступлением средней тяжести, имели место только один раз, причем больше года назад, какого-либо материального ущерба или иных убытков своими действиями он не причинил, а, следовательно, указанное деяние потеряло общественную опасность.

При принятии решения по указанному ходатайству защитник также просил учесть личность обвиняемого, который является инвалидом 3 группы с детства, положительно характеризуется, преступление совершено впервые, противоправную деятельность прекратил и способствовал следствию. Кроме того, претензий к обвиняемому не предъявили и в социальной сети, а гражданский иск не подавался.

Суд прислушался к стороне защиты и освободил обвиняемого от уголовной ответственности «в связи со сменой обстановки» и закрыл уголовное производство. Процессуальные расходы были отнесены на счет государства.» ***(Владимир Кондрашов. Суд простил хакера, который взломал украинскую социальную сеть ещё на стадии beta-версии // Internetua (http://internetua.com/sud-prostil-hakera-kotoryi-vzlomal-ukrainskuua-socialnuua-set-esxe-na-stadii-beta-versii). 04.02.2019).***

***

«Коаліція «За вільний інтернет», до якої входять медійні, правозахисні громадські організації, підготувала заяву, в якій закликає відмовитись від неправомірних обмежень інтернету та використовувати законні і прозорі способи боротьби з російською пропагандою та кібератаками.

Таким чином Коаліція відреагувала на виступ начальника Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ Олександра Климчука, який заявив, що найближчим часом указом Президента буде введено рішення РНБО про блокування ще 100 сайтів.

Також нагадується, що восени 2018 року представники Коаліції «За вільний інтернет» намагались з'ясувати, за якими критеріями складають списки сайтів/ресурсів, доступ до яких пропонується заборонити. Проте і Рада національної безпеки і оборони, і Служба безпеки України відмовили в наданні такої інформації.

Наразі в Окружному адміністративному суді міста Києва триває розгляд судової справи про порушення права на доступ до публічної інформації. Аргументів щодо відмови в наданні інформації РНБО та СБУ до суду також не надали.

Зазначимо, що «Детектору медіа» в наданні вищезгаданих критеріїв Міністерство інформаційної політики також відмовило.

Коаліція називає ефективність блокувань сайтів як способу протидії російській пропаганді «дуже сумнівною, адже відвідуваність таких сайтів українцями для отримання інформації – мізерний».

Наприклад, дослідження «Детектор медіа», яке проводилось до Указу Президента про блокування близько 200 сайтів, показало, що лише 0,5% людей використовують російські сайти і 0,1% сайти ОРДЛО для отримання інформації…

Підписанти наголошують, що наявність абсолютно непрозорого механізму обмеження інтернету – це порушення українських законів та міжнародних договорів.

Під заявою підписались:

Учасники Коаліції «За вільний Інтернет»:

Платформа прав людини

Лабораторія цифрової безпеки

Центр інформації про права людини

Кримська правозахисна група

Представництво Freedom House в Україні

Микола Костинян

А також:

Катерина Сергацкова, медіа-проект Заборона

Центр громадянських свобод

Інститут масової інформації

Детектор медіа

Ресурсний центр ГУРТ

Донецький інститут інформації

Точка опори ЮА…» ***(Правозахисники та медійники закликають СБУ припинити практики непрозорого блокування інтернету // «ДЕТЕКТОР***

МЕДІА» (https://detector.media/infospace/article/144833/2019-02-13-pravozakhisniki-ta-mediiniki-zaklikayut-sbu-pripiniti-praktiki-neprozorogo-blokuvannya-internetu/). 13.02.2019).

***

«До дня Дня безпечного інтернету Міністерство інформаційної політики України разом із «Google Україна» провели відкритий майстер-клас «Цифрові інструменти та можливості Google для безпечнішого інтернету».

Долучитися до нього можна було як онлайн, так і офлайн…

Одна з частин тренінгу складалася з опитувань. Наприклад, учасників попросили обрати, які, на їхню думку, кіберзагрози є найбільшими, звідки вони дізнаються інформацію про цифрову безпеку, чи вважають вони себе обізнаними в цій тематиці, яких головних трьох правил треба дотримуватися, щоби користуватися інтернетом безпечно… всі дані будуть уважно опрацьовані й використані для складання нових навчальних програм та майстер-класів. Їх також можна буде переглянути на сторінці Google Educator Group у соцмережах.

Так, 83,2 % учасників майстер-класу зазначили, що стикалися з кіберзагрозами. Більшість респондентів (41,4 %) оцінила свій рівень грамотності з кібербезпеки на «трієчку». Лише 5,6 % поставили собі найвищу оцінку. Основними джерелами знань про кібербезпеку учасники назвали соціальні мережі, місце роботи, ЗМІ. Також опитування показало великий запит на онлайн-курси та вебінари про цифрову безпеку, оскільки так користувачі можуть вчитися у зручний для себе час та перебуваючи в будь-якому місці.

Користувачі, які підключилися до майстер-класу, проголосували й за три найбільш ефективні, на їхню думку, поради щодо кібербезпеки: подумай, перш ніж поширити; зупинися, перш ніж завантажити; використовуй надійний пароль. Тренерка також нагадала, що важливо контролювати свої налаштування облікового запису (в Google для цього є окрема сторінка «Центр безпеки») та читати умови використання сервісів, перш ніж клацнути «ОК». Крім того, на тренінгу учасникам пояснили основи роботи з Google Classroom та іншими інструментами, наприклад хмарним сховищем даних Google Drive та поштовим сервісом Gmail.

Перша заступниця міністра інформаційної політики України Еміне Джапарова розповіла, що цей майстер-клас був спрямований у першу чергу на вчителів шкіл та викладачів університетів, щоб вони потім могли навчити безпечного користування інтернетом своїх учнів та студентів.

«Головна мета, яку ми ставили, — освітня. Одним із завдань сталого розвитку суспільства є подолання цифрового розриву між людьми. Напевно, сьогодні немає жодної людини, яка б не користувалася або не чула про інтернет. За статистикою, станом на 1 січня 2019 року у світі приблизно чотири мільярди користувачів інтернету. Дані Європейської комісії показують, що в європейських країнах 51 % не знають про кіберзлочини або не відчувають кіберзагрози. Водночас 86 % європейців вважають, що ризик стати жертвою кіберзлочинців зростає. Це дані за 2018 рік. Тобто ми сьогодні маємо ситуацію, коли зростає використання інтернету, але зростає й загроза кіберзлочинності», — прокоментувала вона.

Майстер-клас, який міністерство реалізувало за підтримки «Google Україна», є лише тестовим…

Учасники майстер-класу також отримали посібники з цифрового громадянства й безпеки «Обачність. Пильність. Захист. Ввічливість. Сміливість». Його можна й безкоштовно завантажити в мережі. Тут зібрано уроки, які вчителі можуть проходити з учнями. В них пояснюються поняття особистої інформації, цифрового сліду, конфіденційності, шахрайства в мережі, створення безпечних паролів та містяться вказівки про доброзичливість в інтернеті…» ***(Тетяна Гордієнко. День безпечного інтернету в Україні: як Мінінформполітики та «Google Україна» вчили кібербезпеки // MediaSapiens (https://ms.detector.media/web/cybersecurity/den_bezpechnogo_internetu_v_ukraini_yak_mininformpolitiki_ta_google_ukraina_vchili_kiberbezpeki/). 07.02.2019).***

***

«Антивирусные решения TrendMicro в 2018 году заблокировали в Украине более 1,44 млн вредоносных URL-адресов и свыше 1,35 млн вирусных программ. За тот же период времени наши владельцы смартфонов скачали 2,2 млн вредоносных приложений.

По данным компании, ее защитное программное обеспечение в течение прошлого года заблокировало более 48 млрд атак по целому миру. Среди них были угрозы по электронной почте, вредоносные файлы и URL-адреса. Появились также 222 новых «семейства» программ-вымогателей.

В пятерку самых вредоносных программ вошли:
криптовалютный майнер CoinMiner — 1 350 951 атак,
вымогатель WannaCry — 616 399,
Powload — 378 825,
Downad — 240 746,
Sality — 166 981.

Для банковской сферы самыми опасными остаются файловые вирусы Emotet и Ramnit. С их помощью было предпринято, соответственно, почти 133,5 попыток взлома и заблокировано 78,062 атак.

Самое вредоносное ПО для Android — это SMSreg (1 638 167 атак) и Shedun (1 345 900). Для iOS — IOS Jail Break Tool.A (397) и IOS_I Back Door.A (65).

Фишинг по-прежнему остался самой популярной и многочисленной киберугрозой в мире.

В общей сложности за год было предотвращено 41 млрд случаев. Самый высокий уровень кибератак оказался в США — там было остановлено свыше 10 млрд атак. В Китае и Бразилии количество остановленных попыток превысило 2 млрд, в Индии — 1,5 млрд.

Самым распространенным вредоносным вложением стал формат .XLS. Всего было зафиксировано 22 миллиона спам-атак. Число заблокированных URL-адресов, ссылающихся на вредоносные приложения или сайты-хостинги, превысило 1 млрд.

Среди стран, жители которых чаще всего сталкивались с вредоносными URL, лидировала Япония» (160 млн заблокированных атак), США (155 млн) и Тайвань

(73 млн). ***(Мыкола Олиярнык . Украинцы миллионами качают вредоносные приложения // ESGROUP (https://ubr.ua/ukraine-and-world/technology/ukraintsy-millionami-kachajut-vredonosnye-prilozhenija-3880364). 14.02.2019).***

***

Кібервійна проти України

«У 2018 році українські фахівці з кібербезпеки заблокували близько 400 кібератак. Про це заявив в ефірі одного з телеканалів начальник Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ Олександр Климчук…

"Загалом за 2018 рік було заблоковано близько 400 кібератак, деякі з них за своїми наслідками могли бути не менші ніж вірус Petya A. Зокрема і атака на енергетику, вірус Grey energy, який був послідовником вірусу Black energy, який ми торік заблокували"- повідомив Климчук…» ***(Анна Мурашко. У 2018 році українські фахівці заблокували близько 400 кібератак // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1779588-u-2018-rotsi-ukrayinski-fakhivtsi-zablokuvali-blizko-400-kiberatak). 12.02.2019).***

***

«Захист сайту Центральної виборчої комісії (ЦВК) від кібернетичних загроз став набагато надійніший з 2014 року, що виключає можливість зламу для фальсифікації результатів виборів. Таку думку висловив секретар комітету по нацбезпеці й обороні, народний депутат Іван Винник…

"…Моніторинг IP-адрес її активності, постійна зміна кодів захисту тощо – все організовано на абсолютно іншому якісному рівні", - зазначив нардеп.

При цьому він додав, що вважає малоймовірною можливість зламу сайту ЦВК з боку росіян.

"Можливо, будуть спричинені деякі затримки в передачі інформації, але вони будуть не критичними. Зламати ж наші сервера, викривити результат виборів, щось стерти, намалювати – я не вірю, що вони це спричинять", - наголосив Винник…» ***(Марія Мамаєва. У комітеті з нацбезпеки виключили імовірність зламу сайту ЦВК // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/exclusive/1779873-u-komiteti-z-natsbezpeki-viklyuchili-imovirnist-zlamu-saytu-tsvk). 13.02.2019).***

***

«Напередодні виборів президента 2019 в Україні посилюють заходи безпеки. Головна загроза – втручання Російської Федерації у хід перегонів.

Генерал-майор СБУ Олександр Климчук, який очолює Департамент контррозвідувального захисту інтересів держави в сфері інформаційної безпеки (ДКІБ), розповів… як спецслужби готуються до виборів та як щоденно запобігають сотням кібератак зі сторони РФ.

Інформаційний простір атакують

Виборча кампанія стартувала 1,5 місяці тому, а російські спецслужби вже намагаються вплинути на вибори.

– Ми вже фіксуємо збільшення фейкових інформаційних повідомлень, фіксуємо розгалужені мережі інтернет-агітаторів, які підпорядковуються кураторам з Росії, бачимо, що створюються нові сайти.

Так, наприклад, у грудні Службою безпеки було викрито акаунт, з якого розповсюджували фейкові повідомлення стосовно введення воєнного стану. Доведено його зв'язок з Росією.

– Олександр Климчук зазначив, що на найближче засідання РНБО Служба безпеки подала близько 100 сайтів, які використовувались російськими спецслужбами для інформаційної агресії. Відповідно, всі вони будуть заблоковані.

До речі, з 2014 року ДКІБ викрив діяльність 3500 осіб, які використовувались Росією в гібридній агресії.

Соціальні мережі – найпопулярніша платформа для дезінформації та фейків. Підтвердження тому вибори у США, коли реклама у соцмережі посприяла формуванню інтересів виборців. Відтак, Facebook нещодавно змінив правила розміщення політичної реклами. З метою запобігання зовнішньому втручанню, рекламу можуть розміщувати лише сторінки з України.

Окрім того, співпрацює з мережею і СБУ:

– Ми співпрацюємо з Facebook, Google, Twitter. Всі виявлені фейкові сторінки завчасно подаємо на розгляд керівництву Facebook для їх блокування. Цей механізм налагоджений і працює на високому рівні, – зазначив Климчук.

За словами експерта, українці за останні роки адаптувались і навчились сприймати фейкові новини.

До виборів готові

Наймасштабніша кібератака відбулась у 2017 році, коли майже всі урядові структури України були заражені так званим вірусом Petya. Ця ситуація послужила своєрідним уроком, тому тепер уряд ретельно дбає про безпеку.

– Зараз всі суб'єкти кібербезпеки в Україні – Служба безпеки України, Служба спеціального зв'язку та захисту інформації та ІТ-підрозділі всіх об'єктів критичної інфраструктури – приділяють цій ситуації дуже велику увагу і мають на озброєнні висококваліфікованих спеціалістів.

Окрім того, державні структури тепер мають відповідне технологічне оснащення для відбиття атак.

– І основне – є досвід. Наші хлопці стояли на вістрі з подолання наслідків цих кібератак, розслідували їх, і сьогодні вже навчились їх попереджати, – наголосив Олександр Климчук.

Росія працює постійно

СБУ регулярно фіксує кібератаки зі сторони Росії.

– Наші спеціалісти постійно фіксують спроби зламу тих чи інших ресурсів. Таких атак, які б привели до якихось наслідків, за цей час не було. Вони були попереджені на ранніх стадіях…

Російські атаки – складні за своєю структурою:

– Вони проходять місяцями, задіяні дуже великі ресурси – і технічні, і людські (в них можуть брати участь близько 50 хакерів одночасно). В день фіксується сотні кіберінцидентів…» ***(Лілія Ященко. Сотні масованих кібератак на день. Як Росія готується до виборів в Україні // ФАКТИ. ICTV (https://fakty.com.ua/ua/ukraine/20190213-sotni-masovanyh-kiberatak-na-den-yak-rosiya-gotuyetsya-do-vyboriv-v-ukrayini/). 13.02.2019).***

***

«В Україні фактично створені кібервійська, однак офіційно вони не проголошені. Таку думку висловив секретар комітету по нацбезпеці й обороні, народний депутат Іван Винник…

За його словами, такі підрозділи отримають належне фінансування. Крім того, як зазначив Винник, західні партнери України, зокрема США, надають широку експертну, фахову допомогу, а також надають обладнання.

При цьому він додав, що питання протидії кіберзагрозам для України набуває неабиякої актуальності у зв'язку із тим, що наразі в країні автоматизовано дуже багато процесів – від функціонування державних органів, проведення військових операцій, так і, наприклад, до подачі електроенергії в будівлі…» ***(Марія Мамаєва. Комітет нацбезпеки: в Україні фактично вже створені кібервійська // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/exclusive/1779815-komitet-natsbezpeki-v-ukrayini-faktichno-vzhe-stvoreni-kiberviyska). 13.02.2019).***

***

«МВС виділило експертів з кіберполіції, що працюють над превенцією можливих атак, які можуть вплинути на хід виборчої кампанії…

"Важливо створити систему яка протидіятиме втручанню кібератак. А якщо атака і буде — щоб вона не спричиняла катастрофічні наслідки. Ведеться активна робота з Європолом, Інтерполом, ФБР та ЦРУ, СБУ, Генпрокуратурою та Держспецзв'язком. З нашого боку — потужна кіберполіція. Існує координація між усіма органами, і вони уважно відстежують ситуацію", — розповів міністр внутрішніх справ України Арсен Аваков.

Також, у МВС створили робочу групу, завдання якої — забезпечити проведення виборчого процесу в правовому полі. Робоча група відстежує оперативну ситуацію по всій країні, перевіряє факти та передає їх до Нацполіції…» ***(Анна Мурашко. Аваков запевнив, що МВС не допустить кібератак на бази ЦВК // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1777476-avakov-zapevniv-scho-mvs-ne-dopustit-kiberatak-na-bazi-tsvk). 01.02.2019).***

***

«Невідомі хакери атакували офіційний сайт Міністерства охорони здоров'я

Через це сайт був тимчасово недоступний для користувачів. О 15:30 фахівці відновили роботу сайту…

Зараз сайт працює у звичному режимі. У відомстві вибачилися за незручності…» ***(Невідомі хакери атакували офіційний сайт Міністерства охорони здоров'я // Goodnews.ua (http://goodnews.ua/technologies/nevidomi-xakeri-atakuvali-oficijnij-sajt-ministerstva-oxoroni-zdorovya/). 15.02.2019).***

***

«СБУ передбачає збільшення кібератак РФ перед виборами президента …Служба безпеки України найближчим часом почне блокування сайтів, які запідозрить у підриві національної безпеки країни. Про це… заявив начальник департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ Олександр Климчук.

За словами Климчука, такі заходи СБУ буде робити у відповідь на інформаційні та кібератаки, у першу чергу з боку Росії. Так, в останній час СБУ фіксує групи інтернет-агітаторів, які співпрацюють з російськими кураторами та отримують від них грошову винагороду та завдання з дискредитації виборчого процесу. "Наявна у Служби безпеки інформація свідчить про те, що основний ухил російські спецслужби будуть робити на гібридну агресію: кібератаки, атаки на кібернетичний простір та об'єкти критичної інфраструктури. А також другий вектор — інформаційні впливи, фейкові новини і атаки на інформаційний простір", — заявив Климчук. За його словами, у СБУ є інформація про те, що спецслужби РФ готують потужні кібератаки напередодні і під час президентських виборів в Україні. "Вони можуть проходити не тільки на електронні системи безпосередньо Центральної виборчої комісії, а можуть атакувати будь-які об'єкти критичної інфраструктури, такі як транспорт, зв'язок, фінанси і енергетика", — зазначив Климчук. Начальник департаменту зазначив, що за останній рік було заблоковано близько 2 тис фейкових акаунтів. "Було подано для санкцій близько 200 інтернет-сайтів, які пропагували російську ідеологію. У цьому році подано ще 100 сайтів, які найближчим часом, найближчим указом президента буде введено в дію рішення РНБО і ці сайти будуть заблоковані", — додав Климчук.» ***(Росія готує масштабні кібератаки: сайти, які загрожують українській нацбезпеці, блокуватиме СБУ // Varta1 (https://varta1.com.ua/rosiya-gotuye-masshtabni-kiberataky-sajty-yaki-zagrozhuyut-ukrayinskij-natsbezpetsi-blokuvatyme-sbu-video/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+varta1news+%28VARTA1%29). 12.02.2019).***

***

«Служба реагирования на киберугрозы Украины на своей странице в Facebook сообщила, что на электронные почты украинцев стали поступать сообщения с вложением, активация которого приводит к поражению операционной системы компьютера.

Отмечается, что фишинговая рассылка осуществляется со скомпрометированного ящика государственного учреждения - gov.ua. Опасные сообщения содержат вложения, скачав и открыв которые сразу же произойдет заражение операционной системы компьютера вредоносным программным обеспечением.

Ведомство также уточнило, что такие опасные письма приходят с темой "Информация о программе Минэкономразвития". Вложение, которое после открытия начинает инфицировать операционную систему, называется "КМУ база даних.zip".

В связи с существующей угрозой заражения компьютера, сотрудники ведомства настоятельно не рекомендуют открывать вложения писем, которые кажутся подозрительными.

Кроме того, стоит обращать внимание на имя электронной почты и проверять, действительно ли этот человек отправил сообщение с зараженным вложением…» ***(Украинцам на электронную почту стали приходить письма с вирусным вложением // Телеграф (https://telegraf.com.ua/ukraina/obshhestvo/4870353-ukraintsam-na-elektronnuyu-pochtu-stali-prihodit-pisma-s-virusnyim-vlozheniem.html). 08.02.2019).***

***

«Секретар Ради національної безпеки і оборони України Олександр Турчинов заявив, що Росія збирається задіяти весь наявний арсенал включно з кібернетичними засобами для впливу на демократичне волевиявлення українського народу.

Про це повідомила прес-служба РНБО України.

В РНБО відбулося засідання Національного координаційного центру кібербезпеки, під час якого були розглянуті питання щодо стану захищеності серверів ЦВК та готовності до протидії можливим кібератакам під час виборчого процесу, проект Концепції підготовки до відбиття воєнної агресії у кіберпросторі, та інші актуальні питання кібербезпеки держави…

О. Турчинов також зазначив, що за результатами попереднього засідання Національного координаційного центру кібербезпеки Центральна виборча комісія уклала Меморандуми про співпрацю з суб'єктами забезпечення кібербезпеки, «в рамках яких виборчим комісіям надається всебічна технічна та методична допомога». У цьому контексті Секретар РНБО України відмітив злагоджену роботу ЦВК, СБУ, та Держспецзв'язку.

Окрім того, на засіданні було обговорено питання практичної міжвідомчої взаємодії, зокрема, створення на базі управління інформатизації ЦВК робочої групи, до якої увійдуть кращі фахівці СБУ та Держспецзв'язку. «Буде організовано цілодобове чергування сил та засобів кібербезпеки СБУ та ДССЗЗІ, спрямоване на виявлення, попередження та припинення будь-яких несанкціонованих дій щодо інформаційних ресурсів ЦВК», – повідомив секретар РНБО України.

Також члени Національного координаційного центру кібербезпеки заслухали розроблену Міністерством оборони України разом з Генеральним штабом Концепцію підготовки до відбиття воєнної агресії у кіберпросторі. Цей документ підготовлено в рамках реформування та розвитку сектору оборони держави, реалізації завдань щодо досягнення оперативної сумісності з НАТО, активної протидії кіберзагрозам в умовах гібридної війни, практичної імплементації Стратегії кібербезпеки та Закону України «Про основні засади забезпечення кібербезпеки».» ***(Росія задіє кіберзасоби для впливу на вибори в Україні, –***

Турчинов // Західна інформаційна корпорація (https://zik.ua/news/2019/02/19/rosiya_zadiie_kiberzasoby_dlya_vplyvu_na_vybory_v_ukraini__turchynov_1513301). 19.02.2019).

