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

№ 5 (травень)

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. – №5 (травень) . – 79 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

«…Військовослужбовці Маріупольського загону морської охорони зі складу Об'єднаних сил отримали можливість пройти профільне навчання із кібербезпеки на безкоштовній основі.

В одному з провідних комп'ютерних навчальних закладів Маріуполя, за ініціативи його керівництва, морські прикордонники вивчають кібершифрування, захист комп'ютерів у мережі, сучасні програми, програмування та багато інших дисциплін. Після завершення навчання військовослужбовці отримають диплом за напрямком підготовки «Кібербезпеки».

Директор комп'ютерної академії Ігор Смаглій власною ініціативою запропонував командуванню Маріупольського загону морської охорони співпрацю із навчання…» ***(Морські прикордонники зі складу ООС навчаються основам кібербезпеки // Громадсько-політичний Інтернет-портал «Рупор Житомира» (http://ruporzt.com.ua/ukraina/125748-morsk-prikordonniki-z-skladu-oos-navchayutsya-osnovam-kberbezpeki.html). 06.05.2019).***

***

«Основанная в 2010 году группа украинских киберактивистов FalconsFlame заявила о прекращении участия в работе Украинского киберальянса. Своё решение FalconsFlame объяснили «пророссийским реваншем».

Соответствующее сообщение появилось на странице Украинского киберальянса в Facebook…

– За эти годы мы провели большое количество эпических операций, большинство из которых не было опубликовано по понятным причинам, но мы не можем работать против врага, когда нет надежного тыла, – говорится в заявлении.

Украинский киберальянс – сообщество украинских киберактивистив из разных городов Украины и уголков мира, возникшее весной 2016 года для противодействия российской агрессии в Украине путем объединения двух групп киберактивистов FalconsFlame и Trinity. Также в УКА входят группа хактивистов RUH8 и отдельные участники КиберХунты. На счету FalconsFlame – взломы пропагандистской блогерской платформы CONT.WS, хищение данных сотрудника ФСИН РФ Николая Владимировича Рейхенау, воевавшего на Донбассе, взлом страницы российского террориста Геннадия Дубового и многие другие операции…

Sean Townsend также подчеркнул, что альянс отнюдь не расформирован, а находится в «спящем режиме», но пока неизвестно, каким будет формат взаимодействия УКА и новой власти…» ***(Владимир Кондрашов. Хакерская группа FalconsFlame прекращает свою работу в составе Украинского киберальянса // Internetua (https://internetua.com/hakerskaya-gruppa-falconsflame-prekrasxaet-svoua-rabotu-v-sostave-ukrainskogo-kiberalyansa). 20.05.2019).***

***

«Якщо хтось думає, що кібербезпека держави — це про умовних хакерів, які ламають сайти та крадуть гроші, і це не стосується вас персонально, то ви помиляєтеся. Хакери можуть впливати на життя кожного, наприклад, дистанційно

вимкнути електроенергію в цілій області, заблокувати роботу аеропорту, водоканалу. Що робить держава, щоб захиститися від таких атак, та що потрібно знати для власної кібербезпеки, розповів «Детектору медіа» директор і співзасновник компанії Berezha Security Костянтин Корсун після виступу на конференції з практичної кібербезпеки NoNameCon…

Загрози для державної безпеки ми побачили дуже чітко, коли були кібератаки на «Прикарпаттяобленерго». Тоді, щоб подивитися, що теоретична можливість такої атаки реалізована практично, злетівся весь інформаційний світ…

Ще були атаки на аеропорти, медіа, банки, фінансово-транспортну інфраструктуру…

Якщо можна віддалено перекрити воду чи відключити хакерськими методами цілий регіон від електроенергії на 5-6 годин, то це важливий виклик… Якщо не приділяти уваги питанням кібербезпеки, то це впливатиме навіть на тих людей, які нічого не чули про кібербезпеку.

Є чимало випадків кричущої некомпетентності людей, які мають захищати ці системи. Тобто, це рівень хакера-школяра — настільки легко зламати систему інфраструктурних об’єктів…

Проблема в тому, що в нас на абсолютній більшості державних органів і на практично всіх об’єктах критичної інфраструктури не дотримано мінімальних вимог з безпеки…

Кібербезпека на державному рівні залежить від обізнаності звичайних людей, які працюють у компаніях і держустановах. Проблема в тому, що в держустановах не завжди є навіть системний адміністратор, а тим паче — фахівець із кібербезпеки…

Кібероперації проти України — це лише складова загальних операцій з боку Росії. Це такий додатковий вектор атаки, щоби вплинути на громадську думку і змінити її на більш проросійську.

Яким чином такі кібератаки впливають? Їхня кінцева мета — це розум українців. «Якщо на 6 годин відключили електроенергію, значить влада не може забезпечити мою безпеку», — думають люди.

Деякі кібератаки проводилися з тактичними цілями — випробувати нові методи, перевірити ефективність нової зброї, показати замовнику свої можливості…

Що робить держава? Щось робить. Але велике питання, наскільки ефективно. У мене найменше питань до роботи правоохоронних органів — кіберполіції та контррозвідки СБУ. Вони виконують точкові завдання. Це дуже вузька галузь — знаходити злочинців та попереджувати кіберзлочини, але вони не можуть займатися просвітою.

Держава цим не займається. У нас є координаційний центр РНБО і шість відомств, які працюють для власних потреб, як-от розвідка, Міноборони чи Нацбанк.

Державна служба спеціального зв'язку та захисту інформації України, яка начебто має відповідати за інформаційну безпеку країни, — некваліфікована. У багатьох нормативних актах вони значаться як відповідальні за все, що

відбувається як у державних, так і приватних компаніях, що стосується кібербезпеки. Але вони мають застарілі технології та підходи ще з 90-х років.

Держспецзв'язку виконує функцію регулятора. На мій погляд, дуже неефективно. Наприклад, вони вимагають створення КСЗІ (комплексна система захисту інформації, —ред.). Але ця система застаріла. А вони штрафують, тиснуть і пропонують фірми, які все це зроблять за великі гроші. Я їх публічно критикую і наголошую, що це відомство потрібно або ліквідувати, або значно скоротити.

Кіберполіція вже після скоєння злочину займається розслідуванням. Нацбанк опікується лише фінансовим сектором. Так само вузький профіль має Міноборони та контррозвідка СБУ.

Вихід — масова просвіта. Системи найбільш вразливі через елементарну неуважність та необізнаність людей, через яких хакери отримують доступ до інформаційних систем. Я переконаний, що масова просвіта — це правильна стратегія. Вона не дасть швидких результатів. Вона потребує величезних зусиль, ресурсів, але якщо закласти на це два роки, то буде видно результат.» ***(Володимир Рихліцький. Чому Україна є вразливою для хакерських атак і як це виправити – розповідає експерт із кібербезпеки // MediaSapiens (https://ms.detector.media/web/cybersecurity/chomu_ukraina_e_vrazlivoyu_dlya_khakerskikh_atak_i_yak_tse_vipraviti_rozpovidae_ekspert_iz_kiberbezpeki/). 20.05.2019).***

***

Національна система кібербезпеки

«В Одеському облуправлінні СБУ відкрили регіональний центр кібербезпеки…

Фахівці захистять від кібератак такі об'єкти, як облдержадміністрація, АТ "Укрзалізниця", морські торговельні порти.

"Основне завдання новоствореного центру – ефективне реагування на кіберінциденти і кібератаки, цілями яких є державні електронні ресурси і об'єкти критичної інфраструктури… Готові співпрацювати і з іншими потужними бізнес-структурами, а також надавати їм бази можливих кібератак", – зазначив керівник Управління СБУ в Одеській області.

Як відомо, це третій регіональний центр кібербезпеки в Україні, перші два відкрито у Дніпрі та Сумах.» ***(Новий центр кібербезпеки СБУ відкрили в Одесі // #ШоТам (https://shotam.info/novyy-tsentr-kiberbezpeky-sbu-vidkryly-v-odesi/). 04.05.2019).***

***

Правове забезпечення кібербезпеки в Україні

«…Группа народных депутатов зарегистрировала в Верховной Раде проект постановления об обращении парламента к правительству

относительно создания министерства по вопросам инноваций, цифровизации и будущего Украины. Соответствующий зарегистрирован на сайте ВР под номер 10297.

Предполагается, что новое ведомство должно стать центральным органом исполнительной власти для обеспечения формирования и реализации государственной политики в сферах развития общества, инноваций, информатизации, электронных коммуникаций, радиочастотного ресурса Украины, почтовой связи, информационной безопасности и кибербезопасности, единого электронного пространства.

Один из авторов проекта, председатель парламентского комитета по вопросам информатизации и связи Александр Данченко написал у себя в Facebook, благодаря созданию нового министерства будут закрыты 18 разных департаментов в Кабмине, расформировано Агентство по вопросам электронного управления, сокращены функции еще в пяти министерствах.

Данченко пишет, что такое сокращение сэкономит бюджету 1,2 млрд грн в год. А эффективная работа нового министерства, по его подсчетам, должна добавлять минимум 90 млрд. грн в бюджет ежегодно.» ***(В Украине хотят создать министерство будущего // Информационное агентство ЛІГАБізнесІнформ (https://news.liga.net/economics/news/v-ukraine-hotyat-sozdat-esche-odno-ministerstvo-buduschego). 20.05.2019).***

***

«27 травня Кабінетом міністрів України зареєстровано у Верховній Раді проект закону №10328 про критичну інфраструктуру та її захист.

Уряд має на меті створити умови для формування та ефективної реалізації державної політики у сфері захисту критичної інфраструктури.

Наразі, за словами представників Кабміну, світові тенденції до посилення загроз природного та техногенного характеру, підвищення рівня терористичних загроз, збільшення кількості та підвищення складності кібератак, а також пошкодження інфраструктурних об'єктів у східних та південних регіонах України внаслідок збройної агресії РФ зумовили актуалізацію питання захисту систем, об'єктів і ресурсів, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення національної безпеки.

Проектом передбачено створення окремого державного органу зі спеціальними повноваженнями, який буде скеровувати інші органи державної влади та управління у сфері захисту критичної інфраструктури. Пропонуються також визначення основних засад державної політики у сфері захисту критичної інфраструктури, заходи із врегулювання правових і господарських відносин, що виникають під час такої діяльності, повноважень державних органів у сфері захисту критичної інфраструктури.