***

«Фахівці Ситуаційного центру забезпечення кібербезпеки ДКІБ СБУ у взаємодії зі співробітниками Центральної виборчої комісії попередили масштабну кібератаку на комп'ютерне обладнання, що забезпечує роботу офіційного Інтернет-сайту ЦВК.

Про це повідомляє прес-цетр С Б України.

За висновками експертів кібератака була спрямована на блокування доступу користувачів до інформації про підготовку до чергових виборів Президента України. Спеціалісти спецслужби встановили, що атаку було проведено за технологією «http flood», через генерацію постійних запитів, які ускладнювали роботу інформаційної системи та блокували можливість доступу звичайних користувачів.

Для проведення кібератаки зловмисники використовували розгалужену мережу сайтів на базі неоновленої версії системи «WordPress», що дозволило хакерам без відома власників використати їх для генерації об'ємних запитів. З метою локалізації кібератаки та усунення її негативних наслідків фахівцями здійснено низку практичних заходів, що дозволили припинити негативний вплив на роботу веб-ресурсу Центральної виборчої комісії. Фахівцями С Б України перевіряється можлива причетність до організації кібератаки російських спецслужб та підконтрольних їм хакерських угруповань. Служба безпеки України у межах компетенції постійно реалізовує комплекс вичерпних заходів з метою захисту життєво важливих інтересів, суспільства та держави від протиправного кібернетичного та інформаційного впливу спецслужб РФ.» ***(СБУ попередила масштабну кібератаку на сайт ЦВК // ТОВ «Видавничий Дім «Високий Замок» (https://wz.lviv.ua/news/385998-sbu-poperedyla-masshtabnu-kiberataku-na-sait-tsvk). 27.02.2019).***

***

«Віце-прем'єр-міністр з питань європейської та євроатлантичної інтеграції України Іванна Климпуш-Цинцадзе розповіла низці депутатів Європарламенту про посилену кібердіяльність Росії напередодні виборів в Україні.

Напередодні чиновниця зустрілася з депутатами Європейського парламенту Даріушем Росаті, Міхаелем Галером та Ельмаром Броком в Брюсселі, повідомили у офісі віце-прем'єра.

Климпуш-Цинцадзе зазначила, що Україна розраховує на активну участь міжнародних спостерігачів ОБСЄ/БДІПЛ та Європейського парламенту під час президентських виборів в Україні…

За словами Климпуш-Цинцадзе, Кремль сподівається "привести до влади в Україні проросійські політичні сили, щоб нівелювати всі позитивні зміни".» ***(Віце-прем'єр розповіла євродепутатам про посилене кібервтручання Росії //***

Mediastar (http://mediastar.net.ua.host1361643.serv39.hostland.pro/79950-vce-premyer-rozpovla-yevrodeputatam-pro-posilene-kbervtruchannya-rosyi.html). 27.02.2019).

***

«Президент Украины Петр Порошенко заявил, что Центральная избирательная комиссия 24 и 25 февраля подвергалась DDoS-атакам со стороны Российской Федерации.

Такую информацию обнародовал П.Порошенко в ходе встречи с представителями IT-индустрии во вторник в Киеве.

"В СНБО разработали механизмы защиты вместе со Службой безопасности Украины и полиции Департамент … по киберзащите Центральной избирательной комиссии совместно с нашими американскими партнерами, поскольку вчера и позавчера произошли кибератаки со стороны Российской Федерации", - сказал президент.» ***(На серверы ЦИК 24-25 февраля была совершена хакерская атака со стороны России, - Порошенко // АНТИКОР — национальный антикоррупционный портал (https://antikor.com.ua/articles/288976-na_servery_tsik_24-25_fevralja_byla_sovershena_hakerskaja_ataka_so_storony_rossii_-_poroshenko). 26.02.2019).***

***

Боротьба з кіберзлочинністю в Україні

«35-річний мешканець Київщини здійснював технічну підтримку британської біржі з онлайн обміну криптовалют. Маючи доступ, зловмисник скористався своїм становищем та викрав кошти з Bitcoin- та різноманітних Altcoin-рахунків клієнтів. Таким чином, за декілька місяців, йому вдалося заробити більше півмільйона гривень.

Заволодіння криптовалютою клієнтів відбувалося в декілька етапів. Спочатку зловмисник підбирав облікові записи клієнтів криптобіржі, які протягом тривалого часу не відвідували свої акаунти та на яких не було встановлено багатофакторної автентифікації. Після цього - правопорушник здійснював підміну резервних електронних скриньок або самостійно додавав такі скриньки до облікових записів, де резервні адреси не були зазначені. Це надавало можливість останньому пізніше відновлювати паролі доступу до гаманців та ініціювати списання електронних коштів.

Конвертація та виведення коштів відбувалося через онлайн обмінники. На даний час встановлена сума збитків, що в еквіваленті складає понад 720 тисяч гривень…

За попередньою кваліфікацією, останній, підозрюється у вчиненні правопорушення передбаченого ст. 361 Кримінального кодексу України за несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Вирішується питання, щодо

оголошення зловмиснику додаткової підозри за крадіжку коштів (ст. 185 КК України)…» ***(Кіберполіція викрила чоловіка у викраденні електронних коштів з крипто гаманців // Кіберполіція України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-cholovika-u-vykradenni-elektronnyx-koshtiv-z-kryptogamancziv-2102/). 09.02.2019).***

***

«Сотні мільйонів шахраї залучають у свої сумнівні фінансові проекти і в Україні громадяни все частіше стають їх жертвами. Зловмисники використовують схеми, за якими пропонують клієнтам швидкий та легкий заробіток. Натомість – втягують жертву у боргову кабалу. Тільки у 2018 році кіберполіція припинила діяльність 18 злочинних груп, які позиціонували свою діяльність як роботу різноманітних фінансових проектів.

Щоденний обіг на всесвітньому ринку Forex має грошовий обіг, який обліковується мільярдами доларів. Саме це і привертає увагу шахраїв. Більшість з рекламованих останнім часом проектів побудовані за принципом фінансових пірамід і не мають жодних реєстраційних документів, або мають сфальсифіковані документи.

Реклама подібних проектів відбувається виключно в мережі, оскільки цільова аудиторія шахраїв – інтернет-користувачі. При цьому, належність позитивних відгуків в мережі та на форумах не дає гарантії того, що брокеру можна довіряти.

При цьому, зазвичай шахраї використовують спеціальні програмні засоби, які створюють ілюзію торгів на реальних фінансових ринках. Використовуючи можливості SIP телефонії, які надають можливість підміни номеру, шахраї формують враження роботи офісу за кордоном. Також, для залучення іноземних інвесторів, шахраї набирають в штат іноземців, які можуть спілкуватися з клієнтами їх рідною мовою. Зазвичай, це іноземні студенти, яким пропонують нібито легальний заробіток.

Усі схеми діяльності шахраїв схожі між собою. Як приклад, вже у 2019 році кіберполіція припинила діяльність офісу, який позиціонував себе як «бінарний опціон». Зловмисники, під виглядом участі в онлайн торгах валютними парами (бінарні опціони) пропонували бажаючим отримання додаткового пасивного прибутку. Для цього необхідно було створити свій робочий онлайн кабінет на сайті «dax100.org» та зробити внесок - 100 євро.

Коли ж клієнт намагався вивести гроші, шахраї під різними приводами відмовляли в цьому та пропонували продовжити торги. Якщо клієнт відмовлявся й надалі вкладати кошти в торги, адміністрація майданчика цілеспрямовано проводила ряд операцій, що призводили до повної втрати клієнтом грошей.

Організатором даної шахрайської схеми був 36-річний мешканець Черкас. Саме він організував та підтримував роботу офісу в місті Черкаси. Штат співробітників цього офісу налічував 15 менеджерів.

Слідчі Черкаської поліції за даним фактом розпочали кримінальне провадження за ч.3 ст. 190 (шахрайство) КК України. Після отримання результатів експертизи буде вирішено питання щодо оголошення підозри. Роботу

шахрайського сайту наразі припинено. Зловмисникам загрожує до восьми років ув'язнення.

Кіберполіція звертає увагу громадян, що на сьогоднішній день подібні шахрайські схеми не є поодинокими та з кожним днем кількість жертв таких злочинних схем збільшується. Україна не є єдиною країною, де такий вид шахрайства поширюється. Ефективні методи протидії таким явищам намагаються знайти по всьому світу. Різни країни використовують сьогодні різни методи – від обмежень до заборони…» ***(Кіберполіція фіксує збільшення випадків шахрайств, вчинених під виглядом інвестування на фінансових ринках // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-fiksuje-zbilshennya-vipadkiv-shaxrajstv-vchinenix-pid-viglyadom-investuvannya-na-finansovix-rinkax/). 15.02.2019).***

***

«Сьогодні, 8 лютого, перший заступник Голови Національної поліції України В'ячеслав Аброськін нагородив двох працівників Департаменту кіберполіції за сприяння у припиненні роботи найбільшого у DarkNet майданчику з продажу зламаних серверів з конфіденційною інформацією.

Почесні відзнаки від Федерального бюро розслідувань Міністерства юстиції США отримали двоє працівників Управління протидії злочинам у сфері інформаційної безпеки Департаменту кіберполіції - Дмитро Семенюк та Ігор Аніськін…» ***(У Нацполіції нагородили кіберполіцейських за допомогу у припиненні роботи інтернет-платформи «xDedic» // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/u-naczpolicziji-nagorodili-kiberpoliczejskix-za-dopomogu-u-pripinenni-roboti-internet-platformi-xDedic/). 08.02.2019).***

***

«Мешканця Гадяцького району засудили до 4 років умовно за викрадення особистих даних з комп'ютерів за допомогою «троянських» вірусів

Октябрський райсуд Полтави виніс вирок Руслану П., який влітку минулого року інфікував комп'ютери вірусами та викрав з них особисті дані користувачів. 21 січня суддя Тетяна Січиокно засудила його до 4 років умовно та заборонила користуватися комп'ютерами…

Мешканець Гадяцького району інфікував 2500 комп'ютерів

За інформацією Департаменту кіберполіції Нацполіції України, 32-річний мешканець села у Гадяцькому районі викрадав персональні дані власників уражених комп'ютерів та займався прихованим майнінгом. Для цього він модифікував та розповсюджував шкідливе програмне забезпечення.

Відповідне кримінальне провадження правоохоронці відкрили 13 липня за:

ст.361-1 ККУ (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут);

ч.2 ст. 361 ККУ (Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж).

Руслан П. отримував доступ до ураженого комп'ютера та збирав відомості про збережені у браузері логіни, паролі, дані банківських карт, дані про гаманці криптовалют та файли з робочих столів. За оцінкою поліцейських, загальна кількість інфікованих комп'ютерів становила понад 2,5 тисячі…

Так, згідно з матеріалами справи, у квітні 2018 року Руслан П. придбав замовив хостинг сайтів у провайдера з юридичною реєстрацією на Сейшельських островах. До хостингу він підключив зареєстровані на свій нікнейм «Руслан Шторм» домени land-seo.ru, ukrmetkol.org, privatlux.ru.com та privlux.ru.

На цих сайтах він розміщував файли із «троянським» вірусом. Найімовірніше, маскував він їх під реальне програмне забезпечення. Завдяки вірусам Руслан П. втручався до даних комп'ютерів, де запускалися завантажені файли.

Так він збирав логіни та паролі, кукі (дані, які сайти зберігають на комп'ютерах відвідувачів для їх ідентифікації), дані банківських карт, автозаповнення форм у браузерах, гаманців криптовалют, файлів з робочого столу, даних про обладнання та встановлене програмного забезпечення і займався прихованим майнінгом криптовалют.

Зокрема, один з таких випадків зафіксували 22 липня, інший — 23 липня. Комп'ютери двох користувачів були уражені і стався виток особистої інформації. Одні й ті самі файли знайшли у комп'ютерах Руслана П. та двох потерпілих.

Експерти МВС проводили перевірку вірусів через безкоштовний портал VirusTotal…» ***(Дарина СИНИЦЬКА. Хакер з Гадяча, який заразив 2500 комп'ютерів, отримав 4 роки умовно // Інтернет-видання «Полтавщина» (https://poltava.to/news/50052/). 26.02.2019).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Міністр закордонних справ Павло Клімкін у четвер на міжнародній конференції з врегулювання ситуації на Близькому Сході у Варшаві, говоритиме про кібербезпеку та інформаційні війни…

"Наш досвід дуже цінується, оскільки, крім звичайних дискусій і виступів, мене попросили спеціально виступити з питань кібербезпеки та інформаційних війн. Саме наш досвід значною мірою зараз використовується тими, хто розуміє, як побудувати стратегію і як працювати тактично", - заявив Клімкін…» ***(Клімкін говоритиме про кібербезпеку на близькосхідній конференції у Варшаві // ЗаКиїв.com (http://zakyiv.com/index.php?nma=news&fla=stat&cat_id=1&nums=133110). 14.02.2019).***

***

«Офіційний Вашингтон відправляє заступника держсекретаря з питань контролю над озброєнням Андреу Томсон до Німеччини й Ізраїлю, де вона

обговорить питання кібер-безпеки, протиракетної оборони, нерозповсюдження зброї масового знищення.

Про це заявили в понеділок в Офісі речника Держдепартаменту США…

«Заступник Державного секретаря з питань контролю над озброєннями та міжнародної безпеки Андреа Томпсон перебуватиме в Німеччині й Ізраїлі впродовж 13 – 21 лютого 2019 року», – зауважили в зовнішньополітичному відомстві.

У Німеччині Томсон представить США на Мюнхенській конференції з питань безпеки. Вона обговорить питання кіберзахисту за круглим столом та візьме участь у панельній дискусії з питань контролю над озброєннями…» ***(Заступник держсекретаря США обговорить кібербезпеку в Німеччині та Ізраїлі // Західна інформаційна корпорація (https://zik.ua/news/2019/02/12/zastupnyk_derzhsekretarya_ssha_obgovoryt_kiberbezpeku_v_nimechchyni_ta_1507851). 12.02.2019***

***

«У Києві під головуванням співробітників Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ відбулося засідання Робочої групи з кібербезпеки (РГК) Організації за демократію та економічний розвиток ГУАМ.

У заході взяли участь представники спеціальних та правоохоронних органів Азербайджану, Грузії та Молдови, інформує прес-центр СБУ.

Під час засідання сторони узгодили розроблений за ініціативою української спецслужби проект Меморандуму про співробітництво країн-членів ГУАМ у сфері кібербезпеки. Також обговорено додаткові заходи щодо забезпечення регіональної безпеки у зазначеній галузі.

Представники країн-учасниць обмінялися актуальною інформацією про стан кібербезпеки, існуючі загрози та зауважили на необхідності посилення відповідної взаємодії.

Учасники заходу висловили вдячність представникам СБУ за роботу в межах РГК ГУАМ та запропонували залишити за нашою державою право країни-координатора Робочої групи на 2019-2020 роки.» ***(СБУ провела засідання робочої групи ГУАМ з кібербезпеки // Leopolis.news (http://leopolis.news/sbu-provela-zasidannya-robochoyi-grupy-guam-z-kiberbezpeky/). 04.02.2019).***

***

Світові тенденції в галузі кібербезпеки

«Независимое исследование Ponemon Institute показало, что 30% автомобильных компаний не имеют собственной программы кибербезопасности… Также выяснилось, что эти предприятия даже не нанимают сторонние организации для защиты программного обеспечения, используемого в их продуктах.

Более того, опрос показывает, что около 63% всех автомобильных компаний игнорируют тестирование уязвимостей. Менее половины программного обеспечения, оборудования и других технологий, которые они разрабатывают, остаются непроверенными.

По заказу Synopsys и SAE International в исследовании использовалась выборка из 15 900 специалистов и инженеров по ИТ-безопасности в автомобильном секторе. Чтобы удостовериться в актуальности представленных ответов, Ponemon Institute выбрал только тех респондентов, которые участвовали в оценке или содействовали обеспечению безопасности автомобильных компонентов.

…по данным исследования, 73% респондентов заявили, что они очень обеспокоены состоянием кибербезопасности автомобильных технологий. При этом только 44% сообщили, что их организации навязывают требования кибербезопасности для продуктов, предоставляемых вышестоящими поставщиками…». ***(Ирина Фоменко. Эксперты: автомобилем "без водителя" может легко управлять хакер // Internetua (http://internetua.com/eksperty-avtomobilem-bez-voditelya-mojet-legko-upravlyat-haker). 11.02.2019).***

***

«Зміни клімату розглядаються більшістю громадян у 13 країнах світу як “головна міжнародна загроза”. На це вказують результати оприлюдненого дослідження, проведеного американським науково-дослідним центром Pew Research Center. Дослідники провели опитування загалом у 26 країнах світу…

У чотирьох країнах учасники опитування визнали проблеми з кібербезпекою найбільшою загрозу для сучасного світу. Дещо по-іншому наявні на сьогодні глобальні загрози оцінили респонденти в Польщі. У цій країні опитані визнали головною небезпекою для світу Росію.

Виявилося, що “жінки в багатьох країнах Європи і Північної Америки більше стурбовані загрозами, породженими ядерною програмою Північної Кореї, глобальними змінами клімату та ІД, ніж чоловіки”. Крім того, зростає усвідомлення тієї небезпеки, яку можуть становити кібератаки, додав дослідник.» ***(Названо найбільші загрози у світі // Інформаційне агентство «1NEWS» (https://1news.com.ua/tsikave/nazvano-najbilshi-zagrozy-u-sviti.html). 11.02.2019).***

***

«…5 лютого світ відзначає День безпечного інтернету. Компанія Google в офіційному блозі звернула увагу на п’ять необхідних дій, щоб зробити перебування користувачів в мережі безпечним.

Вона також зазначає, що дані опитування у США, проведеного Google за участю Harris Poll, підтверджують: багато людей можуть не знати ці основи безпеки.

Перше, на чому наголошує Google, — треба слідкувати за оновленнями програмного забезпечення. Друге — використовувати різні паролі для декількох облікових записів.

«Двоє з трьох (65%) респондентів у нашому опитуванні заявили, що повторно використовують той самий пароль для декількох акаунтів. Але використання одного і того ж пароля для входу до декількох облікових записів збільшує ризики для безпеки. Це схоже на те, як використовувати один ключ для вашого будинку, машини та офісу — якщо хтось отримає доступ до одного, всі вони можуть бути зламані», — пише Google.

Третій крок — налаштувати номер телефону або адресу електронної пошти для відновлення доступу до акаунта та слідкувати за їхньою актуальністю. Для багатьох веб-служб, зокрема облікового запису Google, наявність опції відновлення доступу може допомогти вам повідомити про наявність підозрілої діяльності у вашому акаунті або, якщо вам потрібно заблокувати когось від використання вашого акаунту без дозволу.

Також слід налаштувати двоетапну перевірку при вході в обліковий запис. Вона значно зменшує ймовірність того, що хтось неавторизований отримає до нього доступ. Останнім кроком компанія радить пройти їхню перевірку безпеки.

Крім того, Google сьогодні представила два оновлення для безпеки даних. Перший — додаток до браузера Chrome Password Checkup. Він сигналізуватиме, коли виявить, що ваші ім’я користувача та пароль на якомусь сайті скомпрометовані.

Ще одне оновлення — перехресний захист акаунтів. «Коли ви входите до інших програм і сайтів за допомогою Google-акаунту, вони можуть бути вразливими. Перехресний захист акаунтів допомагає вирішити цю проблему. Коли програми та сайти його виконують, ми можемо надсилати їм інформацію про події, пов'язані з безпекою, щоб вони також могли захистити вас», — пише Google…» ***(Google дала п’ять порад для зміцнення вашої онлайн-безпеки // MediaSapiens (https://ms.detector.media/web/cybersecurity/google_dala_pyat_porad_dlya_zmitsnennya_vashoi_onlaynbezpeki/). 05.02.2019).***

***

«Специалисты компании Comparitech составили рейтинг стран по уровню кибербезопасности. Всего в списке присутствуют 60 стран, первое место занимает Япония, последнее — Алжир. Россия расположилась на 23 строчке, обогнав Украину (51 место) более чем на 20 позиций. При составлении рейтинга аналитики опирались на статистические показатели: количество зараженных вредоносными программами компьютеров и мобильных устройств, способность отразить различные кибератаки и актуальность законодательства относительно кибербезопасности. Подсчет велся на основании полученных каждой страной баллов. Чем больше баллов набрала страна, тем хуже все обстоит с кибербезопасностью, в итоге рейтинг имеет вид «от самого худшего к самому лучшему».

Из основных выводов специалистов можно выделить следующие: Самый высокий процент зараженных мобильных устройств был зафиксирован в Бангладеше — 35,91%. Самый высокий процент финансовых атак принадлежит Германии — 3%. Самый высокий процент заражений компьютеров — Алжир с 32,41%. Самый высокий процент атак криптомайнеров — Узбекистан с 14,23%.

Наименее подготовленная к кибератакам страна — Вьетнам с 0,245 баллами. Стоит отметить, что Украина показала наименьший показатель финансовых атак — 0,3%. Наименьшее количество зараженных мобильных устройств оказалось в Японии. А среди тех стран, которые оперативно актуализируют свое законодательство под современные киберреалии…: Франция, Китай, Россия и Германия.» ***(Олег Иванов. Россия заняла 23 место по кибербезопасности, обогнав Украину в два раза // Anti-Malware.ru (https://www.anti-malware.ru/news/2019-02-07-1447/28791). 07.02.2019).***

***

«Внедрение новых цифровых технологий сопровождается увеличением количества кибернетических рисков для бизнеса, поскольку расширяет множество уязвимостей, которыми могут воспользоваться злоумышленники. К такому выводу пришли аналитики мирового страхового и перестраховочного брокера Aon в своем Отчете о рисках кибербезопасности на 2019 год.

Интернет ресурс УкрСтрахования из материалов отчета выяснил, что, кроме технологических инноваций, высокие риски киберугроз связаны с изменением цепочки поставок и увеличением объемов оперативных данных, которыми обмениваются участники транзакций. Подобным образом растущие кибернетические риски сопровождают устройства с технологией Интернета Вещей, — отмечается в отчете.