Окремо в законопроекті зазначені завдання з формування і реалізації державної політики захисту критичної інфраструктури України і створення державної системи захисту критичної інфраструктури, такі як:

– забезпечення безпеки, стійкості та цілісності критичної інфраструктури України;

– попередження кризових ситуацій, що порушують стале функціонування критичної інфраструктури;

– створення та організація державної системи захисту критичної інфраструктури, у тому числі шляхом визначення уповноваженого органу у справах захисту критичної інфраструктури України, а також компетенцій і повноважень у сфері захисту критичної інфраструктури інших суб'єктів державної системи захисту критичної інфраструктури;

– розробка нормативно-правової бази з питань правового регулювання безпеки на об'єктах критичної інфраструктури;

– розробка та реалізація державних цільових програм із захисту критичної інфраструктури;

– розробка комплексу заходів з виявлення, запобігання та ліквідації наслідків інцидентів на об'єктах критичної інфраструктури України;

– встановлення обов'язкових вимог із забезпечення безпеки об'єктів критичної інфраструктури, їхньої захищеності на всіх етапах життєвого циклу, в тому числі під час створення, прийняття в експлуатацію, модернізації;

– аналіз викликів та загроз, що впливають на стійкість критичної інфраструктури, оцінка стану її захищеності;

– встановлення науково обґрунтованих підходів до аналізу результативності державної політики у сфері захисту критичної інфраструктури.

Також законом регулюватимуться питання критеріїв віднесення об'єктів до критичної інфраструктури, категоризації об'єктів критичної інфраструктури, складення та ведення національного переліку об'єктів критичної інфраструктури тощо.» ***(У Кабміні пропонують врегулювати питання критичної інфраструктури // Судово-юридична газета (https://sud.ua/ru/news/publication/142656-u-kabmini-proponuyut-vregulyuvati-pitannya-kritichnoyi-infrastrukturi). 28.05.2019).***

***

Кібервійна проти України

«Голова Центральної виборчої комісії України Тетяна Сліпачук під час панельної дискусії "Моніторинг зовнішнього втручання в українські президентські вибори 2019 року" заявила, що ЦВК не стикалася з масивними кібератаками під час президентських виборів. Її слова у Twitter цитує журналістка Тетяна Магазова…

"Цього разу не було масштабних хакерських атак на ЦВК. Однак найбільше ми зазнавали серйозних дезінформаційних атак з метою делегітимізувати українські вибори", - сказала Сліпачук…» ***(Саша Картер. Голова ЦВК розповіла про кібератаки під час виборів президента України // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1800513-golova-tsvk-rozpovila-pro-kiberataki-pid-chas-viboriv-prezidenta-ukrayini). 15.05.2019).***

***

«Під час президентської виборчої кампанії Служба безпеки України виявила в соцмережах близько 400 акаунтів, через які російські спецслужби планували поширювати фейкову інформацію. Про це на панельній дискусії "Моніторинг зовнішнього втручання в українські президентські вибори 2019" повідомив заступник глави СБУ Олег Фролов…

Крім того, за його словами, в лютому цього року СБУ зареєструвала кілька кібератак на інформаційні ресурси Центральної виборчої комісії.

"29 березня цього року, якраз напередодні першого туру президентських виборів, ми зареєстрували відправку фішингових електронних листів на електронні адреси членів Центральної виборчої комісії, і наявна у нас інформація дозволяє нам сказати, що цей вірус був відправлений спецслужбами РФ. Після розшифровки цього вірусу ми побачили деякі коментарі в програмі російською мовою", - розповів заступник голови СБУ…» ***(Саша Картер. Під час виборчої кампанії СБУ виявила 400 акаунтів з фейками РФ // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1800512-pid-chas-viborchoyi-kampaniyi-sbu-viyavila-400-akauntiv-z-feykami-rf). 15.05.2019).***

***

«Социальные сети Facebook и Instagram удалили 97 аккаунтов, страниц и групп, через которые якобы «осуществлялись скоординированные акции» в отношении Украины. Как утверждается в сообщении главы департамента кибербезопасности Facebook Натаниэла Глейшера, размещенном в на информационном сайте Facebook, речь идет о двух «не связанных друг с другом операциях, исходящих из России, в которых использовалась одна и та же тактика»:

«Мы удалили 97 учетных записей Facebook, страниц и групп, которые были причастны к скоординированному недостоверному поведению, в рамках работы единой сети из России, деятельность которой сосредоточена на Украине.

Люди, стоящие за этими действиями, использовали фальшивые аккаунты для управления страницами и группами, распространения их контента и повышения вовлеченности, а также для привлечения людей к внеплатформенному домену, который собирает различный веб-контент. Они часто публиковали новости о местных и политических новостях, включая такие темы, как: военный конфликт в Восточной Украине; российская политика; политические новости в Европе; политика в Украине и гражданская война в Сирии.

Мы уже отключили многие учетные записи участвующих в этой операции пользователей за различные нарушения, включая поддельные личности, и некоторые из обнаруженных нами действий были связаны с учетными записями, которые мы удалили в ходе предыдущих принудительных действий».

В качестве примера материалов, подвергшихся удалению, приводится пост с анонимным комментарием на высказывания главы украинского МИД Павла Климкина об украинско-российских отношениях, а также пост под заголовком «В МИД РФ обвинили ВСУ в умышленном нападении на российских журналистов под Донецком».

Удаленные аккаунты и страницы были найдены «в ходе продолжающихся внутренних расследований предполагаемых скоординированных действий,

имеющих отношение к России», — указывается в сообщении. Информация о предпринятых мерах «передана в правоохранительные органы, политикам и партнерам по бизнесу».

Кроме этого было удалено ещё 21 аккаунтов, которые сосредоточены на Австрии, Прибалтике, Германии, Испании, Украине и Великобритании…» ***(Facebook отчитался об удалении сети фальшивых российских аккаунтов // РосКомСвобода (https://roskomsvoboda.org/46977/). 07.05.2019).***

***

«Усі спроби пробити контур кіберзахисту державних органів, залучених до виборів, були локалізовані. Про це повідомив секретар Ради національної безпеки і оборони України Олександр Турчинов на засіданні Національного координаційного центру кібербезпеки…

Зі слів Турчинова, незважаючи на спроби російських спецслужб пробити контур кіберзахисту державних органів, залучених до виборів президента України, "вдалося забезпечити безперебійне функціонування системи "Вибори" та Державного реєстру виборців".

Секретар РНБО заявив, що вчасні упереджувальні заходи та координація роботи суб'єктів забезпечення кібербезпеки були достатньо ефективними.

Турчинов наголосив, що суб'єкти забезпечення кіберзахисту здатні "своєчасно виявити, запобігти і нейтралізувати реальні і потенційні загрози кібернетичного характеру в інформаційно-телекомунікаційних системах ЦВК під час наступних парламентських виборів".

Також на засіданні обговорювалося питання впровадження організаційно-технічної моделі кіберзахисту, що передбачає реалізацію на системній основі комплексу заходів, спрямованих на оперативне реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості державних інформаційних та комунікаційних систем.

Крім того, були заслухані результати розслідування кібератак на інформаційно-телекомунікаційні системи державних органів, об'єкти критичної інфраструктури, які відбулися в останні роки та завдали шкоди нацбезпеці в інформаційній і економічній сферах, та ефективність міжнародного співробітництва у цьому питанні…» ***(Ясамін Мохаммад. Турчинов: усі спроби пробити контур кіберзахисту залучених до виборів органів були локалізовані // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1800664-turchinov-usi-sprobi-probiti-kontur-kiberzakhistu-zaluchenikh-do-viboriv-organiv-buli-lokalizovani). 16.05.2019).***

***

«Росія перекинула до кордону з Україною нову установку для виявлення і попередження комп'ютерних атак "СОПКА". Керівництво Луганської військово-цивільної адміністрації вважає, що Кремль готується до здійснення нових кібератак.

Про це повідомив заступник керівника Луганської ОВЦА, полковник СБУ Юрій Клименко у Facebook…» ***(Керівництво Луганської області очікує на***

посилення Кремлем кібератак // UATV (https://uatv.ua/kerivnytstvo-luganskoyi-oblasti-ochikuye-posylennya-kremlem-kiberatak/). 28.05.2019).

***

Боротьба з кіберзлочинністю в Україні

«Суд арестовал имущество мужчины, которого подозревают в продаже данных со взломанных им компьютеров. Полиция несколько месяцев «вела» злоумышленника и даже провела санкционированную контрольную закупку…

Согласно материалам дела, в следственное подразделение поступил рапорт начальника отдела противодействия киберпреступности в Николаевской области Причерноморского Управления киберполиции Департамента киберполиции НПУ о выявлении факта распространения вредоносных программных средств жителем Николаева.

При проведении оперативно-розыскных мероприятий следствие установило, что подозреваемый, действуя по предварительному сговору с неустановленными лицами в течение января-сентября 2018 года, «осуществлял приготовления к распространению вредоносного программного обеспечения с целью получения конфиденциальной информации об учетных записях пользователей с пораженных компьютеров для их последующей продажи на форумах хакерской тематики».

Полицейские установили, что в сентябре прошлого года обвиняемый разместил на форуме exploit.in объявления о продаже имеющихся у него логов – информации с браузеров пораженных компьютеров, логинов и паролей от электронных платежных систем, электронных кошельков криптовалют, по цене 15 долларов США за один полный лог – полную информацию из всех браузеров одного пораженного компьютера. Стало известно, что у мужчины есть доступ к информации с 509 зараженных машин.

19 октября полицейские провели «контроль за совершением преступления» – закупили у подозреваемого через мессенджер Telegram 11 логов за 2800 гривен, о чем был составлен соответствующий протокол. Протокол в дальнейшем использовали как основание для начала досудебного расследования.

В ходе обыска в доме у жителя Николаева обнаружены и изъяты банковские карточки украинских и зарубежных банков, несколько мобильных телефонов и компьютерная техника. Спустя практически 5 месяцев после обыска, 3 мая, суд наложил арест на изъятое имущество.