Рассматривая ошибки сотрудников компаний, которые также повышают кибернетическую уязвимость на предприятии, авторы отчета указывают на необходимость разработки комплексного подхода к снижению внутренних рисков, включая строгое управление и внедрение эффективного доступа к данным.» ***(Кибернетическая уязвимость на предприятиях связана с внедрением технологий: отчет Aon // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/kiberneticheskaya-uyazvimost-na-predpriyatiyah-svyazana-s-vnedreniem-tehnologiy-otchet-aon). 15.02.2019).***

***

Специалисты по автомобильной кибербезопасности утверждают, автомобильные технологии, такие как Wi-Fi, Bluetooth, системы автономного управления и телематическое оборудование, открыты для взлома, в то время, как автопроизводители и поставщики уделяют недостаточно внимания предотвращению возможных электронных атак.

Отчет, основанный на опросе 593 IT-специалистов и инженеров, работающих в автомобильной промышленности, выявил ряд серьезных проблем.

Среди них:

62 % IT-специалистов и инженеров считает, что атака на продукты их компании вероятна уже в следующем году

52 процента говорит, что знают о потенциальном вреде для водителей или транспортных средств из-за «небезопасных автомобильных технологий»

62 % заявляет, что их компания не обладает достаточными навыками кибербезопасности при разработке продуктов

В компаниях, принявших участие в исследовании, в программах, связанных с кибербезопасностью, работает в среднем только девять штатных сотрудников, а 30 % респондентов заявило, что в их компании нет ни программы, ни команды по кибербезопасности.

Продукты, которые опрошенные считают наиболее вероятными для взлома:

RF-системы, такие как Wi-Fi и Bluetooth (больше всего подвержены риску по мнению 63 процента специалистов)

Телематические системы, которые регистрируют данные о скорости и местоположении (больше всего подвержены риску по мнению 60 процентов опрошенных)

Системы автономного вождения и транспортные средства (больше всего подвержены риску по мнению 58 процентов участников исследования)

Отчет составлен калифорнийской компанией-разработчиком программного обеспечения Synopsys и SAE International (Обществом инженеров автомобильной промышленности), базирующейся в США организацией по разработке стандартов.

Опрошенные в ходе исследования сотрудники говорят, что наиболее существенными причинами наличия уязвимостей программного обеспечения является отсутствие понимания проблемы руководством компаний и давление, оказываемое на них, чтобы заставить уложиться в сроки разработок. Около 69 процентов респондентов заявили, что не могут выразить свою обеспокоенность старшим сотрудникам своих компаний.

А авторы доклада «главным виновником» называют «сложную и разрозненную цепочку поставок в автомобильной промышленности», ибо в большинстве компаний-поставщиков нет авторитетной команды по кибербезопасности.

Комментируя отчет, Майк Хоус, исполнительный директор Общества автопроизводителей и трейдеров, назвал кибербезопасность «приоритетом для автомобильной промышленности» и сказал, что автопроизводители «вкладывают значительные средства в новые функции, помогающие обеспечивать безопасность автомобилей»…» ***(Анатолий Гребенюк. Исследование: современный автомобиль не защищен от кібератак // АвтоМания (https://avtomaniya.com/site/publication-full/16242). 07.02.2019).***

***

«Финтех-стартап Revolut наймет «белых хакеров», чтобы взломать и потом регулярно тестировать собственную систему безопасности…

Специалисты отдела информационной безопасности Revolut будут искать уязвимости и анализировать даркнет на предмет угроз, чтобы предотвратить возможные кибератаки и утечки данных.

Компания также планирует модернизировать свою IT-платформу, чтобы не полагаться на традиционную банковскую инфраструктуру, которую в Revolut считают ненадежной, отметили в стартапе.

Revolut ожидает, что в будущем обычные банки будут покупать финтех-стартапы, чтобы укреплять свою безопасность.

«Самый простой способ для банка — купить финтех-стартап и перевести своих клиентов на его инфраструктуру», — считает главный специлист по информационной безопасности Revolut Пол Хеффернан.

По его словам, на разработку своих решений для укрепления безопасности у крупных банков с многомиллионной базой клиентов нет времени, так как они не могут рисковать репутацией и прибылью из-за простоя…» ***(Наталья Бархатова. Revolut наймет хакеров, чтобы взломать свою систему безопасности // Rusbase (https://rb.ru/news/revolut-selfhack/). 19.02.2019).***

***

«Консалтинговая компания Frost & Sullivan составила прогноз по рынку информационной безопасности. Ожидается, к 2021 году расходы на нее в глобальном масштабе достигнут $202,3 млрд против $122,4 млрд в 2016-м. Затраты будут увеличиваться примерно на 10,6% в год.

В исследовании говорится, что крупнейшие инвестиции в кибербезопасность ожидаются в таких отраслях, как информационно-коммуникационные технологии, энергетика, здравоохранение, промышленность и финансовый сектор.

По словам аналитиков, подъему спроса на услуги и продукты в области киберзащиты способствуют растущее число предприятий, использующих концепцию Bring Your Own Device (BYOD), и набирающие популярность облачные сервисы.

Самые высокие темпы роста в Frost & Sullivan прогнозируют в таких сферах, как мобильная безопасность, обеспечение безопасности облачных хранилищ данных, анализ потенциальных угроз и профилактика кибератак.

Одним из драйверов мирового рынка кибербезопасности аналитики считают развитие и внедрение биометрических технологий, которые активно используются, например, в банковском и финансовом секторах для противодействия мошенникам и хакерским нападениям.

По словам экспертов, рост числа и характера угроз открывает возможности для выхода на него новых участников - небольших технологических компаний, специализирующихся на разработке систем и решений для конкретных задач. В результате рынок будет становиться еще более привлекательным для инвестирования.

В исследовательской компании International Data Corporation (IDC) предсказывают, что объем мирового рынка информационной безопасности в 2022 году вырастет на 45% относительно 2018-го и достигнет $133,7 млрд.

Среднегодовые темпы роста расходов на оборудование, программное обеспечение и сервисы для кибербезопасности ожидаются на уровне 9,9%.

Крупнейшей и самой быстрорастущей категорией рынка ИБ-технологий аналитики называют сервисы, продажи которых в нынешнем году будут измеряться $40,2 млрд, а в 2017-2022 годы они будут увеличиваться на 11,9% ежегодно. Наибольшим сегментом здесь станут услуги по управлению информационной безопасностью, на которые в 2022 году придется примерно половина затрат. Оставшуюся часть рынка ИБ-сервисов займут консалтинговые услуги и услуги интеграции.

По прогнозам Gartner, в 2019 году расходы компаний и потребителей на соответствующие продукты и сервисы повысятся на 8,7%, до $124 млрд.» ***(Владимир Смирнов. Мировые расходы на кибербезопасность будут расти на 10,6% в год // ChannelForIT (http://channel4it.com/publications/Mirovye-rashody-na-kiberbezopasnost-budut-rasti-na-106-v-god-33338.html#). 27.02.2019).***

***

Сполучені Штати Америки

«Державний секретар Майк Помпео заявив про те, що використання країнами Європи розробок китайської компанії Huawei може нести загрозу інформаційній безпеці Сполучених Штатів.

"Ми не збираємося ставити під удар нашу інформацію", - сказав глава дипломатії США в інтерв'ю Fox Business Network, відповідаючи на питання, чи стане американська розвідка ділитися меншою кількістю інформації з тими європейськими союзниками, які використовують технології Huawei.

Помпео звинуватив Китай в масованих кібератаках. Він додав, що таку ж активність, ведуть КНДР, Іран і Росія…» ***(Використання союзниками Huawei представляє загрозу для США – Помпео // «Дзеркало тижня. Україна» (https://dt.ua/WORLD/vikoristannya-soyuznikami-huawei-predstavlyaye-zagrozu-dlya-ssha-pompeo-303538_.html). 21.02.2019).***

***

«Венчурный фонд из США Sequoia Capital возглавил раунд финансирования стартапа по кибербезопасности Tessian (Лондон, Великобритания), который ориентирован на предотвращение доступа к персональным данным клиентов и защиту от ошибок при отправке электронной почты.

Интернет ресурс УкрСтрахование из пресс-релиза Tessian выяснил, что платформа цифровой безопасности привлекла $42 млн в рамках цикла финансирования серии B, участниками которого также выступили действующие инвесторы Balderton Capital, Accel Partners и LocalGlobe.

Технология Tessian использует машинное обучение для устранения уязвимости корпоративной электронной почты, в том числе нарушений безопасности вследствие фишинговых действий.

Алгоритм платформы состоит из анализа архивных данных электронной почты и определения контекста общения между корреспондентами. Известный характер взаимодействия людей, состоящих в переписке, позволяет автоматически обнаруживать любые аномалии, например, ошибочную отправку конфиденциального письма по другому адресу…» ***(Стартап цифровой безопасности Tessian привлек $42 млн финансирования // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/startap-tsifrovoy-bezopasnosti-tessian-privlek-42-mln-finansirovaniya). 28.02.2019).***

***

«Юридическая компания DLA Piper выпустила отчёт о нарушениях GDPR (Общего регламента по защите данных) в Европейском союзе

В новом отчёте DLA Piper приведены статистические данные о количестве нарушений в области регулирования персональных данных, о которых было сообщено регулирующим органам, о первых штрафах, наложенным в соответствии с правилами GDPR, в период с 25.05.2018 (день вступления в силу Регламента) по 28.01.2019 года (Международный день защиты данных). Общее количество зарегистрированных нарушений по части персональных данных составляет 59 000, а наложенных штрафов — 91.

Эти данные отражают ситуацию в 26 странах Европейского экономического пространства (European Economic Area, EEA), которыми были предоставлены данные о нарушениях. Однако 5 стран не опубликовали статистику уведомлений о нарушениях, а некоторые из тех, кто предоставил данные, сделали это только за часть рассматриваемого в отчете периода. Поэтому можно предположить, что представленные результаты могут быть несколько искажены. Страны, данные которых отсутствуют, это Словакия, Болгария, Хорватия, Эстония и Литва.

Согласно отчету, в тройку стран с наибольшим количеством зарегистрированных нарушений входят Нидерланды (примерно 15 400), Германия (12 600) и Великобритания (10 600). Наоборот, страны с наименьшим количеством зарегистрированных нарушений — это Лихтенштейн (15), Исландия (25) и Кипр (35)…

Гораздо менее значительно выглядят некоторые другие штрафы, упомянутые в отчете. Например, один из первых штрафов GDPR был наложен в Австрии в размере 4 800 евро за неправильно маркированную камеру видеонаблюдения. Кипр сообщил о 4 штрафах (из 35 уведомлений о нарушениях) на общую сумму 11 500 евро. Цифры на Мальте интересны — сообщается о 17 штрафах, которые можно считать высоким результатом для населения страны с менее чем полумиллиона жителей…

Ближе к финалу отчет поднимает еще один интересный вопрос. В нем упоминаются комментарии некоторых юридических представителей в Германии, утверждающих, что применение принципов законодательства ЕС о конкуренции для расчета штрафов по GDPR может привести к нарушению принципов законности и соразмерности уголовных преступлений и наказаний в соответствии с Хартией Европейского союза по правам человека. Разумное решение этой проблемы — местные процедурные правила, а не стандартизированные. Это приведет к уменьшению штрафов…» ***(Европейский регламент по защите данных был нарушен около 60 тысяч раз // РосКомСвобода (https://roskomsvoboda.org/44941/). 10.02.2019).***

***

«Крупнейший производитель телекоммуникационного оборудования китайская компания Huawei предлагает построить в Польше, где недавно власти арестовали ее бывшего сотрудника по обвинению в шпионаже, центр кибербезопасности. Об этом сообщил глава польского подразделения Huawei Тонни Бао (Tonny Bao).

На недавней пресс-конференции он отметил: «Мы [компания Huawei] готовы построить центр кибербезопасности в Польше, если власти примут это как решение о доверии».

Huawei уже создала лаборатории информационной безопасности в Германии и Великобритании, чтобы повысить уверенность в том, что ее оборудование не содержит, так называемых back doors «черного входа» для китайских спецслужб.

Правительство Польши намерено исключить оборудование Huawei из своей будущей сети 5G, из-за опасений, впервые высказанных США, о том, что технологии Huawei могут использоваться китайскими спецслужбами для шпионажа.

Региональный директор по связям с общественностью Huawei Остин Чжан (Austin Zhang) сказал, что у польского правительства нет оснований исключать китайскую компанию из проектов развития сети 5G. «Если это все же произойдет… мы приложим все усилия для защиты нашего бизнеса и репутации в Польше», — сказал Чжан.» ***(Антон. Huawei предлагает построить центр кибербезопасности в Польше // Droidbug.com (https://droidbug.com/huawei-predlagaet-postroit-tsentr-kiberbezopasnosti-v-polshe/). 07.02.2019).***

***

«Росія має намір тимчасово відключитися від Інтернету в рамках підготовки до потенційної кібервійни в майбутньому…

Тестове відключення інтернету, яке повинно пройти до квітня цього року, покаже, що передача даних між організаціями і громадянами Росії, залишаються всередині країни, а не направляються в інші країни.

Так, в минулому році в російський парламент був внесений законопроект, що пропонує технічні зміни, необхідні для того, щоб російський інтернет працював самостійно.

Повідомляється, що 1 квітня був встановлений крайній термін для подання поправок до законопроекту під назвою Національна програма "Цифрова економіка Російської Федерації", проте, як повідомляється, терміни проведення випробувань ще не визначені.

Відповідно до закону, російські інтернет-провайдери повинні будуть забезпечити незалежність інтернет-простору Рунету, якщо іноземні держави спробують ізолювати націю в Інтернеті…» ***(Саша Картер. Росія планує відключити весь інтернет в рамках підготовки до кібервійни – BBC //***

Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1779471-rosiya-planuye-vidklyuchiti-ves-internet-v-ramkakh-pidgotovki-do-kiberviyni-bbc). 11.02.2019).

***

«Зампред Банка России Дмитрий Скобелкин… рассказал о результатах, к которым привели изменения в законе «О национальной платежной системе». Согласно последним, банки обязаны возвращать клиенту списанную киберпреступниками сумму, если тот сообщил о пропаже денег не позже чем через день после инцидента. Также поправки расширили требования к отчетности о кибератаках для финансовых организаций: теперь они обязаны сообщать о сумме возмещенных средств.

По словам Скобелкина, первая отчетность, составленная по новым требованиям, показала, что вкладчики стали лучше защищены от потери денег в результате киберпреступлений…

Причиной для принятия поправок к закону стал рост активности кибермошенников. По данным Генпрокуратуры, в 2018 году число инцидентов, подпадающих под ст. 159.3 УК РФ «Мошеннические действия, совершенные с использованием электронных средств платежа», увеличилось в семь раз…» ***(Egor Nashilov. Россиянам вернули украденные кибермошенниками деньги // Threatpost (https://threatpost.ru/banks-in-russia-return-230-mln-rubles-to-cybercrooks-victims/31108/). 13.02.2019).***

***

«Государственная дума приняла в первом чтении закон о защите рунета. За документ проголосовали 334 депутата, против – 47. Сразу отметим, что закон не грозит отключением от мировой сети. Так, в документе говорится, что необходимо обеспечить устойчивую работу российского сегмента интернета, в случае отключения РФ от всемирной сети другими странами.

Ранее документ вызвал широкий резонанс в обществе. Кроме того в Госдуме говорили о дополнительной нагрузке на федеральный бюджет. В ближайшие три года, в целях защиты рунета от внешних угроз, потребуется потратить около 2 миллиардов рублей.

Некоторые положения законопроекта требуют корректировки, что будет сделано во втором чтении. По словам директора проекта Роскомсвобода Станислава Шакирова, этот законопроект позволит властям при необходимости отключить «внешний интернет» и фильтровать трафик – как внутренний, так и внешний.

Проект является ответом на американскую стратегию национальной кибербезопасности, где Россию назвали одной из стран-организаторов хакерских атак. Противники инициативы, среди которых неправительственные организации и оппозиционные силы, называют ее «законопроектом об изоляции российского интернета». ***(Александр Лазарчук. В России приняли закон об автономности ренета // MobiDevices (https://mobidevices.ru/russias-autonomous-internet). 12.02.2019).***

***

«Крупнейшие операторы связи России намерены провести учения, в ходе которых проверят на практике возможность применения закона «о суверенном интернете», внесенного в декабре в ГосДуму сенатором Андреем Клишасом.

Такое решение… было принято на заседании рабочей группы «Информационная безопасность», реализующей национальный проект «Цифровая экономика».

В учениях примут участие «МегаФон», «ВымпелКом» (бренд «Билайн»), МТС, «Ростелеком» - вместе они попробуют понять, как именно следует проводить задуманную интернет-реформу.

Закон, напомним, требует, чтобы весь трафик внутри России проходил через точки обмена, одобренные Роскомназдором. Для этого мобильные операторы и интернет-провайдеры должны установить на своих сетях оборудование, с помощью которого РКН сможет вмешиваться в потоки трафика, а также блокировать запрещенные в РФ ресурсы.

Проект также требует минимизировать «передачу за рубеж данных, которыми обмениваются между собой российские пользователи» и обеспечить возможность автономной работы рунета.

«Все участники обсуждения сходятся в том, что у него благие цели, но механизмы его реализации вызывают много вопросов и споров. Тем более, способы его реализации пока точно не прописаны, - заявила глава рабочей группы Наталья Касперская. - Поэтому пришли к тому, что участникам рынка надо организовать учения или что-то подобное, чтобы понять, как это все может быть реализовано на практике»…

Правительство также в целом одобрило инициативу, хотя и с оговорками: во-первых, на ее реализацию нужно предусмотреть деньги в бюджете (Клишас утверждал, что средства налогоплательщиков не потребуются), а во-вторых, четко прописать в законе, что именно является угрозой безопасности и в каких случаях может осуществляться централизованное управление сетью.

К хвалебным отзывам присоединились национальные интернет-гиганты в лице «Яндекс» и Mail.ru Group.

Технический директор Mail.ru Group заявил, что закон позволит интернет-компаниям «чувствовать себя более спокойно», а директор по развитию сетевой инфраструктуры «Яндекса» Алексей Соколов отметил своевременную «защиту российского сегмента сети интернет».

Из госструктур отрицательный отзыв дала лишь Счетная палата. «Реализация законопроекта потребует дополнительных расходов федерального бюджета. Кроме того, реализация законопроекта приведет к росту стоимости товаров и услуг на российском рынке, что содержит риск увеличения расходов бюджетов всех уровней бюджетной системы РФ на их оплату», - отмечается в отзыве СП.» ***(В России проведут учения по отключению от глобального интернета // finanz.ru (https://www.finanz.ru/novosti/aktsii/v-rossii-provedut-ucheniya-po-otklyucheniyu-ot-globalnogo-interneta-1027937958). 09.02.2019).***

***

«Экс-сотрудник Центра информационной безопасности ФСБ Сергей Михайлов и бывший топ-менеджер "Лаборатории Касперского" Руслан Стоянов приговорены к 22 и 14 годам лишения свободы соответственно по делу о госизмене. По данным СМИ, они могли быть причастны к передаче данных о российских хакерах США.

Заседание Московского окружного военного суда проходило в закрытом режиме.

Ранее адвокат Михайлова Руслан Голенков сообщил Русской службе Би-би-си, что обвинение запросило для его подзащитного 23 года лишения свободы.

Адвокат Стоянова Александр Гусак сообщил Би-би-си, что в своем последнем слове его подзащитный назвал себя истинным патриотом России и вину в госизмене не признал. Михайлов, по словам защитника, заявил то же самое…

До ареста в декабре 2016 года полковник ФСБ Михайлов руководил 2-м управлением Центра информационной безопасности (ЦИБ) ФСБ и считался одним из главных специалистов по киберпреступности в российских спецслужбах.

Стоянов возглавлял отдел расследования киберинцидентов Лаборатории Касперского и отвечал за связь компании с правоохранительными органами.

По этому же делу были арестованы подчиненный Михайлова, офицер ЦИБ ФСБ Дмитрий Докучаев и интернет-предприниматель Георгий Фомченков.

Суть предъявленных им обвинений доподлинно неизвестна, поскольку материалы дела составляют государственную тайну.

По данным СМИ, в материалах говорится, что в 2011 году Михайлов через цепочку посредников передал ФБР сведения об оперативно-розыскной деятельности по делу основателя процессинговой компании Chronopay Павла Врублевского, которого в США считают киберпреступником. К выполнению этой задачи, по версии следствия, их привлек Фомченков.

При этом, как сообщал ряд СМИ, Михайлов, Стоянов, Докучаев и Фомченков могли быть причастны к утечке данных об атаках на сервера американских демократов перед президентскими выборами в 2016 году…». ***(Борец с хакерами из ФСБ получил 22 года за госизмену // Русская служба BBC (https://www.bbc.com/russian/news-47367728) 26/02/2019)***

***

Інші країни

«Агенты, работающие под прикрытием, пытались дискредитировать израильскую компанию по кибербразведке NSO Group…

Программное обеспечение для взлома смартфонов от NSO Group якобы помогло Саудовской Аравии отследить и убить журналиста Джамаля Хашогги. Мексика использовала то же ПО для наблюдения за правозащитниками и критиками правительства.

Шесть человек, вовлеченных в тайные операции, считают, что действия были попыткой получить информацию, которая может быть использована для их дискредитации. Среди них два эксперта по кибербезопасности, занимающиеся исследованием программного обеспечения NSO, три юриста, ведущие судебные процессы против NSO Израиле на Кипре, и журналист из Лондона, написавший о судебном процессе.

Журналист и адвокат согласились на встречи, которые были тайно записаны. Видео транслировалось по израильскому телевидению. "Оперативники искали грязь и неуместную информацию о вовлеченных людях", - прокомментировал адвокат Мазен Масри.

Один из исследователей попросил Associated Press записать на видео встречу. Он был опознан как Аарон Алмог-Ассулин, бывший сотрудник израильской службы безопасности.

Согласно докладу Ронана Фэрроу, опубликованному в 2018 году в журнале New Yorker, эта тактика схожа на ту, что и с Харви Вайнштейном, которого заставили замолчать и дискредитировать женщин, обвиняющих его в сексуальном насилии.

Международная частная разведывательно-аналитическая компания Black Cube описывает себя как "избранную группу ветеранов из элитных разведывательных подразделений Израиля, которая специализируется на индивидуальных решениях сложных деловых и судебных задач".» ***(Ирина Фоменко. Шпионы пытались дискредитировать израильскую компанию по киберразведке // Internetua (http://internetua.com/shpiony-pytalis-diskreditirovat-izrailskuyu-kompaniyu-po-kiberrazvedke). 12.02.2019).***

***

«В Израиле запустили горячую линию, чтобы помогать частным лицам и крупным корпорациям предотвращать взломы личных страниц и сайтов.

Данную линию открыл директор Израильского центра реагирования на компьютерные инциденты Лейви Штохамер. Она работает по номеру 119.