Следствие продолжается. Мужчине грозит до двух лет лишения свободы.» ***(Владимир Кондрашов. Украинский хакер продавал в сети данные 509 зараженных компьютеров // Internetua (https://internetua.com/ukrainskii-haker-prodaval-v-seti-dannye-509-zarajennyh-kompyuterov). 13.05.2019).***

***

«Суд закрыл уголовное дело в отношении ранее несудимого безработного украинца, который распространил вредоносное программное обеспечение, предназначенное для взлома банкоматов…

Согласно обвинительному акту, 25 марта 2018 мужчина с помощью своего iPhone, «действуя умышленно, с целью распространения вредоносного программного средства, предназначенного для несанкционированного вмешательства в работу электронно-вычислительных машин», с помощью мессенджера «Telegram» со своего аккаунта прислал другому пользователю вредоносную программу для взлома банкоматов.

– Вредоносная программа включает в себя конфигурацию файлов, предназначенных для несанкционированной выдачи наличных с АТМ – автоматического кассового аппарата, который является электронным программно-техническим комплексом со встроенной специализированной электронно-вычислительной машиной (банкомата). Каждый модуль выполняет свою функцию, а именно «cQdecalc.exe» - генерирует пароли для запуска программы на банкомате, «Stimulator» - показывает количество и номинал банкнот в кассетах банкомата, «Cutlet» - основной модуль для выдачи денег с банкомата, – говорится в определении суда.

Действия обвиняемого, которые выразились в распространении вредных программных средств, предназначенных для несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров), органом предварительного расследования квалифицированы по ч. 1 ст. 361-1 УК Украины.

Обвиняемый на судебном заседании свою виновность в совершении уголовного преступления признал полностью, искренне раскаялся в содеянном, не отрицал правильности установленных фактических обстоятельств и обоснованности объявленного ему подозрения. Суду он сообщил, что не владел информацией о вреде данного ПО и узнал об этом от полиции. В связи с искренним раскаянием и полным признанием вины мужчина в подготовительном судебном заседании представил суду ходатайство об освобождении его от уголовной ответственности на основании ст. 45 УК Украины. Прокурор против ходатайства не возражал.

Суд данное ходатайство утвердил и уголовное дело закрыл, однако теперь безработному придется найти деньги, затраченные на привлечение эксперта к делу – 4 576 гривен.» ***(Владимир Кондрашов. Украинскому хакеру суд простил распространение ПО для взлома банкоматов // Internetua (https://internetua.com/ukrainskomu-hakeru-sud-prostil-rasprostranenie-po-dlya-vzloma-bankomatov). 08.05.2019).***

***

«Суд отправил под домашний арест одного из хакеров, которым, по версии следствия, удалось взломать счета 33 клиентов ПриватБанка и украсть у украинцев более 800 тысяч гривен. Уголовное дело было открыто ещё в апреле 2018 года по подозрению в совершении уголовных преступлений, предусмотренных частями 2 и 3 статьи 185 («Кража») и частью 2 ст. 361

(«Несанкционированное вмешательство в работу электронно-вычислительных машин») УК Украины…

В ходе досудебного расследования было установлено, что двое граждан Украины осуществляли поиск и сканирование портов, IP-адресов с отрытым портом RDP.

– В дальнейшем найденные компьютеры с открытым RDP-портом проходили проверку на подбор паролей и логинов, и в результате совпадения проводилось подключение к удаленному компьютеру, после чего запускалось вредоносное программное обеспечение, собиравшее логины, пароли, и автоматически осуществлялся запуск программы «KeyLoger», которая была встроена в указанное вредоносное ПО, «KeyLoger», в свою очередь, сохраняла каждый натиск клавиш клавиатуры пользователя, – говорится в решении суда. – Таким образом двое граждан получали доступ к системе «Клиент-Банк» АО КБ «ПриватБанк», после чего осуществляли несанкционированное списание денежных средств со счетов на заранее подконтрольные карточные счета, а в дальнейшем сами их и обналичивали в банкоматах или конвертировали в криптовалюты на кошельки.

Досудебным расследованием установлено 33 потерпевших лица из числа жителей Харьковской, Донецкой, Запорожской, Житомирской, Днепропетровской, Львовской, Закарпатской, Ровенской, Николаевской областей и Киева, у которых аналогичным способом вышеуказанные лица, в результате несанкционированного вмешательства, похищали денежные средства со счетов, открытых в ПАО КБ «ПриватБанк».

Размер ущерба, причиненного уголовным правонарушением, составляет 804 тысячи 233 гривны 07 копеек.

Решением суда один из подозреваемых был отправлен под домашний арест (с 23-00 по 6 часов утра). Хакерам светит до шести лет лишения свободы.» ***(Владимир Кондрашов. Хакеры украли со счетов ПриватБанка 800 тысяч гривен // Internetua (https://internetua.com/hakery-ukrali-so-scsetov-privatbanka-800-tysyacs-griven). 03.05.2019).***

***

«В операции были задействованы полицейские из США, Болгарии, Германии, Грузии, Молдовы и Украины. Злоумышленники при помощи вредоносной программы GozNym перехватывали пароли доступа пострадавших к онлайн-банкам. Членов группы рекрутировали из тех, кто рекламировал соответствующие "услуги" в интернете, сообщили на брифинге в штаб-квартире Европола - полицейской службы Евросоюза - в Гааге. Киберпреступность Десяти членам группировки предъявлены обвинения в США по целому ряду статей, включая кражу денег и их отмывание через американские и зарубежные банковские счета. Среди них есть пять граждан России, все из которых скрываются, как полагают в Европоле, на российской территории. В их числе - создатель трояна GozNym, также отвечавший за применение этой программы. Среди прочего, он сдавал ее в аренду другим преступникам. Нескольким членам группировки предъявлены обвинения еще в нескольких странах: Среди жертв

преступной группировки были небольшие бизнесы, юридические конторы, международные корпорации и благотворительные организации.

В результате оперативной деятельности полиции сразу нескольких стран стало ясно, насколько распространенной стала продажа или сдача в аренду вредоносных программ, говорит Алан Вудворд, профессор информатики из Суррейского университета в Англии. "Разработчики вредоносных программ продают свой "товар" преступникам, чтобы те могли взломать банковские счета, - говорит он. - Подобные преступные "услуги" предлагаются все чаще, и организованные преступные группировки теперь могут перейти от традиционной торговли наркотиками к гораздо более доходной киберпреступности". Что такое GozNym? Это гибрид из двух вредоносных программ - Nymaim и Gozi. Первая из них - так называемый сбрасыватель (dropper), программа, рассчитанная на то, чтобы незаметно установить в устройство вредоносную программу. До 2015 года Nymaim использовалась преимущественно для захвата компьютеров с требованием выкупа за восстановление доступа к ним. Gozi существует с 2007 года. Программа часто видоизменялась, но ее основной целью всегда было получение доступа к финансовой информации. Эту программу использовали не раз в кибератаках на американские банки. Соединение двух программ создало, по выражению экспертов, "двухголового монстра".» ***(Раскрыта группа киберпреступников, применявших троян GozNym // Новости Великобритании на русском языке (https://theuk.one/raskryta-gruppa-kiberprestupnikov-primenyavshix-troyan-goznym-sredi-nix-pyatero-rossiyan/). 16.05.2019).***

***

«Неизвестные вмешались в работу автоматизированных систем и ПЭВМ одного из филиалов АО «Ощадбанк» и завладели денежными средствами клиентов банка. Сумма имущественного вреда устанавливается, однако уже известно, что с 12 счетов клиентов финучреждения украдено более 200 тысяч гривен…

Как стало известно, 20 марта было открыто уголовное дело по статье 362 (ч.1) Уголовного кодекса Украины («Несанкционированные действия с информацией, которая обрабатывается в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или хранится на носителях такой информации, совершенные лицом, имеющим право доступа к ней»).

По данным следствия, неустановленные лица совершили несанкционированное удаленное вмешательство в автоматизированную систему и ПЭВМ Днепропетровского филиала АО «Ощадбанк», что к ней подключено, и в дальнейшем привело к искажению информации, которое выражается в несанкционированном формировании заявок на перевыпуск пластиковых карт клиентов банка и завладении денежными средствами клиентов.

18 января этого года при проведении тематической проверки главный ревизор отдела ревизий и контроля обнаружил сомнительные операции по перечислению средств с вкладных счетов, открытых в разных ТОБО по Днепропетровской области, по которым длительное время не было движения

средств, на карточные счета, по которым персонификация платежных карточек INSTANT была осуществлена на одном ТОБО IV, с последующим снятием средств в кассе отделения в городе Каменское.

По состоянию на 21 февраля 2019 года общая сумма имущественного ущерба составила 200 081,79 грн. по 12 счетам клиентов. На данный момент следствие получило доступ к информации о движении средств на этих 12 счетах.» ***(Владимир Кондрашов. Хакеры обокрали счета клиентов «Ощадбанка» // Internetua (https://internetua.com/hakery-obokrali-scseta-klientov-osxadbanka-). 17.05.2019).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Премьер-министр Британии Терезы Мэй встретилась с генеральным секретарем НАТО Йенсом Столтенбергом, предложив ему «британский опыт» для борьбы с киберугрозами со стороны России и Китая.

Об этом сообщает пресс-служба британского правительства…

В сообщении сказано, что глава британского правительства поблагодарила Столтенберга за внимание к вопросам кибербезопасности, предложив альянсу опыт Объединенного королевства…» ***(Мэй предложила НАТО «британский опыт» для борьбы с киберугрозами // Газета НикВести (http://nikvesti.com/news/politics/158475). 15.05.2019).***

***

«Совместные учения по отражению угроз в киберпространстве, а также совершенствованию механизмов информационной защиты проведут страны "Большой семерки" (G7) в июне. Об этом заявил в пятницу министр экономики и финансов Франции Брюно Ле Мэр, выступая на открытии конференции по информационной безопасности в финансовой сфере…

Министр заявил, что по-настоящему эффективно бороться с угрозами в информационном пространстве можно только на глобальном уровне, поэтому "принципы, которые вырабатываются внутри G7, должны быть приняты более широким кругом стран".

"G20, как первый шаг, и далее (остальные страны), как второй шаг", — пояснил он, отметив, что преступники будут искать лазейки в системах наименее защищенных стран.

"Банки и финансовые институты должны продолжать укрепляться против потенциальных кибератак", — сказал Ле Мэр.