Штохамер говорит, что кибератака не может быть ограничена только материальным ущербом. Это также может угрожать жизни. И главная задача данной линии заключается в том, чтобы как можно быстрее узнать об угрозах, предотвратить их и поделиться с людьми информацией, чтобы в дальнейшем избежать попытки взлома.

Штохамер утверждает, что с момента открытия данной линии к ним обращается более 100 человек в день. Многие из них действительно стали жертвами киберпреступников, а часть обращений - это ложные извещения.» ***(Новая горячая линия Израиля готова помочь взломанным // Jewishnews (https://jewishnews.com.ua/society/novaya-goryachaya-liniya-izrailya-gotova-pomoch-vzlomannyim). 18.02.2019).***

***

«…уряд Швейцарії запрошує хакерів випробувати свої сили у зламі нової системи електронного голосування країни. Таким чином влада планує випробувати її захист.

«Вони можуть намагатися маніпулювати голосами, зчитувати дані бюлетенів, порушувати таємницю голосування, виводити з ладу чи обходити системи безпеки, що працюють на захист голосів виборців», — заохочує до дій уряд.

Сума винагороди за втручання в хід голосування буде залежати від глибини маніпуляції. Найбільшу суму — 45 тис. євро — отримає той, хто зможе непомітно зманіпулювати голосуванням. Порушення таємниці волевиявлення оцінюють у 8,8 тис. євро, а знищення електронної урни — у 4,4 тис. Всього на винагороду хакерам передбачено 132 тис. євро…» ***(Швейцарія заплатить винагороду тим, хто зламає її систему електронного голосування // MediaSapiens (https://ms.detector.media/web/cybersecurity/shveytsariya_zaplatit_vinagorodu_tim_khto_zlamae_ii_sistemu_elektronnogo_golosuvannya/). 08.02.2019).***

***

Протидія зовнішній кібернетичній агресії

«Європейський союз розробив нові санкції за кібератаки… Брюссель має намір вводити проти іноземних юридичних і фізичних осіб, які відповідають за витік даних, крадіжку інтелектуальної власності, атаки на ІТ-інфраструктуру і викрадення секретної інформації.

…представники 28 країн ЄС проведуть 8 лютого, зустріч в Брюсселі з метою обговорення питань розширення режиму санкцій. Це відбувається на тлі зростання тривоги по передбачуваної китайської і російської діяльності…» ***(Євросоюз розробив нові санкції за крадіжку інтелектуальної власності // Інформаційне агентство «Українські Національні Новини» (http://ipexpert.org.ua/novini/yevrosoyuz-rozrobyv-novi-sanktsiyi-za-kradizhku-intelektualnoyi-vlasnosti/). 08.02.2019).***

***

«Бронетранспортеры США Stryker Dragoon, которые больше года назад прибыли в Европу, страдают уязвимостью перед хакерскими атаками, сообщил Пентагон в докладе.

Как сообщили в военном ведомстве США, «кибератаки продемонстрировали способность ухудшить некоторые возможности БТР в условиях оспариваемой киберсреды», пишет «Российская газета»…

Подробности не раскрываются, но вероятно, имеются в виду проблемы, возникающие в процессах обмена данными, навигации и цифровых коммуникаций.

Уязвимыми перед кибератаками оказались и стандартные M1126 Stryker, и модернизированные M1256.

Кроме того, если уязвимости выявлены не в самих БТР, а в сетях, где работают их бортовые системы, угроза может распространяться и на другую бронетехнику.

Drive отмечает, что не сообщается, кто именно атаковал БТР. Речь идет о неуказанных «противниках» – так американцы уже обозначали предполагаемых «российских хакеров», но это же обозначение может использоваться и для условного противника в ходе учений.

Напомним, СМИ сообщали, что бронетехнику США, включая Stryker, в Европе преследуют неудачи.» ***(Антон Антонов. Хакеры взломали американские БТР // Деловая газета «Взгляд» (https://vz.ru/news/2019/2/13/963953.html). 13.02.2019).***

***

«Італія пропонує НАТО змінити принцип розрахунку витрат на оборону. У Римі вважають, до таких видатків мають належати фінансування кібербезпеки і захист енергетичної інфраструктури.

…ці чинники не менш важливі, ніж купівля танків. Вони безпосередньо пов'язані з обороною, але разом із тим не входять в оборонний бюджет…» ***(Італія пропонує змінити принцип розрахунку витрат на оборону // ООО "Национальные информационные системы" (http://podrobnosti.ua/2282905-talja-proponu-zmniti-printsip-rozrahunku-vitrat-na-oboronu.html). 12.02.2019).***

***

«Росія не сходить зі шляху порушення міжнародних стандартів і норм – зокрема, від її кібератак не застрахований ніхто. Однак якщо Кремль вирішить розпочати в Україні наступальні воєнні дії, то зробить велику помилку.

Передбачити дії кремля у цьому контексті неможливо, сказав екс-держсекретар США Джон Керрі…

Окрім того, Керрі зазначив, що зараз ніхто не застрахований від російських кібератак "і Україна в цьому році стане їх головною ціллю".

За словами екс-держсекретаря, неприємні та трагічні події в Азовському морі довели, що "Росія обрала шлях порушення міжнародних стандартів і норм".

Тому міжнародне співтовариство повинне вийти і пояснити, що така поведінка Росії неприпустимо. І моя надія, звичайно, на те, що ситуацію вдасться розрядити, моряки і суду зможуть повернутися додому,– додав він…» ***("Ніхто не застрахований": екс-держсек США про загрози з боку Росії та можливий наступ на Україну // Телеканал новин «24» (https://24tv.ua/nihto_ne_zastrahovaniy_eks_derzhsek_ssha_pro_zagrozi_z_boku_rosi_ta_mozhliviy_nastup_na_ukrayinu_n1113721?utm_source=rss). 17.02.2019).***

***

«Відкриваючи нову штаб-квартиру німецької розвідки в Берліні, канцлерка Німеччини Анґела Меркель назвала основні загрози й наголосила, що країна, як ніколи до цього, потребує сильної і дієздатної розвідслужби.

Федеральна розвідувальна служба Німеччини (BND) відіграє важливу роль у захисті країни від кіберзагроз та дезінформаційних кампаній. Про це заявила канцлерка Німеччини Анґела Меркель (Angela Merkel), виступаючи на церемонії відкриття нової штаб-квартири BND у Берліні в п'ятницю, 8 лютого, повідомляє агенція AFP.

За словами канцлерки, сьогодні багато країн ведуть досить активні гібридні війни. "І на цьому напрямку ми потребуємо сильної розвідслужби, яка зможе своєчасно проаналізувати і попередити про кіберзагрози, що надходять з-за кордону", - підкреслила Меркель.

Особливу увагу очільниця уряду ФРН приділила також боротьбі проти дезінформації. "Ми повинні навчитися поводитися з фейковими новинами, як зі складовою частиною гібридної війни", - зазначила вона, нагадавши, що найчастіше за подібними повідомленнями стоїть цілеспрямована державна пропаганда. На думку канцлерки, BND відводитися особлива роль на цьому напрямку. Спецслужба повинна аналізувати, хто стоїть за подібними пропагандистськими атаками. Це, за її словами, особливо актуально незадовго до виборів до Європарламенту…» ***(Наталія Мехед. Меркель наголосила на ролі розвідки у захисті від кіберзагроз і дезінформації // Deutsche Welle (https://www.dw.com/uk/%D0%BC%D0%B5%D1%80%D0%BA%D0%B5%D0%BB%D1%8C-%D0%BD%D0%B0%D0%B3%D0%BE%D0%BB%D0%BE%D1%81%D0%B8%D0%BB%D0%B0-%D0%BD%D0%B0-%D1%80%D0%BE%D0%BB%D1%96-%D1%80%D0%BE%D0%B7%D0%B2%D1%96%D0%B4%D0%BA%D0%B8-%D1%83-%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%96-%D0%B2%D1%96%D0%B4-%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%B0%D0%B3%D1%80%D0%BE%D0%B7-%D1%96-%D0%B4%D0%B5%D0%B7%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97/a-47433577). 08.02.2019).***

***

«Министры обороны Североатлантического альянса на своей встрече в Брюсселе 13-14 февраля затронут кибербезопасность в рамках обсуждения вопроса сдерживания и обороны, заявил генеральный секретарь НАТО Йенс Столтенберг.

"Кибербезопасность является частью этого процесса. У нас не будет отдельного заседания по кибербезопасности, но это вписывается в общую дискуссию", — объяснил Й.Столтенберг, отвечая на соответствующий вопрос на пресс-конференции во вторник в Брюсселе.

По его словам, одной из проблем, которую приходится решать, является "установление источников кибернападений".

"Мы должны иметь возможность определять эти источники, и нам нужно договориться о процессе. Так что кибербезопасность будет обсуждаться. Это как раз вписывается в укрепление нашей готовности вот уже несколько лет", — объяснил Й.Столтенберг.

"Мы активизировали наши системы по кибербезопасности. Мы взяли обязательства по обеспечению кибербезопасности. Все страны (НАТО — ИФ) должны укреплять свой потенциал в этой области. Мы обмениваемся передовым опытом. Мы провели крупнейшие в мире учения в Эстонии, и будем продолжать учения, повышение готовности, улучшение осведомленности, чтобы лучше распознавать киберугрозы, исходящие из разных источников и направлений", — сообщил глава Североатлантического альянса.» ***(Министры обороны НАТО обсудят кибербезопасность как важную составляющую сдерживания и обороны // Goodnews.ua (http://goodnews.ua/politics/ministry-oborony-nato-obsudyat-kiberbezopasnost-kak-vazhnuyu-sostavlyayushhuyu-sderzhivaniya-i-oborony/). 12.02.2019).***

***

«Любой человек, получивший доступ к СПРН, может включить сирену или вовсе отключить функцию оповещения об авиационном ударе.

Более года назад Иран осуществил попытку взломать израильские системы предупреждения о ракетном нападении (СПРН). Об этом сообщил командующий Подразделением киберзащиты Армии обороны Израиля Ноам Шаар изданию Israel Hayom.

СПРН является одним из наиболее чувствительных элементов гражданской и военной инфраструктуры Израиля. Любой человек, получивший к ней доступ, может по своему усмотрению включить сирену или вовсе отключить функцию оповещения об авиационном ударе.

По словам Шаара, его подразделению удалось успешно отразить кибератаку, тем самым избежав возможных катастрофических последствий. Предотвратить инцидент удалось благодаря непрерывному мониторингу активности иранской хакерской группировки – одной из десятка группировок, работающих на Корпус стражей исламской революции.

Помимо СПРН, хакеры пытались взломать еще ряд компьютерных систем в Израиле. Как сообщил Шаар, Иран непрерывно атакует израильские системы, как военные, так и гражданские. В общей сложности Подразделение киберзащиты отразило порядка 130 кибератак, большая часть из которых осуществлялась из Ирана…» ***(Иран пытался атаковать израильские системы предупреждения о ракетном нападении // SecurityLab.ru (https://www.securitylab.ru/news/497856.php). 10.02.2019).***

***

«В США внесли в санкционные списки две иранские организации, восемь связанных с ними физических лиц из Ирана и еще одного гражданина этой страны за причастность к деятельности Корпуса стражей исламской революции (КСИР, элитные части ВС Ирана). Об этом говорится в сообщении Министерства финансов США.

"Министерство финансов предпринимает меры против иранских лиц, действующих в киберпространстве и осуществляющих операции под прикрытием, направленные против американцев на их родине и за рубежом. Эти меры приняты в

рамках усилий по противодействию кибератакам иранского режима", - заявил министр финансов Стивен Мнучина.

Одна из попавших под санкции организаций New Horizon Organization оказывала поддержку КСИР и "проводила международные конференции, которые являлись для иранских разведчиков площадкой для вербовки людей и сбора разведданных у участников этих мероприятий".

Вторая организация Net Peygard Samavat Company, предпринимала попытки внедрения вирусов в компьютерные системы действующих и бывших агентов контрразведки США.» ***(Из-за кибератак Ирана США расширили список санкций // ФОКУС (https://focus.ua/world/420551-izza-kiberatak-irana-ssha-rasshirili-spisok-sankcij.html). 13.02.2019).***

***

«…APT-группировка Fancy Bear (другие названия Strontium и APT28) атаковала Центр стратегических и международных исследований в Вашингтоне.

…суд штата Вирджиния передал специалистам Microsoft контроль над несколькими принадлежащими группировке доменами под общим названием «Strontium Domains» (LOGIN-CSIS.ORG, CSIS.EVENTS, CSIS.EXCHANGE и CSIS.CLOUD). Согласно материалам суда, сайты представляли собой поддельные страницы авторизации во внутренних системах Центра и могли использоваться преступниками для похищения учетных данных и целенаправленного фишинга…» ***(Fancy Bear атаковала американский «мозговой центр» // SecurityLab.ru (https://www.securitylab.ru/news/497728.php). 01.02.2019).***

***

«Нет причин сомневаться в том, что выборы в Европейский парламент (ЕП) станут целью хакерских атак, дезинформационных кампаний и попыток манипулирования в социальных сетях: ретроспективный взгляд позволяет четко реконструировать, что со времен президентских выборов в США в 2016 году любое крупное политическое событие в Европе сопровождается попытками манипулирования в киберпространстве. Начиная с референдума о выходе Великобритании из ЕС, продолжая президентскими выборами во Франции и заканчивая неоднозначным народным голосованием по поводу независимости Каталонии – в течение всего этого периода разным аналитическим центрам, неправительственным организациям и государственным деятелям удавалось фиксировать попытки и реальное осуществление дезинформационных кампаний и кибератак в разных уголках Европы…

В декабре прошлого года в Бельгии даже распалась правительственная коалиция из-за разногласий вокруг миграционного пакта ООН, которые в значительной мере были раскручены ультраправыми движениями через социальные сети. Потому нет ничего удивительного в том, что, согласно данным одного из последних опросов Евробарометра, три четверти всех европейцев обеспокоены дезинформацией в Сети.

Главы европейских государств и правительств – в качестве реакции на современные угрозы из киберпространства – придали огромное значение данной теме в декларации Европейского совета, принятой в октябре 2018 года. Вскоре после этого Европейская комиссия представила новый план действий, в котором содержатся конкретные предложения по обеспечению безопасности выборов. В действительности же принятые (и не принятые) до сего дня меры недооценивают характер общеевропейских выборов, которые сегодня угрожают превратиться в пиршество для агрессоров из виртуального закулисья. При этом три основных фактора на порядок усиливают реальный размах кибератак в рамках общеевропейских выборов по сравнению с национальными волеизъявлениями избирателей и придают особый резонанс нынешним дискуссиям о теневых сторонах цифровой демократии в контексте ЕС. Одно из важнейших первоочередных различий обнаруживается уже при взгляде на партийно-политическую ситуацию на европейском континенте. Правее центральной точки политического спектра с нарастающей интенсивностью формируются евроскептические партии, заявленная цель которых состоит в ослаблении ЕС. Именно эти силы уже используют в рамках национальных выборов и референдумов социальные медиа в качестве ключевого инструмента манипуляции общественным мнением и не брезгуют при этом даже целенаправленными дезинформационными кампаниями и фейковыми новостями, как это, к примеру, имело место в рамках избирательной борьбы за кресла в бундестаге…

Особое значение приобретает сетевое сходство антиевропейских сил в свете актуальных объединительных устремлений в правом лагере, в рамках которых лидер итальянских правых популистов Сальвини добивается создания альянса между самыми разнообразными евроскептическими партиями. Если бы такому союзу действительно посчастливилось состояться, то за счет этого в масштабах всей Европы возникла бы агрессивная ось в виртуальном пространстве. Тогда бы – в отличие от национальных выборов – результаты самых разных национальных и националистических кампаний в киберпространстве слились бы в конце мая в единый итог выборов, который мог бы поспособствовать значительному расширению присутствия в ЕП объединенных антиевропейских сил.

Во время выборов в Европейский парламент наряду с национальными действующими лицами особое значение для процессов в киберпространстве вполне может приобрести некий внеевропейский игрок. Россия в недавнем прошлом неоднократно пыталась оказывать влияние на выборы в Европе – как посредством фейковых новостей, так и посредством целенаправленного использования ботов в социальных сетях, а также знаменитой фабрики троллей из Санкт-Петербурга. При этом данное намерение Кремля демонстрирует коварное совпадение интересов с текущими целями антиевропейских сил: длительная дестабилизация Европейского союза как единого целого. Как следствие, Москва оказывает в том числе и финансовую поддержку евроскептическим партиям по всей Европе. Упомянутая принципиальная разница между волеизъявлениями избирателей на национальном уровне и выборами в Европейский парламент приобретет впоследствии взрывоопасный характер, поскольку за счет этого ключевые фигуры виртуального пространства больше не будут использовать выборы в мае 2019 года только для

классического определения курса за или против той или иной политической повестки дня (например, за или против повышения размеров минимальной зарплаты), а подадут их под соусом выбора за или против ЕС как единого целого – немыслимый процесс на национальном уровне…

Более того, в рамках выборов в ЕП этот мрачный сценарий потенциальных угроз наталкивается на все еще слабо консолидированную линию обороны, которая представляет собой второе базовое отличие от национальных выборов. Ключевой аспект при этом заключается в характере грядущих выборов: вместо одного тура голосования выборы в Европейский парламент охватывают более длительный временной отрезок с 23 до 26 мая и одновременно проходят в формате национальных выборов в 27 (или 28) государствах – членах ЕС. Тем самым на плечи каждого из этих государств – членов ЕС ложится в том числе и ответственность за защиту избирательной инфраструктуры от кибератак, однако их меры предосторожности воплощаются в жизнь с разной интенсивностью. Эта фрагментированная структура национальных мер безопасности в сочетании со сравнительно долгой длительностью голосования открывает широкий диапазон возможностей для атак из виртуального пространства. Осознавая свое бессилие в этом отношении, европейский комиссар по вопросам юстиции, защиты прав потребителей и гендерного равенства назвала лоскутным ковриком те меры, которые государства – члены ЕС приняли на текущий момент. При этом мало хорошего сулит и тот факт, что даже в Германии во время выборов в бундестаг в 2017 году удалось провести хакерскую атаку на главный программный комплекс, который передавал результаты выборов председателю Федеральной избирательной комиссии.

Третий и последний решающий фактор проистекает из результатов будущих выборов. Если, с одной стороны, дезинформационные кампании или автоматизированное распространение фейковых новостей в социальных медиа будут иметь успешный результат, то антиевропейские силы смогут заполучить приз в виде колоссального количества мандатов и тем самым ощутимо ограничить дееспособность ЕС. Если, с другой стороны, окажется успешной кибератака на избирательную инфраструктуру лишь в одном отдельно взятом государстве – члене ЕС, то можно будет открыто поставить под сомнение результат выборов в целом, а также итоговую легитимность нового Европейского парламента. В обоих случаях была бы оказана медвежья услуга необходимому сегодня усилению позиций парламента и дальнейшей демократизации ЕС. В конечном итоге в дискуссиях на тему правильного обхождения с виртуальными угрозами в отношении ЕС дает о себе знать фатальный дисбаланс: если государства – члены ЕС не проявят ответственного отношения к защите выборов, то Союзу придется заплатить за это высокую цену. И эта цена вполне может оказаться неоправданно высокой в свете сложившейся ныне ситуации в Европе, когда споры о политическом курсе ЕС все больше и больше отягощаются дебатами о его выживании.» ***(Мориц Фесслер. Выборы в Европарламент под угрозой воздействия: кибератаки и фейкньюс // Украина сегодня (https://ukr-today.com/news/world/379461-vybory-v-evroparlament-pod-ugrozoj-vlijanija-kiberataki-i-fejknjus.html). 11.02.2019).***

***

«Власти ЕС готовятся к возможным попыткам России вмешаться в выборы в Европарламент в мае через хакерские атаки и "фейковые" новости…

"Мы знаем, что они уже пытаются сделать это, и с нашей стороны мы готовимся к этому", — заявил изданию один из собеседников.

По словам экспертов в сфере кибербезопасности, в последние месяцы участились случаи проявления хакерской активности со стороны пророссийских групп в отношении европейских госучреждений, социальных институтов и СМИ.

Так, Бен Рид, глава американской компании FireEye, занимающейся кибербезопасностью, отмечает, что были выявлены участившиеся попытки атак на европейские госструктуры и медиа за последние полгода. "В большинстве своем эта деятельность направлена на министерства обороны и иностранных дел стран НАТО, а также на немецкие СМИ", — отметил он.

В Брюсселе говорят, что намерены разработать систему предупреждения об информационных атаках и борьбы с пропагандой извне, хотя многие дипломаты скептически смотрят на подобную инициативу.

При этом в Вашингтоне считают, что Россия может использовать выборы в ЕС в качестве плацдарма для отработки новых стратегий и способов вмешательства во внутренние дела других стран, в частности, в преддверии президентских выборов в Америке в 2020 году.

"Западные демократии находятся под угрозой вмешательств извне, и Украина является главной тестовой площадкой подобных действий. Российская Федерация испробовала многие техники и стратегии на Украине", — уверен Дэвид Крамер, бывший помощник госсекретаря США.

Российские власти отрицают любые попытки вмешательства в выборы или внутренние дела других государств.» ***(ЕС не исключает попыток вмешательства России в майские выборы // Goodnews.ua (http://goodnews.ua/politics/es-ne-isklyuchaet-popytok-vmeshatelstva-rossii-v-majskie-vybory/). 28.02.2019).***

***

«…Компания Microsoft во второй раз за шесть месяцев выявила связанную с российским правительством операцию, направленную против влиятельных аналитических центров, занимающих критическую позицию в отношении России…

Речь идет об атаках с использованием методики «адресного фишинга», когда хакеры рассылают фальшивые письма с целью заманить людей на сайты, которые выглядят аутентичными, но на деле позволяют злоумышленниками проникнуть в корпоративные компьютерные системы своих жертв.

Как утверждает Microsoft, атаки были связаны с хакерской группировкой APT28 – подразделением российской военной разведки, причастной к вмешательству на выборах в США в 2016 году.

Мишенью хакеров стали более 100 европейских сотрудников Германского фонда Маршалла, германского отделения Аспенского института и Немецкого

общества внешней политики – влиятельных организаций, занимающихся вопросами трансатлантической политики.

Атаки происходили в октябре-декабре 2018 года, в преддверии выборов в Европарламент в мае этого года. Они свидетельствуют о непрерывной агрессивной кампании со стороны российских агентов с целью подрыва демократических институтов в странах, которые они считают противниками.

Это уже второй раз за последние шесть месяцев, когда Microsoft публично сообщает о своих усилиях по противодействию группировке APT28, которую также иногда называют Strontium или Fancy Bear (Microsoft использует исключительно название Strontium).