Он напомнил о нескольких масштабных хакерских операциях с распространением вирусов Wannacry и notPetya, ущерб от которых обошелся банкам и различным коммерческим организациям в миллионы евро. По словам министра, Banque de France, выполняющий роль центрального банка страны, уже разработал меры для проверки финансовых учреждений на устойчивость к киберугрозам, признав в то же время, что банкам "еще предстоит выполнить

домашнюю работу", чтобы соответствовать повышающимся требованиям в этой сфере…» ***(Страны G7 проведут учения по кибербезопасности // Goodnews.ua (http://goodnews.ua/technologies/strany-g7-provedut-ucheniya-po-kiberbezopasnosti/). 11.05.2019).***

***

«Представники "Укрінмашу", що входить до складу концерну "Укроборонпром", обговорили із керівництвом офіційної делегації Міністерства оборони Колумбії питання співпраці з розробок систем кібербезпеки та протидії кібератакам…

"У рамках VII Міжнародної виставки оборонних технологій, озброєння та запобігання стихійним лихам "SITDEF 2019", яка відбулася у Лімі (Республіка Перу), пройшла зустріч представників "Укрінмаш", що входить до складу "Укроборонпрому", із керівництвом офіційної делегації Міністерства оборони Колумбії", - йдеться в повідомленні.

Як зазначається, директор із технологій, науки та інновацій Міноборони цієї країни Хільда Лопес Гомес та почесний консул України в Колумбії Луїс Бранд висловили зацікавленість у вивченні і застосуванні українського досвіду з розробок систем кібербезпеки та протидії кібератакам.

Йшлося також про спільні проекти зі створення двосторонніх освітніх програм з питань дослідження кібербезпеки, розробки систем захисту і зняття інформації, обміну спеціалістами.

Сторони обговорили також можливості здійснення наукових досліджень у сфері кібербезпеки у рамках інноваційних проектів Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"…» ***(Колумбія співпрацюватиме з Україною з розробок систем кібербезпеки // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (http://day.kyiv.ua/uk/news/220519-kolumbiya-spivpracyuvatyme-z-ukrayinoyu-z-rozrobok-system-kiberbezpeky). 22.05.2019).***

***

«Глава НАТО Йенс Столтенберг заявив, що альянс допомагає Європейському союзу (ЄС) боротися з кібератаками під час виборів до Європейського парламенту…

За словами Столтенберга, напередодні виборів до Європарламенту експерти НАТО обговорили з представниками ЄС відповідні заходи захисту від кіберзагроз під час голосування.

"Експертна група НАТО декілька тижнів тому зустрілась із спеціалістами ЄС, щоб обговорити конкретні заходи з протидії кіберзагрозам та дезінформації напередодні виборів до Європарламенту", - розповів він.

Столтенберг зазначив, що НАТО та ЄС в режимі реального часу здійснюють обмін інформацією про шкідливі програми та кібератаки. Він додав, що альянсу вдалося не допустити поширення присутності в інтернеті терористичної організації "Ісламська держава".

Крім того, глава НАТО заявив, що Російська Федерація "цілеспрямовано втручається в життя демократичних країн, поширюючи неправдиву інформацію та здійснюючи кібератаки".

"Це, перш за все, відбувається під час виборів", - підкреслив Столтенберг…» ***(НАТО допомагає ЄС боротися з кібератаками під час виборів // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (http://day.kyiv.ua/uk/news/260519-nato-dopomagaye-yes-borotysya-z-kiberatakamy-pid-chas-vyboriv). 26.05.2019).***

***

Світові тенденції в галузі кібербезпеки

«…Обеспечение кибербезопасности обходится компаниям в $2,3 тыс. в год за одного сотрудника. Такие данные приводятся в отчете специалистов Deloitte и Центра информационного обмена и анализа финансовых служб (Financial Services Information Sharing and Analysis Center, FS-ISAC).

Согласно отчету, банки, страховые фирмы, инвестиционные и другие компании финансовой сферы тратят на кибербезопасность 6-14% от всех средств, выделяемых в год на информационные технологии. Это примерно 0,2-0,9% от всего дохода компании или от $1,3 тыс. до $3 тыс. на каждого сотрудника.

В отчете учтены различные аспекты операций по обеспечению кибербезопасности, в том числе их управление и организация – перед кем отчитывается директор по информационной безопасности, уровень заинтересованности правления в работе директора по ИБ и приоритетные области в обеспечении ИБ.

Крупные компании тратят примерно одну пятую от всех выделяемых на кибербезопасность средств на управление идентификацией и доступом. Представители среднего и малого бизнеса тратят на это в два раза меньше. Для них приоритетными областями является защита конечных точек и сети.

По словам авторов исследования, размер суммы, выделяемой на обеспечение кибербезопасности, необязательно пропорционален уровню защищенности. То есть, большой бюджет не всегда гарантирует высокий уровень кибербезопасности.

Наиболее успешные программы по ИБ характеризуются несколькими основными чертами. Во-первых, заинтересованность в них проявляется на уровне правления. Во-вторых, информация о кибербезопасности не сосредотачивается исключительно у сотрудников IT-отдела, а распространяется по всей организации, благодаря чему ей уделяется больше внимания. Третья основная черта – согласование программы компании по ИБ с ее бизнес-стратегией.