Незадолго до промежуточных выборов в США Microsoft обезвредила фишинговые операции, направленные против влиятельных консервативных организаций и американского Сената. Тогда APT28 создала поддельные сайты, имитирующие сайты этих организаций и собственность Microsoft. Хакеры также выдавали себя за коллег пострадавших…

В связи с предыдущей попыткой обезвредить хакеров Microsoft сообщала, что ей удалось использовать новую юридическую стратегию для отключения поддельных доментов.

Компания получила судебный ордер о переводе доменных имен на свои собственные сервера, заявив, что поддельные сайты являются нарушением прав интеллектуальной собственности компании, после чего закрыла их…

Директор Германского фонда Маршалла по коммуникациям Эндрю Колб заявил, что он не удивлен тем, что его организация стала мишенью для России.

«Примерно два года мы проводим программу, которая посвящена конкретно авторитарному вмешательству в Интернете, и во многих случаях это означало наблюдение за действиями России, – сказал Колб. – Мы в какой-то мере предполагали, что можем стать объектом подобных атак в любое время».

При этом Колб заметил, что в этот раз он впервые смог связать атаку с конкретной российской хакерской группировкой.» ***(Microsoft выявила атаку российских хакеров на аналитические центры в ЕС // "Українські медійні системи" (https://glavcom.ua/ru/news/microsoft-vyyavila-ataku-rossiyskih-hakerov-na-analiticheskie-centry-v-es-571599.html). 21.02.2019).***

***

«Від імені міністра оборони Латвії Артіса Пабрікса з російських серверів на адресу держустанов розсилали недостовірні і компрометуючі повідомлення…

У листах, підписаних Пабріксом, стверджувалося, що міністр 16 лютого відвідав якийсь бар в Старій Ризі, де нібито брав участь у "двозначних розвагах".

…є копії листів, до яких додані скріншоти, що імітують записи в Твіттері Пабрікса і пост в фейсбук-профілі NATO enhanced Forward Presence Battle Group Latvia, а також колаж з обличчям міністра оборони в інтер'єрі бару…

Міністерство оборони розцінює розсилку листів як класичну операцію з підробки ідентичності з елементами шпигунства - щоб з'ясувати, з яких IP-адрес відкривали ці листи. "Крім того, це спосіб у максимально широкому масштабі

дискредитувати міністра оборони і сферу оборони загалом, щоб стимулювати недовіру в суспільстві", - повідомили в Міноборони Латвії.» ***(Кібератака на Латвію: з російських серверів розсилали фейкові листи // Espreso.tv (https://espreso.tv/news/2019/02/20/kiberataka_na_latviyu_z_rosiyskykh_serveriv_rozsylaly_feykovi_lysty). 20.02.2019).***

***

«Під час проведення проміжних виборів в США у 2018 році американські військові змогли заблокувати так звану фабрику тролів.

Кілька чиновників США заявили, що американські військові змогли заблокувати діяльність так званої фабрики тролів в РФ під час проведення проміжних виборів…

Відповідно до одного з американських законів, у міністра оборони США є право прийняти кроки для захисту країни, якщо Росія, Китай, Іран або Північна Корея проводять кібератаки на уряд чи громадян країни.

Ефективність блокування у 2018 році була настільки високою, що співробітники фабрики тролів скаржилися на порушення роботи.

Наказ провести операцію проти російської фабрики тролів віддав президент США Дональд Трамп…» ***(США вдалося заблокувати фабрику тролів під час проміжних виборів // ФАКТИ. ICTV (https://fakty.com.ua/ua/svit/20190228-ssha-vdalosya-zablokuvaty-fabryku-troliv-pid-chas-promizhnyh-vyboriv/). 28.02.2019).***

***

«В ноябре 2018 года Киберкомандование США US Cyber Command провело хакерскую атаку на российское Федеральное агентство новостей (ФАН). Это подтвердили в самом издании.

Редакция интернет-портала поясняет, что 5 ноября 2018 года был уничтожен RAID контроллер на внутриофисном сервере ФАН и выведены из строя два жестких диска из четырех. Были также отформатированы жесткие диски на арендованных в Швеции и Эстонии серверах, где размещались «зеркала» издания. Однако атака провалилась, поскольку издание продолжило работу в штатном режиме.

Основным источником атаки стал iPhone сотрудника, который был подключен к компьютеру. Гаджет автоматически загрузил вредоносные файлы и предоставил злоумышленникам удаленный доступ.

Генеральный директор ФАН Евгений Зубарев рассказал, что сотрудники IT-департамента ФАН не сочли атаку США достойной особого внимания на первом этапе, так как «действия US Cyber Command были больше похожи на работу хакеров-самоучек, а не профессионалов»…» ***(Раскрыты подробности первой кибератаки США на Россию // Goodnews.ua (http://goodnews.ua/technologies/raskryty-podrobnosti-pervoj-kiberataki-ssha-na-rossiyu/). 28.02.2019).***

***

«Міністр національної оборони Польщі Маріуш Блащак представив концепцію щодо створення сил оборони кіберпростору…

За словами Блащака, сили оборони кіберпростору будуть новою структурою в польській армії.

“Ця структура буде поєднанням Національного центру криптології та інспекції інформатики. Щоб ця структура працювала добре, люди завжди є ключовими, усі ті, хто створить армію захисту кіберпростору, – підкреслив міністр.

Голова міністерства оборони також призначив свого повноважного представника для створення сил оборони в кіберпросторі. Ним став полковник Кароль Моленда, фахівець з кібербезпеки, який раніше працював у військовій контррозвідці.

Блащак наголосив, що створення сил оборони в кіберпросторі – це імплементація керівних принципів НАТО…

Блащак також наголосив на своїй вдячності територіальним силам оборони, які, за його словами, присвячують свій вільний час, “щоб у кризовій ситуації бути присутнім, реагувати і захищати Польщу”.

“У рамках військ територіальної оборони ми створюємо кібер-компонент, щоб ті, хто сьогодні працює в ІТ-компаніях, які є професіоналами, які мають високі позиції на ринку, у разі бажання могли приєднатися до війська і захищати безпеку Польщі та поляків” – заявив Блащак.» ***(Польща анонсувала створення війська оборони кіберпростору // Рубрика (https://rubryka.com/2019/02/06/polshha-anonsuvala-stvorennya-vijska-oborony-kiberprostoru/). 06.02.2019).***

***

«В Польше планируют создать войска обороны киберпространства — соответствующий указ уже подписал министр национальной обороны страны. Полномочным представителем был назначен полковник Кароль Моленду. Министр безопасности отметил, что перед Моленду сейчас стоят конкретные задачи по обеспечению должного уровня кибербезопасности Польши. По замыслу властей, первое подразделение кибервойск должно быть создано уже в этом году. К 2020 году полное формирование нового подразделения должно быть завершено. В Польше заявили, что создаваемая структура будет напрямую связана с центром криптологии и инспекторатом информатики…» ***(Олег Иванов. В Польше создают войска кибербезопасности // Anti-Malware.ru (https://www.anti-malware.ru/news/2019-02-06-1447/28779). 06.02.2019).***

***

«…Німеччина приєдналась до країн, які надають в розпорядження НАТО свої кіберпотужності…

«Так само, як ми надаємо в розпорядження НАТО сухопутні війська, військово-повітряні та військово-морські сили, тепер ми також можемо надавати в розпорядження НАТО і наші потужності у кіберсфері», - заявила міністр оборони Німеччини Урсула фон дер Ляєн. Мета цього кроку – краща озброєність НАТО у

кіберпросторі з огляду на заплановане використання під час операцій Альянсу кіберзброї. Йдеться, для прикладу, про місії в Афганістані чи Іраку. В НАТО оголосили кіберпростір окремою сферою проведення операцій у 2016 році, а в 2017-му домовилися про відповідні директиви щодо військових кібернападів.

У Бундесвері в 2017 році створили окремий підрозділ «кібер- та інформаційний простір». На даний момент він нараховує 13,5 тисяч військових та цивільних співробітників і повинен бути у повній боєготовності до 2021 року.

Поки НАТО не розвиває власні потужності для кібератак, їх добровільно надають держави-члени Альянсу. Минулого року це робили вже США, Великобританія, Нідерланди, Естонія та Данія. Як у випадку з іншими військовими ресурсами, такими як танки і літаки, члени Альянсу зберігають контроль над своїми кіберпотужностями і надають їх у розпорядження НАТО, коли це необхідно для місій і операцій… ***(Німеччина надасть НАТО свою кіберзброю // "Українські медійні системи" (https://glavcom.ua/news/nimechchina-nadast-nato-svoyu-kiberzbroyu-569919.html). 15.02.2019).***

***

Кіберзахист критичної інфраструктури

«Німецькі спецслужби фіксують істотне зростання кількості і масштабу хакерських атак на життєво важливі інфраструктурні об'єкти.

Про це в неділю, 17 лютого, повідомило видання Welt am Sonntag з посиланням на неопубліковану статистику Федерального відомства з безпеки в сфері інформаційних технологій (BSI).

"Існує помітне збільшення кількості та масштабу нападів з метою відключення електропостачання та водопостачання", - йдеться у матеріалі.

У другій половині 2018 року BSI стало відомо про 157 хакерських атак на системи критичної інфраструктури. З них 19 стосувалися електричних мереж. За попередні 12 місяців відомство зафіксувало 145 кібератак такого характеру, роком раніше - 34.

При цьому експерти підкреслюють, що насправді ця кількість ще більша, оскільки провайдери часто не розголошують інформацію про хакерські атаки чи спроби зламу, побоюючись зіпсувати репутацію.» ***(Німеччина фіксує істотне збільшення атак на критичну інфраструктуру – ЗМІ // Європейська правда (https://www.eurointegration.com.ua/news/2019/02/17/7092933/). 17.02.2019).***

***

«Эксперты мирового уровня обеспокоены потенциальными кибератаками на объекты ядерной сферы и их возможными последствиями. Достаточно одной успешной атаки, чтобы случилась катастрофа общепланетарного масштаба. В связи с этим, как никогда актуален вопрос кооперации между странами по снижению киберугроз в отношении ядерного оружия и его систем.

Таков был главный посыл обращения Группы лидеров по вопросам евроатлантической безопасности (EASLG). Специалисты также отметили, что

уровень развития киберпространства и современные возможности в данной сфере значительно обостряют ситуацию и повышают риски.

Наиболее трагическими сценариями, которых опасаются эксперты, могут стать случаи несанкционированного использования ядерного оружия или его применение в ответ на ложную тревогу.

Поскольку этот вопрос ставит под угрозу все государства планеты, EASLG призывает США и Россию выйти на конструктивный двусторонний диалог. Его итогом должны стать конкретные методы противостояния киберугрозам в ядерной сфере. Также, по мнению экспертов, совершенно необходимо повысить качество международного сотрудничества по снижению рисков в киберпространстве.» ***(Кибератаки на ядерную сферу чреваты страшными последствиями // SecureNews (https://securenews.ru/experts-are-concerned-about-cyber-attacks-on-the-nuclear-field/). 15.02.2019).***

***

Захист персональних даних

«Нещодавно стало відомо, що найбільша соцмережа світу платить користувачам гроші в обмін на усі їхні приватні дані. Переважно цей сервіс пропонувався підліткам, які отримували до $20 на місяць. Свої дані вони «зливали» через спеціальний додаток VPN під назвою Facebook Research. Ця програма відкривала Facebook доступ до всіх куточків смартфону користувача та його веб-активності.

Facebook вже не вперше намагається зазирнути в приватні дані користувачів глибше, ніж це сьогодні публічно прийнято. Раніше соцмережа створила додаток Onavo Protect, але його довелося зупинити через заперечення Apple з приводу приватності. Реінкарнація у вигляді Facebook Research дозволяє обійти політики Apple.

Представники Facebook визнали журналістам TechCrunch про існування додатку Facebook Research. За їхніми даними, ця програма дозволяє отримати більше інформації про звички користувачів. Попередньо відомо, що її розповсюджують щонайменше з 2016 року…

Угода користувача Facebook Research зобов'язує юзера погодитися з такими умовами: «…ви дозволяєте нашому клієнту збирати інформацію, таку як встановлені на телефоні додатки, як і коли ви їх використовуєте, дані про активність та контент в додатках, взаємодію інших людей з вами та вашого контенту в цих додатках. Ви також дозволяєте нашому клієнту збирати інформацію про свою інтернет-активність (включаючи відвідані сайти та пересланими на ці сайти інформацією), а також ваше використання інших онлайн-сервісів. Є випадки, коли наш клієнт збиратиме цю інформацію навіть якщо додаток використовує шифрування чи в захищених сесіях браузера».

За даними дослідника кібербезпеки Вілла Страфаха, рівень доступу, що вимагає Facebook Research, дозволяє збирати приватні послання, шифровані повідомлення в месенджерах, фото, відео, електронну пошту, веб-активність та

географічні координати.» ***(Євген Корольов. Facebook таємно платить підліткам за повний доступ до їхніх даних // Tech Today (https://techtoday.in.ua/news/facebook-tayemno-platit-pidlitkam-za-povniy-dostup-do-yihnih-danih-109741.html). 02.02.2019).***

***

«Архів з унікальними іменами користувачів та паролями вільно поширюють на форумах для хакерів.

Як пише Wired, такий величезний архів є збіркою попередніх витоків даних — з Yahoo, LinkedIn і Dropbox. Проте, якщо раніше мільйони викрадених даних продавали, то зараз 2,2 млрд логінів і паролів можна вільно завантажити…

Така велика кількість даних полегшує хакерам роботу з підбору паролю користувачів. Особливо, якщо людина використовує один пароль для декількох сайтів.

Перевірити наявність вашого паролю у злитих базах даних можна на сайті Інституту Хассо Платтера (Hasso Plattner Institut). Спеціалісти радять змінити пароль, якщо адреса все ж потрапила до хакерів…» ***(Хакери розповсюджують архів з 2,2 млрд особистих даних користувачів // MediaSapiens (https://ms.detector.media/web/cybersecurity/khakeri_rozpovsyudzhuyut_arkhiv_z_22_mlrd_loginiv_ta_paroliv/). 01.02.2019).***

***

«…Федеральне антимонопольне відомство Німеччини запроваджує обмеження на збір та обробку даних користувачів соціальної мережі Facebook. Про це в четвер, 7 лютого, заявив керівник відомства Андреас Мунд (Andreas Mund). За словами очільника антимонопольного відомства, компанія Facebook зловживає своїм практично монопольним становищем на ринку соціальних мереж ФРН.

У майбутньому заборонятиметься без попередньої згоди користувача систематизовувати отримані з різних джерел дані, приміром, з меседжера повідомлень Whatsapp та фотоплатформи Instagram. Аналогічні обмеження накладатимуться й на інші Facebook-застосунки, розміщенні на сторінках інших компаній.

За словами Мунда, мета таких заходів - не вибити з американського концерну фантастичні суми штрафів, а домогтися зміни бізнес-моделі компанії Facebook. Водночас Мунд наголосив, що впродовж року Facebook має відреагувати на ці рішення та запропонувати свої пропозиції. Поки що рішення антимонопольного відомства не набуло чинності.

В майбутньому такі Facebook-служби, як Whatsapp чи Instagram, зможуть і надалі збирати та обробляти дані користувачів і прив'язувати їх до Facebook-профілю, однак робитимуть вони це лише за попередньої згоди самих користувачів.

В американській компанії вже оголосили намір позиватися до суду проти цього рішення німецького антимонопольного відомства.» ***(Валерій Сааков. У ФРН обмежать Facebook збір даних користувачів // Deutsche Welle***

(https://www.dw.com/uk/%D1%83-%D1%84%D1%80%D0%BD-%D0%BE%D0%B1%D0%BC%D0%B5%D0%B6%D0%B0%D1%82%D1%8C-facebook-%D0%B7%D0%B1%D1%96%D1%80-%D0%B4%D0%B0%D0%BD%D0%B8%D1%85-%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D1%83%D0%B2%D0%B0%D1%87%D1%96%D0%B2/a-47404124). 07.02.2019).

***

«Эксперт по кибербезопасности из Нидерландов Виктор Геверс нашел в Интернете открытую базу данных с отчетами о слежке за 2,6 млн человек, большинство из которых уйгуры - представители тюркского народа, исповедующего ислам и проживающего на территории Китая…

Кроме имен, база содержит фотографии, домашние адреса, даты рождения, номера ID-карт, пол, национальность и место работы. Кроме того, там указаны GPS-координаты мест, в которых побывали люди из базы. Все места, координаты которых указаны в базе, расположены в Синьцзян-Уйгурском автономном районе КНР. Информация попадала в базу в режиме реального времени.

База принадлежит китайской компании SenseNets, которая является подрядчиком полиции КНР. По данным Financial Times, эта компания получила как минимум четыре правительственных контракта в разных регионах Китая. SenseNets уже скрыла базу из свободного доступа, хотя полгода она была открытой.» ***(Китай следит за 2,6 млн уйгуров, - FT // 112 Украина (https://112.ua/mir/kitay-sledit-za-26-milliona-uygurov-ft-480978.html). 18.02.2019).***

***

«Администрация популярного фотохостинга 500px сообщила об утечке персональных данных 14,8 млн пользователей сервиса в результате взлома, который произошел еще в июле прошлого года.

Как пишет The Verge, в сообщении уточняется, что специалисты обнаружили утечку только 8 февраля. В процессе изучения деталей они пришли к выводу, что кто-то взломал защиту сайта в районе 5 июля 2018 года. В результате этого взлома неизвестные хакеры получили доступ к именам пользователей, их логинам, адресам электронной почты, сведениям о дате рождения, поле и местоположении (если они указывали эти сведения в профиле). Кроме того, в распоряжении злоумышленников оказались и пароли, но они хранились в зашифрованном виде.

По данным 500px, пока нет никаких свидетельств того, что хакеры использовали похищенную информацию для доступа к чужим учетным записям. Что же касается данных кредитных карт, то они не попали к злоумышленникам, поскольку 500px не хранит их на своих серверах.

1/2 PLEASE NOTE: We recently learned of a potential security issue and have taken every precaution to ensure our users' data is safe. There is no indication of unauthorized account access, but as a precautionary measure, we are resetting all user passwords.

— 500px (@500px) 13 февраля 2019 г.

В настоящее время компания продолжает расследование инцидента – за помощью в этом деле представители 500px обратились в полицию и независимую компанию, специализирующуюся на вопросах кибербезопасности. Также 500px рассылает затронутым пользователям уведомления об утечке их данных с рекомендацией сменить пароль.» ***(В Сеть утекли данные 15 млн пользователей популярного фотохостинга // Goodnews.ua (http://goodnews.ua/technologies/v-set-utekli-dannye-15-mln-polzovatelej-populyarnogo-fotoxostinga/). 14.02.2019).***

***

«Журналисты обнаружили в Интернете записи телефонных переговоров между клиентами одного из шведских медицинских сервисов. На веб-сервере, который не требовал пароля для подключения, с 2013 года накопилось около 2,7 млн аудиофайлов общей длительностью 170 тыс. часов.

Информация об угрозе поступила в шведское издание IDG от анонимного источника. Как установил репортер Ларс Добос (Lars Dobos), уязвимый сервер обеспечивал работу облачного колл-центра компании MedHelp. Она предоставляет удаленные медицинские консультации в сотрудничестве с государственной организацией Inera — координатором цифровых сервисов для шведских граждан. В цепочке также участвуют компании Voice Integrate Nordic AB, создавшая облачное ПО Biz 2.0 для колл-центра, и Medicall, которая администрирует пострадавший сервер.

Подключившись к хранилищу, Добос смог просмотреть все его содержимое. Более того, новые записи появлялись онлайн прямо на глазах журналиста. Исследователь не уточняет, мог ли он редактировать содержимое, однако даже такой доступ создавал серьезные угрозы для клиентов MedHelp.

Так, 57 тыс. файлов содержали в наименовании телефонные номера звонивших граждан. Некоторые клиенты называли в разговорах свои номера социального страхования. Журналисты отмечают, что такая утечка может повлечь наказание в соответствии как с общеевропейским GDPR, так и местным законодательством о защите прав пациентов.

По словам Добоса, проблемы не ограничивались одним лишь отсутствием аутентификации. Сервер работал на базе Apache HTTP Server 2.4.7, опубликованной в 2013 году. За прошедшее время в этом ПО было обнаружено более 20 уязвимостей, многие из которых можно было использовать, чтобы скомпрометировать хранилище.

Из всех участвовавших в процессе организаций журналисты смогли получить комментарии только от поставщика ПО для колл-центра — Voice Integrate Nordic. Генеральный директор компании Томми Экстрём (Tommy Ekström) признал, что они не знали о существовании проблемы, и пообещал разобраться в ее причинах. Вскоре после публикации материала Добоса веб-сервер стал недоступен для подключения…» ***(Egor Nashilov. Записи 170 тысяч часов телефонных переговоров утекли в Сеть // Threatpost (https://threatpost.ru/swedish-medical-call-center-exposed-27-mln-records-to-world-and-dog/31225/). 19.02.2019).***

***

«По данным, опубликованным компанией Risk Based Security, в прошлом году произошло более 6500 утечек корпоративных данных, что лишь на 3,2% ниже показателя за 2017 год. В результате 5 миллиардов конфиденциальных записей попали в публичный доступ.

66% утечек пришлось на организации финансового сектора, технологические компании, ритейлеров и сегмент HoReCa.

«В современном мире нельзя легкомысленно относиться к защите данных, и результаты исследования Risk Based Security лишний раз это подтверждают. При этом эффективная защита невозможна без мониторинга и полноценной аналитики. В прошлом году только 30% организаций, конфиденциальные данные которых были скомпрометированы, смогли обнаружить проблему своими силами, в то время как остальные 70% узнали о ней из внешних источников постфактум», – говорит Сергей Халяпин, главный инженер представительства Citrix в России и странах СНГ.

«Современные системы автоматической аналитики с использованием технологий ИИ и машинного обучения позволяют не только оперативно обнаружить «прорывы» в периметре безопасности, но также указывают на потенциальные угрозы.

Кроме того, в исследовании отмечено, что 57% скомпрометированных записей содержали данные о паролях пользователей. Чтобы вред от раскрытого пароля был минимальным, компаниям следует обратить внимание на системы с многофакторной аутентификацией, контекстным доступом к сети и поведенческим анализом. В этом случае, даже если киберпреступник получит пароль пользователя и узнает дополнительные данные для МФА, например, путем социальной инженерии, система ограничит его доступ к сети, как только его действия начнут отклоняться от определенного шаблона типичного поведения.» ***(В 2018 году 5 миллиардов конфиденциальных записей оказались в публичном доступе // ООО "ИКС-МЕДИА (http://www.iksmedia.ru/news/5565761-V-2018-godu-5-milliardov-konfidenci.html). 20.02.2019).***

***

Кіберзлочинність та кібертерроризм

«Эксперты Positive Technologies установили, что абсолютное большинство компаний не смогут отразить кибератаку. Основные проблемы связаны с уязвимостями веб-приложений и неограниченным доступом к внутренним сетевым ресурсам.

В прошлом году аналитики провели более 30 внешних и внутренних проверок на проникновение в условиях, максимально приближенных к реальности. В первом случае специалисты взламывали инфраструктуру так, как это мог бы делать сторонний злоумышленник с нулевым уровнем доступа. Второй вариант предполагал инсайдерскую угрозу. В 25% компаний эксперты выполнили оба теста.

В контрольную выборку вошли российские и зарубежные компании разного профиля. Большинство тестируемых организаций осуществляло свою деятельность в таких сферах, как промышленное производство, финансы и транспорт.

Исследование показало, что девять из десяти инфраструктур беззащитны перед взломщиками. В трех случаях из четырех тестировщики проникали внутрь защищенного периметра через уязвимые веб-ресурсы. Для этого они подбирали пароль одного из пользователей и применяли какую-либо брешь приложения. Это позволяло им загрузить сторонние файлы на корпоративный сервер или установить RDP-соединение.

Другой опасный вектор атаки связан с незащищенными протоколами, по которым учетные данные пересылаются без шифрования. Более чем в половине случаев это позволило экспертам получить доступ к панелям администратора, базам данных и аппаратному обеспечению.

В некоторых случаях злоумышленникам достаточно подключиться к корпоративной WiFi-сети, откуда они могут добраться до локальных ресурсов. Зачастую это можно сделать, даже не заходя в офис компании-жертвы, — почти у 90% участников беспроводная сеть доступна за его пределами. В половине случаев таким образом можно получить неограниченный доступ к инфраструктуре.

Примечательно, что системы аутентификации вовсе не являются панацеей — почти все исследованные WiFi-сети использовали протокол WPA2 с поддержкой EAP или PSK. Преступник может обойти эту защиту, если взломает пароль легитимного пользователя после рукопожатия его устройства с точкой доступа. Подбор кодовой фразы по словарю доказал свою эффективность в половине проверок.

Атака инсайдера грозит еще худшими результатами — в ходе всех проверок специалисты добились неограниченного доступа к инфраструктуре. Все необходимые данные они получали методом подбора или добывали из системной памяти с помощью специальных утилит. Ни одна компания не позаботилась о защите внутреннего трафика. Фактически это означает, что вся корпоративная информация доступна любому участнику локальной сети.

В ходе проверок эксперты успешно применяли и социальную инженерию — звонили сотрудникам и вступали в переписку. Почти 15% пользователей сообщили по телефону имена и должности своих коллег, их рабочие и мобильные номера. Около трети кликнули по ссылке в электронном письме или запустили полученное от тестировщиков приложение. В 10% случаев исследователи смогли получить учетные данные пользователей через поддельную форму аутентификации…» ***(Maxim Zaitsev. Бизнес оказался беззащитен перед киберпреступниками // Threatpost (https://threatpost.ru/ptsecurity-sums-up-corporate-infrastructure-pentesting-2018/30977/). 07.02.2019).***

***

«Наблюдатели из Imperva еженедельно фиксируют DDoS-атаки, превышающие 500 Гбит/с, однако с потоком более 500 млн пакетов в секунду (Mpps) они столкнулись впервые. Подобные атаки, по словам экспертов, могут причинить гораздо больший ущерб, так как они нацелены на вывод из строя

сетевого оборудования, которое не рассчитано на такие перегрузки, равно как и ходовые средства специализированной защиты.

Мощность DDoS-атак все привыкли оценивать по дополнительной нагрузке на каналах связи. Магистральные провайдеры и специализированные сервисы обычно расширяют полосу пропускания, чтобы ограждать клиентов от таких нападений.

Так, в прошлом году, попытавшись исчерпать пропускную способность магистрали GitHub, злоумышленники создали трафик, побивший все известные рекорды: на пике он достиг 1,35 Тбит/с. Однако защитники с успехом отразили атаку с помощью фильтров: мусорный поток состоял в основном из пакетов большого размера, передаваемых с относительно небольшой скоростью (до 126,9 Mpps), к тому же их порт-источник был одинаков — 11211.

В Imperva считают, что рост показателя мощности DDoS, измеряемого в pps, специализированной защите тоже нужно непременно учитывать. Скорость передачи пакетов важна для обработчиков трафика — коммутаторов, роутеров, программно-аппаратных средств защиты от DDoS-атак. Сетевые устройства в основном проверяют заголовки пакетов, специализированные комплексы — также их содержимое, и производительность этих элементов сетевой инфраструктуры пока оставляет желать лучшего.

Атаку в 500 Mpps специалистам Imperva довелось отражать 10 января. Нападающие использовали две разные техники SYN flood — с пакетами обычной величины и с крупными, размером 800 – 900 байт (в Radware такие атаки называют SYN-цунами). По словам экспертов, порт-источник и порт-адресат мусорных пакетов, направляемых на сервер клиента компании, генерировались случайным образом — не исключено, что атакующие прибегли к спуфингу…» ***(Maxim Zaitsev. Чем грозит DDoS мощностью в 500 Mpps // Threatpost (https://threatpost.ru/imperva-mitigated-ddos-attack-500-mpps/30843/). 01.02.2019).***

***

«Привычка некоторых интернет-пользователей заклеивать камеру своего ноутбука является эффективной мерой против киберпреступников.

О способах защиты своего компьютера рассказал эксперт по вопросам кибербезопасности Сергей Прокопенко…

"Это очень правильно. Есть преступники, которые этим зарабатывают. Они взламывают ноутбуки пользователей, следят за человеком. Если человек делает что-то, что можно выгодно потом продать, то так и делают", – заявил Прокопенко.

Эксперт также отметил, что для защиты своего компьютера недостаточно обычного антивируса, поскольку программа может обнаружить только те угрозы, которые знает.

"Вирусы постоянно модифицируются. Под каждую атаку или рассылку хакер может сделать новый сайт, который не будет обнаруживаться антивирусом. Всегда у него есть запас от нескольких часов до нескольких недель, в зависимости от массовости. Если это направленная атака на нескольких людей, то этот вирус может обнаружиться спустя годы", – рассказал он.

Также эксперт посоветовал пользователям регулярно менять свои пароли: "Безопасность – это процесс. Невозможно сказать, что мой компьютер сейчас не взломан и быть уверенным, что все в порядке".» ***(Заклеивать ли камеру ноутбука: украинцам дали сонет // Вести-UA (https://vesti-ua.net/novosti/tehnologii/96724-zakleivat-li-kameru-noutbuka-ukraincam-dali-sovet.html). 17.02.2019).***

***

«Группа преступников получила кредит в размере 65 тысяч долларов, используя особенность почтового сервиса Gmail. Также хакерам удалось подать десятки фальшивых деклараций и заявок на социальные пособия. Об этом сообщили исследователи в области кибербезопасности компании Agari.

Хакеры применили известный трюк, называемый «точечной учетной записью». Он основан на функции Gmail, которая игнорирует точки в почтовом адресе пользователя.

В качестве примера специалисты привели имя bad.guy007: согласно принципам Google, такой адрес всегда будет интерпретироваться как badguy007. При этом пользователь может переносить единственную точку или добавлять новые.

Однако большинство сервисов воспринимает подобные вариации как разные адреса. Этой уязвимостью нередко пользуются мошенники. Подбирая имена аккаунтов, они вынуждают жертв подтверждать платежные и личные данные на различных сайтах.

Сотрудники Agari сообщили, что таким образом хакеры скомпрометировали 56 адресов. Они подали 48 заявок на кредитные карты и получили крупную ссуду в банке, а также выслали множество фейковых налоговых деклараций и заявок на различные пособия.» ***(Мошенники нашли дыру в сервисе Gmail и обогатились // Goodnews.ua (http://goodnews.ua/technologies/moshenniki-nashli-dyru-v-servise-gmail-i-obogatilis/). 06.02.2019).***

***

«Злоумышленники попытались перевести на зарубежные счета 13 млн евро.

В среду, 13 февраля, один из крупнейших мальтийских коммерческих банков Bank of Valletta был вынужден прекратить свои операции в связи с кибератакой. Как сообщает Times of Malta, днем ранее неизвестные взломали системы финорганизации и перевели 13 млн евро на зарубежные счета.

В связи с инцидентом все отделения Bank of Valletta приостановили работу, а банкоматы, мобильное приложение, web-сайт и электронная почта были временно заблокированы. Утром в четверг работа мобильного приложения была восстановлена.

По словам мальтийского премьер-министра Джозефа Муската (Joseph Muscat), все мошеннические транзакции были отслежены и обращены. Злоумышленники пытались перевести деньги на счета в Великобритании, США, Гонконге и Чехии, однако их действия были замечены уже через 30 минут. Предполагается, что кибератака осуществлялась из-за рубежа.

Bank of Valletta уверил своих клиентов в том, что их счета и хранящиеся на них средства скомпрометированы не были и находятся в целости и сохранности. Администрация банка тесно сотрудничает с местными и международными правоохранительными органами в расследовании данного инцидента и в скором времени намерена вернуть свои сервисы в рабочее состояние.» ***(Один из крупнейших мальтийских банков стал жертвой киберграбителей // SecurityLab.ru (https://www.securitylab.ru/news/497938.php). 14.02.2019).***

***

«Атака посредника или "человек посередине" (man-in-the-middle, MitM) — когда злоумышленник перехватывает связь между двумя сторонами, либо тайно подслушивает, либо изменяет трафик, проходящий между ними. Хакеры могут использовать атаки MitM для кражи учетных данных или личной информации, шпионажа за жертвой, диверсии коммуникации или искажения данных, пишет IT News.

"Атаки MitM являются тактическим средством для достижения цели, которая может заключаться в шпионаже за отдельными лицами или группами для перенаправления усилий, средств, ресурсов или внимания", — пояснил технический стратег CrowdStrike Зеки Туриди.

Хотя от MitM можно защититься с помощью шифрования, злоумышленники могут перенаправлять трафик на фишинговые сайты либо передавать его к месту назначения или регистрации, что делает обнаружение подобных атак невероятно сложным…

MitM включает в себя широкий спектр методов и потенциальных результатов, в зависимости от цели и задачи. Например, при разборке SSL злоумышленники устанавливают соединение HTTPS между собой и сервером, но с незащищенным HTTP-соединением с пользователем — информация отправляется в виде простого текста без шифрования.

Атаки Evil Twin отражают действительные точки доступа Wi-Fi, но полностью контролируются злоумышленниками, которые теперь могут отслеживать, собирать или манипулировать всей информацией пользователя.

"Эти типы атак могут быть направлены на шпионаж или финансовую выгоду. Наносимый ущерб варьируется от маленького до огромного, в зависимости от целей атакующего и способности причинять вред", — прокомментировал Туриди.

В случае с банками злоумышленник видит, что пользователь совершает перевод, и меняет номер целевого счета или отправляемую сумму. Хакеры используют MitM-атаки для сбора личной информации или учетных данных…

Хотя атаки MitM не так распространены, как вирусы-вымогатели или фишинговые атаки, они представляют собой постоянную угрозу для организаций. В документе IBM X-Force Threat Intelligence Index 2018 сообщается, что 35% эксплуатации включали MitM-атаки…

Протоколы шифрования, такие как TLS, являются лучшим способом защиты от атак MitM. Последняя версия TLS стала официальным стандартом в августе 2018 года. Есть и другие, например, SSH или более новые протоколы — QUIC от Google…

Аналитики прогнозируют, что количество устройств, подключенных к Интернету, может вырасти до десятков миллиардов в течение следующих пяти лет. К сожалению, отсутствие безопасности во многих устройствах означает, что рост числа IoT-девайсов привет к скачку атак MitM…

Новое исследование, проведенное Институтом Ponemon и OpenSky, показало, что 61% специалистов по безопасности в США говорят, что не могут контролировать распространение устройств IoT и IIoT в своих компаниях, в то время как 60% — что они не могут избежать взломов безопасности и нарушений данных, связанных с IoT и IIoT.» ***(Что такое кибератака "посредника" и как ее предотвратить // Goodnews.ua (http://goodnews.ua/technologies/chto-takoe-kiberataka-posrednika-i-kak-ee-predotvratit/). 14.02.2019).***

***

«…Киберпреступник под псевдонимом Gnosticplayers выставил на продажу в даркнете очередной, уже третий за последнее время, массив похищенных данных. На этот раз он предлагает данные пользователей GfyCat, Legendas.tv, Jobandtalent, Onebip, StoryBird, StreetEasy, ClassPass и Pizap. Примечательно, что ни одна из вышеупомянутых платформ об утечке данных не сообщала.

Напомним, на прошлой неделе на сайте Dream Market появились в продаже 16 баз данных с записями 620 млн пользователей, а затем еще восемь с информацией 127 млн пользователей. В воскресенье, 17 февраля, Gnosticplayers предложил покупателям еще восемь БД с данными 92,76 млн пользователей.

Характер содержащихся в БД данных варьируется в зависимости от платформы. Однако все они содержат электронные адреса, имена пользователей и пароли (в открытом виде или зашифрованные). В некоторых БД также указаны полные имена пользователей, почтовые адреса, телефонные номера, IP-адреса и пр. Все БД можно приобрести по отдельности, а их общая стоимость составляет 2,6249 биткойна (около $9,4 тыс.).

Откуда у продавца появились взломанные БД, ранее не уточнялось. Тем не менее, в прошлую пятницу в интервью изданию ZDNet киберпреступник заявил, что не является лишь посредником, и все БД были взломаны им самим лично. Как пояснил Gnosticplayers, он хочет продать более 1 млрд похищенных записей, а затем бесследно исчезнуть. Пока что на продажу выставлено порядка 840 млн записей, но уже в ближайшем будущем киберпреступник планирует пополнить ассортимент своего товара (в том числе за счет БД, похищенных у криптовалютной биржи***).» (Gnosticplayers выставил на продажу третий массив похищенных данных // SecurityLab.ru (https://www.securitylab.ru/news/497977.php). 18.02.2019).***

***

«Аналітики компанії у сфері кібербезпеки Digital Shadows вияснили, що кіберзлочинці можуть заробляти у даркнеті до одного мільйона доларів в рік.

Однак така діяльність є незаконною, передає AIN.ua з посиланням на дослідження Digital Shadows.

Аналітики компанії знайшли у даркнеті так звані «вакансії» у кіберзлочинних організаціях.

Програмістам пропонують зарплату до $ 64 тисяч з можливістю підвищення до $ 90 тисяч через два роки лояльної роботи.

Так, айтішник зможе заробляти у складі угруповання близько мільйона доларів на рік. Окрім того, додатковим плюсом буде знання китайської, арабської або німецької мов – це ще 5% до зарплати.

За допомогу у здирництві грошей з впливових осіб (глав компаній, юристів та лікарів) злочинці пропонують до $ 30 тисяч в місяць.

Також в даркнеті існують методички, де можна навчитися техніки здирництва грошей. Однак це знову-таки незаконно…» ***(Хакери в Інтернеті можуть заробляти до $1 млн на рік «на ставці» // Західна інформаційна корпорація (https://zik.ua/news/2019/02/27/hakery_v_interneti_mozhut_zaroblyaty_do_1_mln_na_rik_na_stavtsi_1518549). 27.02.2019).***

***

«Киберпреступники наносят огромный ущерб, атакуя крупные компании через инфраструктуры их подрядчиков. Счет потерям идет на триллионы долларов, а способов противостоять хакерам не так много.

Хакеры наносят большой ущерб при незначительных затратах

К 2021 г. общемировой ущерб от кибератак составит $6 трлн. Такими данными поделились аналитики американского сервисного провайдера Source One. По их данным, каждая успешная атака на крупную компанию обходится киберпреступникам примерно в $5 млн. В США наиболее уязвимы предприятия, работающие в сфере закупок. Это связано с активной цифровизацией цепочек поставок. Исследователи не исключают, что негативный тренд в ближайшее время может стать глобальным.

В 2017 г., согласно выводам ряда экспертов, 60% атак на американские компании, представленные на биржах, велись через ИТ-системы поставщиков или других сторонних организаций. Вместе с тем, помимо прямого ущерба, предприятия несут и опосредованный – в виде потери клиентов и снижения доверия.

В качестве примера приводится история шестого по величине ритейлера США – компании Target. Из-за бреши в системах подрядчика Fazio, который занимался вентиляцией и кондиционированием офисов, хакеры через межсетевой экран получили доступ к данным Target. Потери составили $162 млн. Годом позже крупнейшее кредитное бюро Experian подверглось масштабной атаке, в результате которой хакеры получили доступ к личной информации 15 млн человек, которые недавно подписались на услуги T-Mobile…

Рядовые сотрудники должны представлять степень угрозы

Эксперты Source One предлагают несколько вариантов если не решения проблемы, то хотя бы снижения опасности и потенциального ущерба. Ключевой пункт – внедрение решения, которое включает все механизмы безопасности.

«Необходимо постоянное внедрение и разъяснение для участников и пользователей инфраструктуры различных организационных и организационно-технических мер безопасности. Это позволит повысить степень осведомленности и, как следствие, степень защищенности инфраструктуры от влияния человеческого фактора, – добавляет Дмитрий Купецкий. – Ваша инфраструктура станет более устойчивой к методам социального инжиниринга, против которых зачастую неэффективны обычные технические средства защиты».

Кроме того, аналитики полагают, что бизнес-подразделения должны сотрудничать с ИТ-отделом для мониторинга систем и обновления внутренних политик. Эти политики, как и недавние киберугрозы должны быть доступны простым сотрудникам, чтобы они понимали степень угрозы и сам факт ее наличия…

Кроме того, предприятиям стоит разработать стратегию аварийного восстановления. Если никакие меры не помогли и ваша система взломана, важно иметь готовый план для ограничения негативных последствий.» ***(Стоимость успешной кибератаки на крупную компанию достигает $5 млн // Goodnews.ua (http://goodnews.ua/technologies/stoimost-uspeshnoj-kiberataki-na-krupnuyu-kompaniyu-dostigaet-5-mln/). 28.02.2019).***

***

«Компания Trend Micro представила Ежегодный обзор кибератак, с которыми компании по всему миру столкнулись в 2018 году. Ландшафт киберугроз 2018 года представлял собой микс из возобновивших активность старых угроз (фишинг, вирусы-вымогатели) и новых (скрытый майнинг, атаки на уязвимости IoT-устройств, аппаратные уязвимости процессоров).

«Каждые пару-тройку лет ландшафт угроз радикально меняется, поэтому даже самые инновационные подходы к защите стремительно теряют свою эффективность. Современным предприятиям необходимо как можно гибче подходить к вопросам обеспечения безопасности и регулярно пересматривать принятые ранее решения. Наш отчет по угрозам за прошлый год является инструментом для формирования правильных векторов развития ИБ на современном предприятии», — комментирует Михаил Кондрашин, технический директор Trend Micro в СНГ.

Напомним, 2018 год начался с обнаружения аппаратных уязвимостей процессоров — Meltdown и Spectre. Патчи, оперативно вышедшие в январе 2018-го, не смогли исправить уязвимости и в ряде случаев вызвали жалобы пользователей на «синие экраны смерти». К концу года устранить полностью уязвимости не удалось.

Также прошлый год запомнился вступлением в силу европейского Общего регламента по защите конфиденциальных данных (GDPR). Регуляторы уже оштрафовали первых нарушителей: систему видеонаблюдения в Австрии — на 5 280 евро за нарушения в хранении и обработки сведений; социальную сеть в Германии — на 9,2 млн евро за хранение паролей в незашифрованном виде; больницу в Португалии — на 400 тысяч евро за серьезные нарушения, связанные с медицинскими данными.

Главной киберугрозой года стал фишинг. По сравнению с 2017 годом на 269% увеличилось количество атак с использованием вредоносных веб-адресов, доступ к которым удалось заблокировать. Кроме того, на 82% возросло число заблокированных попыток пользователей с уникальным IP-адресом перейти на фишинговый сайт.

В общей сложности в 2018 году решениями Trend Micro вредоносные URL-адреса были заблокированы в Украине — 1 442 481 раз, в Казахстане — 71 147 раз. Кроме того, в Украине было зафиксировано 1 353 474 случая с зараженным программным обеспечением, а в Казахстане — 75 002 случая.

Злоумышленники продолжают компрометировать деловую переписку (BEC). Используя метод социальной инженерии, создавая знакомое визуальное оформление и контекст письма, хакерам удается обойти систему безопасности и обмануть пользователя. Так, за предыдущий год был зафиксирован рост подобных так на 28%.

Бесфайловые вредоносные программы — еще один инструмент злоумышленников, активность которого была зафиксирована в прошлом году. Этот метод увеличивает шанс остаться незаметными при атаке и соответственно достичь цели. На конец 2018 года было зафиксировано свыше 140 тыс. 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).

К примеру, в случае с Foxit, решением для работы с PDF-файлами, было зафиксировано наибольшее число уязвимостей — 257, следом идут результаты, обнаруженные в программах для работы с PDF от Adobe — 239, Microsoft — 124, Apple — 66 и Google — 4.

Волна вирусов-вымогателей пошла на спад. Аналитиками Trend Micro отмечено 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 тыс кибератак.

В 2018 году достиг нового пика скрытый майнинг — было зафиксировано более 1 млн случаев, что демонстрирует рост за год на 237%. Увеличилось разнообразие атак в течение года: рекламные платформы, всплывающие объявления, вредоносные расширения браузера и т.д.» ***(Trend Micro: в Украине обнаружено свыше 1 млн вредоносных программ в прошлом году // «Компьютерное Обозрение» (https://ko.com.ua/trend_micro_v_ukraine_obnaruzheno_svyshe_1_mln_vredonosnyh_programm_v_proshlom_godu_127937). 27.02.2019).***

***

«В 2018 году, по данным опроса World Economic Forum, главной угрозой бизнесу в мире признали кибератаки. Они впервые в истории опередили терроризм, энергетический кризис и безработицу. А в Европе опасаются, что хакеры могут сорвать выборы в Европарламент. Взломов опасаются

государственные ведомства и стратегические объекты по всему миру. EtCetera расскажет о тех хакерах, которые сумели войти в историю благодаря своим дерзким кибернападениям…» ***(Гарченко. На грани закона: названы самые известные хакеры мира и их самые громкие атаки // ETCETERA.MEDIA (https://etcetera.media/na-grani-zakona-nazvanyi-samyie-izvestnyie-hakeryi-mira-i-ih-samyie-gromkie-ataki.html). 23.02.2019).***

***

Діяльність хакерів та хакерські угруповування

«Дослідники кібербезпеки з компанії Recorded Future заявили, що китайські хакери зламали мережу норвезької компанії-розробника програмного забезпечення Visma, щоб вкрасти дані їх клієнтів…

Повідомляється, ця атака була частиною глобальної хакерської кампанії Міністерства державної безпеки Китаю по крадіжці інтелектуальної власності та корпоративних секретів.

У свою чергу, Пекін неодноразово заперечує будь-яку причетність до шпигунства з кіберпідтримкою.» ***(Китай здійснив кібератаку на Норвегію // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (http://day.kyiv.ua/uk/news/060219-kytay-zdiysnyv-kiberataku-na-norvegiyu). 06.02.2019).***

***

«Федеральный парламент Австралии заявил о попытке взлома своей компьютерной сети. Правительство не исключает, что за нападением стоит иностранное правительство.

В совместном заявлении Скотт Райан и Тони Смит - председатели парламента - сообщили, что инцидент безопасности в парламентской компьютерной сети произошел в ночь с четверга на пятницу. Однако нет сообщений об утечке данных. Но все же, в целях безопасности, произвели сброс паролей…» ***(Произошла кибератака на Парламент Австралии // SecureNews (https://securenews.ru/australian-parliament-was-cyber-attacked/). 08.02.2019).***

***

«Хакеры Северной Кореи впервые за всю историю исследования информационной безопасности совершили атаку на организации, которые базируются в России.

Как сообщет CNews со ссылкой на данные Check Point, до этого северокорейские хакеры не атаковали Россию, поскольку страны поддерживают дружеские отношения.

Как поясняет Check Point, данная вредоносная активность регистрировалась на протяжении последних нескольких недель. «Мы впервые наблюдаем то, что выглядит как скоординированная атака Северной Кореи против российских организаций», — отмечают исследователи.

Атака была проведена группировкой Lazarus, а точнее ее «коммерческим» филиалом Bluenoroff, который осуществляет хакерские операции ради наживы. У Lazarus есть и другой филиал — Andariel — который занимается кибератаками на Южную Корею. Считается, что Bluenoroff стоит за взломом серверов Sony Pictures Entertainment в 2014 г. Им же приписывают похищение $81 млн у Центробанка Бангладеш в 2016 г. и ограбление как минимум пяти криптовалютных бирж на миллионы долларов.

Новая атака проходила следующим образом. На компьютер пользователя присылалось электронное письмо, которое содержало вредоносные файлы PDF и Word, упакованные в ZIP-архив. Исследователи поясняют, что документы Office были разработаны явно для российских пользователей. На основании этого и было сделано заключение, что мишенями являются российские организации.

Файл PDF служил приманкой, а файл Word, содержащий макросы, являлся непосредственно вредоносным. PDF-приманка представляла собой соглашение о неразглашении информации, составленное якобы от лица российской компании StarForce Technologies (ООО «Протекшен технолоджи»), которая создает решения для защиты контента от копирования. Благодаря этому файлу все письмо выглядело более достоверным.

Документы Office были первым звеном вредоносной цепочки, которая в конечном счете приводила к загрузке бэкдора Keymarble, что является одним из главных доказательств причастности Lazarus к атакам. По данным компьютерной команды экстренной готовности (US-CERT) Министерства внутренней безопасности США, троян предназначен для получения удаленного доступа к данным, инструкции ему присылает удаленный сервер. В качестве механизма защиты данных и связи с сервером используется алгоритм шифрования XOR.

После получения файла Word активировались макросы, которые загружали вредоносный скрипт VBS из Dropbox URL. Затем уже сам VBS загружал файл CAB и извлекал встроенный файл EXE, то есть сам бэкдор, через утилиту Windows expand.exe, после чего бэкдор наконец-то исполнялся. Впоследствии злоумышленники упростили схему — загрузка бэкдора стала возможна непосредственно с помощью макросов в документе Word.» ***(Хакеры из Северной Кореи впервые в истории напали на Россию // ООО "ИКС-МЕДИА (http://www.iksmedia.ru/news/5565850-Xakery-iz-Severnoj-Korei-vpervye.html). 20.02.2019).***

***

«Согласно последнему докладу CrowdStrike, в 2018 году спонсируемая госструктурами Китая активность в киберпространстве значительно возросла. В то же время российские представители были наиболее эффективными.

В Отчете о глобальной угрозе 2019 года, отслеживается относительно новый показатель «breakout time» или же «время прорыва». Он измеряет на сколько быстро хакер перемещаться по сети, в поиске ключевые данных и активов. Ведь именно это, в конечном итоге, является целью атакующей кампании.

Благодаря этому показателю ИТ-команды смогут лучше понять, как быстро они должны реагировать на угрозы.

Согласно представленной в отчете статистике среднее время прорыва составляет 4 часа 37 минут. Однако время значительно варьировалось. Задачи, на которые киберпреступники в среднем тратили 9 часов 42 минуты, выполнялись российскими хакерами всего за 18 минут.

Следующими по скорости стали северокорейские акторы со средним временем прорыва 2 часа 20 минут.

В свою очередь Китай занял первое место в списке наиболее целенаправленных вторжений. В частности, в 2018 году особое внимание было уделено нападениям на телекоммуникационные компании. Основной целью атак было скомпрометировать правительства Азии.

Основной вывод отчета – мир находится в настоящей «гонке вооружений» за кибернетическое превосходство. Однако между гонкой вооружений в кибер-сфере и физическим миром есть некоторые важные различия. Самое главное в том, что в киберпространстве любой игрок может стать супердержавой.

Еще одной важной тенденцией, отмеченной в отчете, является использование таргетированных методов вымогания финансово мотивированными киберпреступниками.

Данные разведки являются еще одним подтверждением того, что вымогатели остаются серьезной головной болью для бизнеса и организаций. Еще в сентябре 2018 года Европол предупредил, что в настоящее время это самая большая угроза для предприятий во всем мире и она сохранится.» ***(Русские хакеры работают быстрее всех в мире // SecureNews (https://securenews.ru/russian-hackers-are-the-fastest-in-the-world/). 20.02.2019).***

***

Вірусне та інше шкідливе програмне забезпечення

«Боты губят Интернет. Когда они не загружают веб-сайт именами пользователей и паролями из длинного списка украденных учетных данных, то пытаются отключить ресурс в течение нескольких часов подряд. Существует целая подпольная экономика, где боты являются основными инструментами для автоматизации мошеннических покупок и запуска кибератак…

Очевидно, что существующий подход Whac-A-Mole не работает. "С этим нужно было смириться как с расходом на ведение бизнеса", - прокомментировал директор Kasada Джонни Кмас. Kasada – антибот-стартап, где ботам затрудняют работу благодаря сложным задачам.

Система достаточно проста. По словам Кмаса, боты – это "белый шум" интернета. Как только бот запущен, он продолжает работать, пока ему не скажут остановиться или пока его работа не будет завершена. Kasada обманывает ботов, заставляя их "думать", что работа никогда не закончится. Предоставляя

небольшую, но сложную математическую головоломку до того, как сайт загрузится, Kasada заставляет бота тратить свое время на ее решение.

Несколькими неделями ранее один бот делал за один день около четырех миллионов запросов к веб-сайту. Kasada отправил роботу сгенерированный код JavaScript, который автоматически загружается в браузер. В течение более 24 часов бот потратил все ресурсы облачной обработки, пытаясь решить невозможную математическую задачу…» ***(Ирина Фоменко. TechCrunch: боты засоряют интернет-трафик // Internetua (http://internetua.com/techcrunch-boty-zasoryaut-internet-trafik). 06.02.2019).***

***

«Исследователи Check Point обнаружили рост активности SpeakUp — нового бэкдора для Linux, который распространяет криптомайнер XMRig. Новое вредоносное ПО способно доставлять любую полезную нагрузку и запускать ее на скомпрометированных компьютерах.

Как сообщается в отчете Global Threat Index, подготовленном Check Point Software Technologies, новый троян пока не обнаруживается антивирусами ни одного поставщика программ безопасности. Он был распространен с помощью серии эксплойтов, основанных на последовательностях команд центра управления, включая 8-ю, наиболее эксплуатируемую уязвимость — инъекция команд в HTTP-заголовки. Исследователи Check Point рассматривают Speakup как серьезную угрозу, поскольку его можно использовать для загрузки и распространения любых вредоносных программ.

В январе первые четыре строчки рейтинга самых активных вредоносных программ заняли криптомайнеры. Coinhive остается главным вредоносным ПО, атаковавшим 12% организаций по всему миру. XMRig снова стал вторым по распространенности зловредом (8%), за которым последовал криптомайнер Cryptoloot (6%). Несмотря на то, что в январском отчете представлены четыре криптомайнера, половина всех вредоносных форм из первой десятки может использоваться для загрузки дополнительного вредоносного ПО на зараженные машины.

«В январе произошли небольшие изменения в формах вредоносных программ, ориентированных на организации по всему миру, однако мы находим все новые способы распространения вредоносных программ. Подобные угрозы являются серьезным предупреждением о грядущих угрозах. Бэкдоры, такие как Speakup, могут избежать обнаружения, а затем распространять потенциально опасное вредоносное ПО на зараженные машины. Поскольку Linux широко используется именно на корпоративных серверах, мы ожидаем, что Speakup станет угрозой для многих компаний, масштабы и серьезность которой будут расти в течение года, — комментирует Василий Дягилев, глава представительства Check Point Software Software Technologies в России и СНГ. — Кроме того, второй месяц подряд в тройке самых активных вредоносных программ в России оказывается BadRabbit.Так что злоумышленники используют все возможные уязвимости для получения прибыли».

Самое активное вредоносное ПО января 2019

*Стрелки показывают изменение позиции по сравнению с предыдущим месяцем.

↔ Coinhive (12%) — криптомайнер, предназначенный для онлайн-майнинга криптовалюты Monero без ведома пользователя, когда он посещает веб-страницу. Встроенный JavaScript использует большое количество вычислительных ресурсов компьютеров конечных пользователей для майнинга и может привести к сбою системы.

↔ XMRig (8%) — Программное обеспечение с открытым исходным кодом, впервые обнаруженное в мае 2017 года. Используется для майнинга криптовалюты Monero.

↑ Cryptoloot (6%) — криптомайнер, использующий мощность ЦП или видеокарты жертвы и другие ресурсы для майнинга криптовалюты, зловред добавляет транзакции в блокчейн и выпускает новую валюту.
Hiddad, модульный бэкдор для Android, который предоставляет привилегии загружаемому вредоносному ПО, заменил Triada на первом месте в списке мобильных вредоносных программ. На втором месте расположился Lotoor, в то время как троян Triada спустился на третье место.

Самые активные мобильные угрозы января 2019

1. Hiddad — Модульный бэкдор для Android, который предоставляет права суперпользователя для загруженного вредоносного ПО, а также помогает внедрить его в системные процессы.
2. Lotoor — программа использует уязвимости в операционной системе Android, чтобы получить привилегированный root-доступ на взломанных мобильных устройствах.
3. Triada — модульный троян для Android, который предоставляет привилегии суперпользователя для загружаемых вредоносных программ, а также помогает внедрить их в системные процессы.

Исследователи Check Point также проанализировали наиболее эксплуатируемые уязвимости. CVE-2017-7269 остался на первом месте (47%). Также в тройке утечка информации через репозитории веб-сервера Git (46%) и критические уязвимости библиотеки OpenSSL TLS DTLS Heartbeat (45%).» ***(Появился опасный троян SpeakUp // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5564807-Poyavilsya-opasnyj-troyan-SpeakUp.html). 15.02.2019).***

***

«В Google Play обнаружили новое вредоносное приложение, которое успели скачать многие пользователи

Вредоносное ПО, замаскированное под полноценный криптовалютный кошелёк, было обнаружено в магазине приложений Google Play экспертом компании Eset Лукасом Стефанко, о чём он написал в блоге.

…целью приложения была кража данных, необходимых для получения доступа к Ethereum-кошелькам пользователей. В частности, оно могло заменять адреса кошельков, копируемые в буфер обмена, на адреса хакеров.

Вредоносное приложение было обнаружено вскоре после его появления в Google Play 1 февраля и к настоящему моменту уже удалено из магазина. Как отметил Стефанко, подобный клиппер попал в Google Play впервые – ранее уже находились вредоносные приложения, выдававшие себя за MetaMask, но они были способны лишь воровать критически значимую информацию для получения доступа к криптовалютным средствам жертвы.

Google утверждает, что регулярно сканирует более 50 миллиардов приложений на вирусы, бэкдоры, шпионские функции, фишинговые инструменты, спам и различные уловки, позволяющие мошенникам получить доступ к устройствам и персональным данным пользователей. Несмотря на это специалисты по кибербезопасности регулярно находят вредоносное ПО, которое маскируется под игры, телевизионные приложения и программы для удаленного управления.

Также ранее сообщалось, что новые вирусные программы поселились в популярном приложение Google Play.

Смартфоны на системе Android все еще уязвимы для разных вредоносных приложений, которые попадают в Google Play. Несмотря на то, что технологический гигант улучшил собственные сервисы скрининга, разные зловредные программы продолжают проникать в магазин приложений, завлекая пользователей их скачать, сообщили в киберзащитной компании Trend Micro.

В этот раз компания обнаружила 29 вредоносных приложений в каталоге Google Play. В частности, это программы для обработки фотографий, выполняющие скрытые вредоносные действия (могут распространять навязчивую рекламу и даже воровать данные).» ***(В Google Play обнаружили серьезные проблемы: «под угрозой все пользователи» // Politeka (https://politeka.net/news/hightech/910541-v-google-play-obnaruzhili-sereznye-problemy-pod-ugrozoj-vse-polzovateli/). 11.02.2019).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«В Нью-Йорке судят российского программиста Станислава Лисова, которого экстрадировали в 2018 году в США из Испании. Мужчина уже признал свою вину в сговоре с целью совершения хакерской атаки, сообщил адвокат россиянина Аркадий Бух…

“Данное признание стало результатом продолжительного переговорного процесса с прокуратурой Южного округа штата Нью-Йорк”, – отметил адвокат.

По его словам, россиянин признал вину по одному из двух пунктов обвинения, теперь ему грозит до пяти лет лишения свободы. Мужчину обвиняют в создании вредоносной программы NeverQuest для кражи банковских данных и личной информации. С помощью этой программы хакеры пытались похитить миллионы долларов.

Сам же Лисов в период с июня 2012 года по январь 2015 года участвовал в создании NeverQuest, а также управлении компьютерной сетью, применявшейся для распространения вируса.» ***(Российский хакер в Нью-Йорке сознался в кибератаке // AGRIMPASA (http://agrimpasa.com/rossijskij-xaker-v-nyu-jorke-soznalsya-v-kiberatake.html). 24.02.2019).***

***

Технічні аспекти кібербезпеки

«Международная организация по стандартизации разработала новый стандарт безопасности промышленного IoT.

Для обеспечения безопасности «умного» производственного оборудования требуются «умные» технологии. Смарт-устройства постоянно находятся под угрозой кибератак, и не только «Интернет вещей» (IoT) в целом, но и отдельные системы. В связи с этим Международная организация по стандартизации (ИСО) разработала новый стандарт, призванный усилить безопасность промышленного IoT-оборудования…

С целью усиления безопасности промышленного IoT-оборудования ИСО представила новый технический стандарт ISO/TR 22100-4 «Безопасность производственного оборудования – Связь с ISO 12100 – Часть 4: Руководство для производителей оборудования по рассмотрению соответствующих аспектов информационной безопасности (кибербезопасности)».

Как понятно из названия, новый стандарт дополняет уже существующий стандарт безопасности промышленного оборудования ISO 12100 «Безопасность производственного оборудования – Основные принципы проектирования – Оценка и снижение рисков».

Новый стандарт призван «проработать аспекты безопасности оборудования, которое может быть затронуто кибератаками, связанными с непосредственным или удаленным доступом и манипуляциями с системами управления безопасностью, осуществляемыми со злым умыслом (не по назначению)». Для этих целей стандарт предоставляет руководство по таким ключевым аспектам ИБ, как шифрование и аутентификация.» ***(Представлен новый стандарт по обеспечению безопасности промышленного IoT // SecurityLab.ru (https://www.securitylab.ru/news/497858.php). 11.02.2019).***

***

«Европейский институт телекоммуникационных стандартов (European Telecommunications Standards Institute, ETSI) опубликовал технические спецификации, призванные повысить безопасность бытовых IoT-устройств. Авторы рекомендаций рассчитывают, что документ поможет производителям избавить продукты от множества мелких проблем, которые сегодня приводят к серьезным последствиям.

По словам экспертов ETSI, растущая популярность Интернета вещей создает множество проблем — угрозы приватности и персональным данным, IoT-ботнеты и

разрушительные DDoS-атаки. Предложенные меры отвечают на все эти угрозы, закладывая базовые установки для защиты как самих устройств, так и построенных на них сервисов.

Заводские пароли. Все коды доступа к IoT-устройствам должны быть уникальными. Производителям следует убрать функции, позволяющие вернуть некое базовое значение пароля.

Обновление ПО. Все IoT-устройства, попадающие под действие нового стандарта, должны иметь функцию безопасного апдейта. Кроме того, производители или поставщики сервисов должны оперативно доносить до пользователей информацию об актуальных версиях ПО. Те продукты, которые невозможно обновить по воздуху, следует изолировать до замены аппаратной начинки.

Работа с важной информацией. Все логины, пароли и прочие закрытые данные необходимо держать в защищенном хранилище. При этом не стоит прописывать их в коде устройства, поскольку такая информация восприимчива к реверс-инжинирингу.

Безопасная передача данных. IoT-устройства должны использовать шифрование при любых процессах, связанных с удаленным управлением и настройкой.

Сокращение площади атаки. Эксперты призывают производителей использовать принцип минимальных прав. Это означает, что программные процессы должны исполняться только на том уровне привилегий, который необходим для текущих задач. Все неиспользуемые компоненты — программные модули, сетевые порты и прочее — должны прекращать работу, а разработчикам не следует оставлять в коде скрытые функции.

Целостность ПО. Чтобы преступник не мог подменить прошивку устройства, необходимо проверять ее с помощью защищенных аппаратных модулей. При обнаружении вмешательства соответствующие уведомления должны получить и владелец гаджета, и разработчик.

Проверка поступающих данных. Все команды и прочая информация, которую можно ввести через пользовательский интерфейс, должны проходить валидацию перед тем, как устройство примет их в обработку.

Защита персональных данных. Потребители Интернета вещей должны четко понимать, какую конфиденциальную информацию использует устройство, зачем это нужно и кто может ее просмотреть. Любые связанные с этим процессы можно запускать только с согласия пользователя. При необходимости владелец устройства должен иметь возможность быстро удалить все свои данные.

Устойчивость к сбоям. Компаниям следует свести к минимуму зависимость от внешних сетей — электрических и коммуникационных. При возобновлении коммуникации IoT-устройство должно возвращаться к нормальной работе максимально бесшовным образом.

Авторы подчеркивают, что рекомендации ориентированы именно на потребительский сектор Интернета вещей. Стандарты безопасности для промышленности и здравоохранения будут сформированы отдельно…» ***(Egor***

Nashilov. Эксперты задают стандарты для бытового Интернета вещей // Threatpost (https://threatpost.ru/iot-gets-safety-standards-by-etsi/31245/). 20.02.2019).

***

Виявлені вразливості технічних засобів та програмного забезпечення

«ArXiv проанализировали отсутствие безопасности в приложениях для устройств Интернета вещей… Эксперты сходятся во мнении, что защищенность девайсов – одно из последних, о чем думают производители, выпуская товар на рынок…

Пять ученых по информатике - Давино Мауро Джуниор, Луис Мело, Харви Лу, Марсело д'Аморим и Атул Пракаш - проанализировали приложения для смартфонов для 96 устройств IoT в рамках своих исследований.

Так, 31% программ вообще не использовали шифрование. 19% - использовали жестко закодированные ключи, которые легко обнаружить.

Около 50% приложений для устройств IoT можно взломать. Учитывая огромное количество девайсов, неудивительно, что Интернет вещей стал целью номер один для хакеров.

Если вы построили "умный" дом, шансы, что у используемого вами приложения будет даже базовая безопасность – всего 50/50. Конечно, не стоит ожидать высокого уровня защищенности устройства, заказанного из Китая…

Исследователи утверждают, что проинформировали каждую из компаний о своих выводах до публикации, в том числе о возможных способах снижения выявленных рисков.» ***(Ирина Фоменко. Половина приложений для устройств интернета вещей делает пользователей уязвимыми // Internetua (http://internetua.com/polovina-prilojeniy-dlya-ustroistv-interneta-veschey-delaet-polzovatelei-uyazvimymi). 06.02.2019).***

***

«…Експерт з кібербезпеки Microsoft Кріс Джексон (Chris Jackson) пише в офіційному блозі Windows IT Pro, що Internet Explorer небезпечний в якості браузера за замовчуванням. Справа в тому, що Microsoft припинила його підтримку ще в 2015 році…

Він не підтримує новітні веб-стандарти, але багато сайти і сервіси досі використовують його в якості основного браузера і можуть некоректно працювати в Google Chrome, Firefox або Microsoft Edge.

Саме тому Microsoft радить користувачам відмовитися від застарілого браузера…» ***(Microsoft закликає користувачів відмовитися від застарілого Internet Explorer // znaj.ua (https://znaj.ua/techno/210453-microsoft-zaklikaye-koristuvachiv-vidmovitisya-vid-zastarilogo-internet-explorer). 11.02.2019).***

***

«Пользователи 65-й версии Mozilla Firefox сообщили, что из-за ошибки безопасности не могут посещать вполне защищенные сайты. Разработчики признали источником неполадок конфликт программы с антивирусным ПО и приостановили автоматическое обновление.

Последняя версия Firefox стала доступна для скачивания в конце января. Среди ее преимуществ — расширенные настройки приватности, дополнительные возможности для персонализации программы и несколько исправлений безопасности.

Вскоре после публикации дистрибутива пользователи начали жаловаться на то, что браузер блокирует безопасные сайты. При переходе на такие страницы Firefox сообщает о незащищенном соединении и проблемах с механизмом принудительного включения протокола HTTPS (HTTP Strict Transport Security, HSTS).

Код ошибки SEC_ERROR_UNKNOWN_ISSUER говорит о том, что браузер не может обнаружить предоставленный сайтом сертификат в своей базе и сомневается в его подлинности. Как установили разработчики, сбой происходит из-за веб-модулей антивирусных продуктов, которые вмешиваются в защищенное соединение, чтобы при необходимости заблокировать нежелательную активность в закрытом канале.

Специалисты поддержки поясняют, что браузер проверяет достоверность доверенных сертификатов по собственной базе Mozilla CA Certificate Store. В зависимости от вендора существует несколько методов добавить сертификат антивируса в каталог браузера для устранения конфликта — переустановить защитное ПО, обновить его, выключить и снова включить проверку трафика либо вовсе отказаться от инструмента HTTPS-сканирования…» ***(Dmitry Nazarov. Firefox 65 не пускает на защищенные сайты // Threatpost (https://threatpost.ru/firefox65-dont-allow-to-visit-secured-websites/30886/). 05.02.2019).***

***

«Скандалы вокруг компании Apple и нарушения безопасности пользователей в их экосистеме не утихают уже несколько месяцев. Не успели люди успокоиться после случая с невероятной дырой в безопасности в FaceTime, как на смену пришел новый скандал, связанный с тотальной слежкой за пользователями со стороны различных разработчиков приложений. Все дело в том, что в начале февраля 2019 года, на технофоруме пользователи iPhone стали замечать, что некоторые приложения на уровне программного кода имеют не лицензируемый доступ к записи экрана смартфона. После поднятия данного вопроса на массовом уровне, Apple моментально отреагировала большим количеством блокировок в App Store.

Своеобразная “охота на ведьм” произошла потому, что App Store и другие сервисы Apple всегда считались образцом заботы о конфиденциальности и безопасности пользователей. Именно поэтому, отдел кибербезопасности корпорации начал массово исследовать как те приложения, на которые жаловались пользователи, так и все остальные — в качестве профилактики. Выяснилось, что сразу несколько десятков программ в App Store имели скрытый доступ к записи

действий экрана в iPhone, а потому были немедленно заблокированы администрацией магазина.

В числе попавших “под нож” недавней проверки Apple, оказались и несколько крайне популярных среди пользователей сервисов. В частности: Abercrombie & Fitch, Hotels.com, Air Canada, Hollister, Expedia и Singapore Airlines, были заблокированы несмотря на свою популярность, так как не запрашивали у пользователей разрешение на запись экрана. Блокировка, по заявлению Apple, продлится какое-то время, за которые разработчики должны удалить из своих программ “код записи экрана”. В противном случае по истечении данного времени все заблокированные приложения будут удалены из магазина App Store.» ***(Павел. Apple массово блокирует популярные приложения в App Store // GEEKon (https://geekon.media/apple-massovo-blokiruet-populyarnye-prilozheniya-v-app-store/). 11.02.2019).***

***

«Исследователь в области кибербезопасности из Германии по имени Линус Хенце обнаружил в macOS опасную уязвимость, которая позволяет третьим лицам получить доступ к сохраненным в «Связке ключей» учетным данным от всех сохраненных аккаунтов. По его словам, брешь присутствует во всех версиях настольной операционной системы от Apple, а потому подвергает опасности взлома миллионы пользователей компьютеров Mac по всему миру. Правда, Хенце не готов раскрывать данные об уязвимости до тех пор, пока ему не заплатят за это.

Хенце считает, что работа, которую проделывают программисты и исследователи в области информационной безопасности, занимаясь поиском уязвимостей, должна оцениваться по достоинству. К сожалению, сегодня это не так. Негласное правило, действующее в отрасли, предполагает, что любой программист, которому удастся найти уязвимость в том или ином продукте, обязан сообщить об этом производителю и только после этого, дав ему достаточно времени на исправление, о ней можно говорить публично.

Уязвимость в «Связке ключей»

Исследователь не стал распространяться об особенностях уязвимости, а только заявил, что она позволяет прочесть содержимое «Связки» без необходимости запрашивать разрешение администратора. Единственное, что, по его словам, нужно сделать, — установить на устройство специальное приложение, которое произведет выемку учетных данных самостоятельно…

Интересно, что у Apple есть программа поощрений для программистов, которые находят уязвимости в iOS, однако ее действие не распространяется на macOS…» ***(Хакер потребовал у Apple денег за подробности об уязвимости в macOS // Український телекомунікаційний портал (https://portaltele.com.ua/news/companies/haker-potreboval-u-apple-deneg-za-podrobnosti-ob-uyazvimosti-v-macos.html). 08.02.2019).***

***

«Розробникам файлового архіватора для Windows WinRAR довелося виправляти помилку 19-річної давнини, яка дозволяла зловмисникам "розпаковувати" шкідливе програмне забезпечення в будь-якому місці жорсткого диска користувача.

Прогалина в безпеці була виявлена дослідниками Check Point Software Technologies, які помітили, що робота архівів WinRARформату ACE забезпечується небезпечним файлом DLL, який з'явився в архівах ще в 2006 році…

Після того, як спеціалісти Check Point повідомили розробників WinRAR про свої висновки, команда архіватора вирішила не виправляти помилку у форматі архівів ACE, а відмовитися від них взагалі. Тим паче, що програма для створення архівів цього формату — WinACE — не оновлювалася з 2007 року…» ***(У архіваторі WinRAR знайшли небезпечну помилку 19-річної давнини // MediaSapiens (https://ms.detector.media/web/cybersecurity/u_arkhivatori_winrar_znayshli_nebezpechnu_pomilku_19richnoi_davnini/). 21.02.2019).***

***

«Прошло лишь девять дней после выхода плановых патчей для Acrobat и Reader, а компания Adobe вновь призывает обновить продукт. Оказалось, что патч, спешно созданный для бреши 0-day, можно обойти.

Возможность кражи NTLM-хешей в ходе автозагрузки таблицы стилей для XML-структур в PDF обнаружил эксперт Cure53 Алекс Инфюр (Alex Inführ), о чем он и поведал в своем блоге 26 января. Ввиду высокой опасности бреши (CVE-2019-7089) специалисты компании ACROS Security подготовили микропатч, который можно было поставить через бесплатную утилиту 0patch. Временная заплатка вышла за день до появления официального патча.

К сожалению, решение Adobe оказалось неполным. Проверяя надежность патча, Инфюр нашел способ обхода привносимых им изменений, и разработчикам пришлось исправлять свой промах.

«Adobe выпустила обновления для системы безопасности Adobe Acrobat и Reader, установленных на Windows и macOS, — сказано в новом бюллетене. — Эти обновления закрывают объявившуюся возможность обхода патча к CVE-2019-7089, который вышел 12 февраля в составе сборок 2019.010.20091, 2017.011.30120 и 2015.006.30475″.

Новой находке Инфюра был присвоен идентификатор CVE-2019-7815. «Успешная эксплуатация может привести к раскрытию конфиденциальной информации в контексте текущего пользователя», — так охарактеризовала Adobe эту брешь в бюллетене.

Доработанному патчу назначен приоритет 2, так как уязвимости подвержен продукт, относящийся к группе повышенного риска. Данных об использовании CVE-2019-7815 в атаках на настоящий момент нет. Чтобы избавиться от бреши, пользователям рекомендуется обновить продукты на обеих платформах следующим образом:

Acrobat DC/Acrobat Reader DC Continuous — до версии 2019.010.20098,

Acrobat/Acrobat Reader Classic 2017 — до 2017.011.30127,

Acrobat DC/Acrobat Reader DC Classic 2015 — до 2015.006.30482.»

(Lindsey O'Donnell. Adobe исправила патч для опасной дыры в Acrobat Reader // Threatpost (https://threatpost.ru/adobe-re-patches-critical-acrobat-reader-flaw/31288/). 22.02.2019).

***

«В этом году команда GitHub отметила пятилетие программы вознаграждений за уязвимости. Разработчики дополнили ее новыми продуктами и повысили суммы выплат. За 2018 год ИБ-специалисты получили за свою работу около $165 тысяч. Если учесть исследовательские гранты, частные программы bug bounty и «живые» хакерские мероприятия, то общая сумма вознаграждений достигает $250 тысяч.

Отныне программа распространяется на весь домен github.com. Например GitHub Education, GitHub Learning Lab, GitHub Jobs, и GitHub Desktop, а также Enterprise Cloud. К тому же уязвимости можно искать во внутренних сервисах на github.net и githubapp.com. Представители компании заявляют, что «защита данных наших пользователей зависит от защищенности наших сотрудников и внутренних систем».

Суммы вознаграждений за ошибки теперь следующие:

Критическая уязвимость — 20 000 – 30 000+ долларов;

Уязвимость высокой опасности — 10 000 – 20 000 долларов;

Уязвимость умеренной опасности — 4000 – 10 000 долларов;

Уязвимость низкой опасности — 617 – 2000.

Помимо всего, был дополнительно проработан Legal Safe Harbor – юридический сборник правил и рекомендаций, который обеспечит исследователям легальность работы и возможность заработать вознаграждение, а не судебный иск.»

(GitHub увеличил вознаграждения по своей программе bug bounty // SecureNews (https://securenews.ru/github-increased-bug-bounty-program-rewards/). 21.02.2019).

***

«Google объявила, что выплатила более $15 миллионов с момента запуска в ноябре 2010 года своей программы вознаграждений за ошибки.

Только за последний год компания распределила 3,4 миллиона долларов среди 317 различных исследователей в области безопасности. Эта цифра немного больше прошлогодней – $2,9 миллиона долларов, которые были выделены 274 исследователям. Половину прошлогодних премий – 1,7 миллиона долларов – присудили исследователям, которые обнаружили уязвимости в Android и Chrome.

Программа Google Bug Bounty является отличным дополнением к существующим программам внутренней безопасности. Это мотивирует как отдельных исследователей, так и группы находить недостатки и сообщать об этом. Такой подход снижает риск злонамеренного использования этих ошибок, а также продажи информации третьим лицам. Награждения исследователей мелочь для компании по сравнению с стоимостью потенциальных последствий от серьезных уязвимостей.

Финансовое вознаграждение Google за найденные ошибки варьируется от 100 долларов до $200 тысяч в зависимости от уровня риска обнаружения. К примеру, в 2018 году самая большая награда составила $41 тысячу…

Программа Google Bug Bounty постоянно растет, как в разнообразии продуктов, так и в финансировании. К примеру, за взлом Chromebook можно получить до $100 тысяч, а за Android – до $200 тысяч.» ***(Исследователи безопасности получили от Google более $15 миллионов // SecureNews (https://securenews.ru/security-researchers-have-received-from-google-financial-support/). 12.02.2019).***

***

«Практически полное отсутствие вирусных программ для macOS компенсируют уязвимости, которые время от времени эксперты в области кибербезопасности в ней находят. Правда, на этот раз брешь нашли не в самой системе, а в интерфейсе Thunderbolt, который используется в компьютерах Mac для подключения периферии. Как сообщили исследователи Университета Райса, института SRI International и Кэмбриджского университета, эксплуатация уязвимости позволяет получить доступ к пользовательским данным и даже внедрить в систему вредоносный компонент.

Суть уязвимости состоит в том, что периферийные устройства, подключаемые к Mac по Thunderbolt, по умолчанию имеют больше привилегий, чем те, что были подключены посредством иных стандартов. Распознав подключение, компьютер автоматически открывает Thunderbolt-совместимым гаджетам доступ к разделам операционной системы, которые могут содержать потенциально важные сведения, нуждающиеся в защите. Например, логины и пароли…

По данным экспертов, обнаруживших уязвимость, она затрагивает практически все модели Mac, выпущенные после 2011 года, а также стандарты Thunderbolt всех поколений. Такой охват делает потенциально уязвимыми миллионы компьютеров с macOS на борту, а также Linux и Windows, при условии, что они были выпущены после 2016 года и также имеют поддержку Thunderbolt. На момент выхода публикации брешь была частично устранена, но далеко не полностью.

Мало того, что Thunderbolt-совместимая периферия может получить доступ к конфиденциальной информации, так с ее помощью можно еще и внедрить в систему вредоносный компонент, который будет заниматься сбором не только имеющихся данных, но и тех, что попадут на компьютер в будущем. И хотя, чтобы проделать нечто подобное, злоумышленникам необходим физический доступ к деск- или лэптопу, это не делает уязвимость менее опасной, особенно, если вспомнить об организациях, большинство из которых не уделяют должного внимания безопасности.» ***(Уязвимость в Thunderbolt позволяет взломать почти все Mac новее 2011 года // Goodnews.ua (http://goodnews.ua/technologies/uyazvimost-v-thunderbolt-pozvolyaet-vzlomat-pochti-vse-mac-novee-2011-goda/). 27.02.2019).***

***

«В браузере Firefox появится страница с предупреждением о возможной атаке «человек посередине». Новая функция запланирована к запуску в 66-й версии обозревателя, которая должна выйти в марте этого года. ИБ-специалисты обращают внимание, что в ряде случаев сообщение о подозрительной активности может быть вызвано работой легитимного программного обеспечения.

Как утверждают разработчики браузера, сообщение об ошибке типа MOZILLA_PKIX_ERROR_MITM_DETECTED будет отображаться, если Firefox обнаружит подмену TLS-сертификата в защищенном HTTPS-соединении. Это может означать, что злоумышленники пытаются удаленно перехватить зашифрованный трафик, чтобы украсть данные или взломать компьютер жертвы. Другие причины для предупреждения — активность вредоносного ПО или мониторинг передаваемых данных на стороне провайдера.

Firefox будет отображать страницу ошибки в случае, если признает новый TLS-сертификат ненадежным или усомнится в его принадлежности к хосту, с которым установлено соединение.

Эксперты отмечают, что в ряде случаев предупреждение может быть вызвано работой антивирусных программ, которые внедряют свои скрипты в защищенное соединение для анализа трафика «на лету». Специалисты рекомендуют воспринимать открытие такой страницы как предварительный сигнал о подозрительной активности и повод провести более глубокую проверку безопасности устройства…» ***(Egor Nashilov. Firefox 66 предупредит пользователей о MitM-атаках // Threatpost (https://threatpost.ru/firefox-66-to-implement-mitm-defense/30867/). 04.02.2019).***

***

«Специалисты планируют протестировать функцию под названием Trusted Types на протяжении 2019 года.

Инженеры Google работают над новым API для браузера Chrome, который призван защитить пользователей от определенного типа XSS-атак, в частности, XSS через DOM (DOM Based XSS). Специалисты планируют протестировать функцию под названием Trusted Types на протяжении 2019 года (в версиях Chrome 73 - 76) и, если все пойдет как положено, новый функционал станет постоянным.

Эксперты различают несколько типов XSS: «отраженные» («reflected XSS» или «Type 1»), «хранимые» («stored XSS» или «Type 2»), XSS через DOM. Последняя, по сути, представляет собой уязвимость в исходном коде сайта, которой злоумышленники могут воспользоваться для совершения различных действий – кражи файлов cookie, манипуляции содержимым страницы, переадресации пользователей и пр.

Задача Trusted Types заключается в предотвращении подобного рода атак путем блокировки «точек внедрения» кода в код web-сайта. Включить новую функцию владельцы сайтов смогут в настройках CSP (Content Security Policy), выставив определенное значение. Более подробно новый функционал описан в блоге Google.

Trusted Types станет второй функцией Chrome, направленной на защиту от XSS-атак, после фильтра XSS Auditor, представленного в выпущенной в 2010 году версии Chrome 4.

XSS в DOM-модели возникает на стороне клиента во время обработки данных внутри JavaScript сценария. Данный тип XSS получил такое название, поскольку реализуется через DOM (Document Object Model) — не зависящий от платформы и языка программный интерфейс, позволяющий программам и сценариям получать доступ к содержимому HTML и XML-документов, а также изменять содержимое, структуру и оформление таких документов. При некорректной фильтрации возможно модифицировать DOM атакуемого сайта и добиться выполнения JavaScript-кода в контексте атакуемого сайта.» ***(В Chrome появится защита от XSS-атак через DOM // SecurityLab.ru (https://www.securitylab.ru/news/497983.php). 18.02.2019).***

***

«На сайте проекта NoMoreRansom доступна свежая сборка бесплатной утилиты для восстановления файлов, зашифрованных GandCrab. Согласно пресс-релизу Европола, декриптор разработали специалисты компании Bitdefender при поддержке правоохранительных органов ряда стран, а также ФБР. Обновленная программа успешно устраняет последствия атаки всех прежних штаммов вымогателя — вплоть до версии 5.1.

Этот релиз полезного приложения стал третьим за последние 12 месяцев. Впервые утилита появилась в свободном доступе в феврале 2018 года. По заверениям разработчиков, она помогла восстановить данные более чем 2 тыс. домашних пользователей и компаний. В октябре того же года ее заменила следующая версия декриптора. Обновленную программу с тех пор скачали более 400 тыс. раз, она помогла почти 10 тыс. жертв зловреда сэкономить более пяти миллионов долларов.

Несмотря на обновления, с точки зрения пользователя принцип работы утилиты остается неизменным. Чтобы вычислить ключ для расшифровки данных, декриптору требуется не менее пяти закодированных файлов и сообщение с требованием выкупа. Зловред помещает текст записки на обои рабочего стола и во все пораженные папки компьютера.

По оценке Европола, GandCrab ныне является самым распространенным шифровальщиком, он опередил даже таких известных зловредов, как SamSam и Locky. К сожалению, его авторы очень ревностно следят за работоспособностью своего детища и оперативно обновляют его, как только ИБ-экспертам удается подобрать ключи. Так случилось и на этот раз: Bleeping Computer уже рапортует о появлении новой версии GandCrab — 5.2, против которой только что доработанный декриптор бессилен.

Для предотвращения заражения шифровальщиками пользователям рекомендуется установить систему многоуровневой антивирусной защиты. Следует также регулярно выполнять резервное копирование данных и не открывать вложения в подозрительных email-сообщениях.» ***(Dmitry Nazarov. Специалисты по безопасности обновили декриптор для GandCrab // Threatpost (https://threatpost.ru/spetsialisty-po-bezopasnosti-obnovili-dekriptor-dlya-gandcrab/31243/). 20.02.2019).***

***

«Компания Munich Re, занимающая лидирующие позиции на рынке киберстрахования, выбрала аналитическую платформу CyberCube для моделирования и контроля кибернетических рисков.

Об этом УкрСтрахованию известно из пресс-релиза CyberCube, в котором подчеркивается растущее влияние кибернетических угроз и связанное с этим развитие киберстрахования во всем мире. «Экстремальное кибер-событие может оказать сильное влияние на тысячи организаций одновременно, и накопление обязательств по нескольким застрахованным портфелям может привести к значительным убыткам», — говорится в пресс-релизе.

С помощью цифровой платформы CyberCube перестраховщик из Германии Munich Re сможет проводить моделирование киберрисков по различным сценариям и ускорить управление ими. Сообщается, что CyberCube использует несколько источников данных и новейшую систему анализа рисков Symantec…» ***(Munich Re для моделирования кибернетических рисков использует платформу CyberCube // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/munich-re-dlya-modelirovaniya-kiberneticheskih-riskov-ispolzuet-platformu-cybercube). 28.02.2019).***

***

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

IV всеукраїнська науково-практична конференція «Перспективні напрями захисту інформації», 02-06 вересня 2018 року : зб. тез. - Одеса : ОНАЗ, 2018. - 103 с.

Зі змісту:

- Костяк М.Ю., Пархуць Л.Т. Підвищення ефективності функціонування захищених інформаційних мереж спеціального призначення;
- Перловский Л.И., Тихонов В.И. Методологические аспекты искусственного интеллекта и проблемы кибербезопасности;
- Кінзерявий В.М., Фесенко В.О. Підвищення рівня захищеності об’єктів критичної інфраструктури за допомогою використання системи біометричної ідентифікації;

- Матієвський В.В. Використання машинного навчання для ідентифікації аномалій та кібератак;
- Шевченко С.О. Поліпшення обробки сигналів в технічних засобах виялення каналів витоків інформації;
- Щепилов Е.А., Гунченко Ю.А. Защита облачных данных;
- Кононович І.В., Стайкуца С.В., Кононович В.Г., Баранюк Г.А. Тенденції технік та технологій кібербезпеки кіберфізичних систем на прикладі телекомунікаційних систем;
- Тихонов А.С. Повышение защищенности интерфейса Wi-Fi в публичных сетях доступа к интернет;
- Голев Д.В., Угрік В.А. Аналіз вразливостей безпровідних мереж за допомогою ОС KALI Linux.

Шифр зберігання НБУВ: ВА827895.

***

Актуальні проблеми реформування кримінальної юстиції : матеріали міжнар. наук.-практ. конф., 20 квіт. 2018 р. - Одеса, 2018. - 151 с.

Зі змісту:

- Юхно О.О. Проблемні питання протидії кіберзлочинцям та підготовки слідчих, детективів і оперативних працівників цього напряму;
- Кондратюк М.В. Професійна готовність майбутніх спеціалістів із забезпечення комп'ютерної безпеки;
- Трапезников В.И. Киберприступность: актуальные проблемы противодействия.

Шифр зберігання НБУВ: ВА827304.

***

Геостратегічні пріоритети України в політичній, економічній, правовій та інформаційній сферах : матеріали міжнар. наук.-теорет. конф., 19 жовт. 2017 р., м. Київ. - Одеса : Фенікс, 2017. - 207 с.

Зі змісту:

- Лісовський П.М., Лісовська Ю.П. Кібербезпека як інформаційна стратегія якості в міжнародно-правовому вимірі;
- Петров В.В. Щодо розбудови системи забезпечення кібербезпеки.

Шифр зберігання НБУВ: ВА827897.

***

Інформаційне забезпечення розслідування злочинів : матеріали VI Міжнар. круглого столу, 24 трав. 2018 р., м. Одеса. - Одеса, 2018. - 126 с.

Зі змісту:

- Калугін В.Ю. Участь спеціалістів у ході кримінального провадження щодо кіберзлочинів.

Шифр зберігання НБУВ: ВА827618.

***

Ткаченко О. Кіберпростір і кібербезпека: проблеми, перспективи, технології / О. Ткаченко, К. Ткаченко // Цифрова платформа: інформаційні технології в соціокультурній сфері. - 2018. - Вип. 1. - С. 75-86.

Розглянуто підходи до тлумачення понять кіберпростору та кібербезпеки, що пов'язані як з організаційними, так і технічними аспектами. Висвітлено сутність кіберпростору та кібербезпеки з позицій державного забезпечення цієї сфери інформаційної діяльності. Визначено основні проблеми кібербезпеки та шляхи їх розв'язання. Подано види комп'ютерних вірусів та описано основні шляхи їх усунення та знешкодження. Запропоновано шляхи забезпечення кібербезпеки інформаційного простору підприємств та комп'ютерних мереж (в тому числі й Інтернет).

Шифр зберігання НБУВ: Ж74805.