Исследование было проведено специалистами FS-ISAC при участии компании Deloitte осенью 2018 года. В нем приняли участие 97 компаний. Среднегодовой доход 39% из них превышает $2 млрд. 23% компаний позиционируют себя как средний бизнес с годовым доходом $0,5-2 млрд.» ***(Эксперты подсчитали, во сколько компаниям обходится обеспечение ИБ // SecurityLab.ru (https://www.securitylab.ru/news/498990.php). 05.05.2019).***

***

«Американская компания Proofpoint, занимающаяся кибербезопасностью, приобрела израильский стартап Meta Networks за 120 миллионов долларов. Из них 111 миллионов — наличные, а 9 миллионов — акции Proofpoint.

Meta Networks, которая была основана два с половиной года назад, с тех пор привлекла 10 миллионов долларов от венчурных компаний BRM Capital и Vertex Ventures. Таким образом, израильскую компанию приобрели в 12 раз дороже ее стоимости.

Технология Meta Networks учитывает, что кибератака нацелена прежде всего на конкретного пользователя, а не на всю сеть, к которой он подключен. Данный принцип предполагает защиту данных пользователей отдельно от корпоративной сети, к которой они имеют доступ.

Эту технологию Proofpoint собирается использовать в своих разработках.

После приобретения сотрудники Meta Networks присоединятся к израильской команде Proofpoint.» ***(Израильский стартап против кибератак подорожал в 12 раз // Jewishnews (https://jewishnews.com.ua/economics-and-business/izrailskij-startap-protiv-kiberatak-podorozhal-v-12-raz). 07.05.2019).***

***

«…У п’ятницю, 17 травня, Єврокомісія оприлюднила нову доповідь щодо результатів дотримання глобальними інтернет-платформами, такими як Facebook, Google та Twitter, умов так званого «Кодексу поведінки проти дезінформації». До нього популярні онлайн-ресурси приєдналися напередодні виборів до Європарламенту. Про це йдеться у повідомленні від Єврокомісії.

У своєму новому документі Єврокомісія визнала ефективність «жорстких заходів», які впровадили інтернет-платформи у протидії спробам будь-як маніпулювати інформацією або ж проводити операції з розповсюдження фейків.

«Ми визнаємо прогрес, який був досягнутий Facebook, Google та Twitter, у виконанні зобов’язань щодо підвищення прозорості та захисту інформації напередодні європейських виборів. Ми також вітаємо ті жорсткі заходи, які всі три платформи здійснили проти маніпулятивної поведінки у використанні їхніх послуг, включаючи скоординовані операції проти дезінформації», — йдеться у звіті від Єврокомісії.

В той же час у Єврокомісії наголосили, що наступні зусилля варто направити на послуги, які надаються платформами, зокрема, у сфері інтернет-реклами. Там уточнили, що глобальні платформи все ще не розкривають важливі деталі власних дій, які би у майбутньому дали підстави для об’єктивного та незалежного аналізу впливу таких послуг на попередження поширення неправдивої інформації…»

(«Жорсткі заходи Facebook, Google і Twitter проти фейків дали результат» — Єврокомісія // MediaSapiens (https://ms.detector.media/web/cybersecurity/zhorstki_zakhodi_facebook_google_i_twitter_proti_feykiv_dali_rezultat_evrokomisiya/). 17.05.2019).

***

Російська Федерація та країни ЄАЕС

«Россияне смогут в интернете жаловаться МВД на киберугрозы: эксперты «Цифровой экономики» создали концепцию специального ресурса для их обращений…

Согласно концепции, МВД предстоит создать ситуационный центр по кибербезопасности с несколькими подразделениями. Вместе они будут принимать и обрабатывать обращения людей по киберугрозам и инцидентам через специальный сайт, по sms-сообщениям, электронной почте, звонкам и в соцсетях, описано в ней. Сотрудники центра будут отсеивать ложные обращения, систематизировать и вносить в базу данных спецресурса случаи реальных угроз и инциденты, оперативно предупреждать компании и ведомства, которые могут пострадать от атак, а также отвечать на обращения людей – спрашивать их о деталях случившегося и объяснять, как инициировать расследование (например, подать в МВД официальное заявление).

Представитель АНО «Цифровая экономика» подтвердил факт разработки концепции, но отказался обсуждать ее содержание. По его словам, техзадание для создания спецресурса эксперты рассчитывают написать к июню этого года, а прототип ресурса должен появиться до конца 2020 г.

Сейчас в стране не хватает единой точки сбора информации о киберпреступлениях, доступ к которой могли бы получить все заинтересованные стороны, включая массовых пользователей сети, объясняют разработчики документа смысл создания спецресурса. Они предполагают, что спецресурс наладит обмен данными в первую очередь с государственной системой защиты от компьютерных атак (ГосСОПКа) и Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ ЦБ).

Пополнять спецресурс данными смогут не только обыватели, но и его доверенные партнеры (концепция не объясняет, какие компании получат такой статус и при каких условиях) – у их данных будет особый статус достоверности. Кроме того, у данных от авторизованных через госуслуги, единую биометрическую или другие системы пользователей статус достоверности будет выше, чем у его анонимных пользователей, указывают составители концепции.

Все люди будут бесплатно пользоваться ресурсом, указано в концепции, а компании – те, для которых подключение к ресурсу сделают обязательным (условия для остальных компаний не указаны)…» ***(Светлана Ястребова. МВД может создать портал для обращений людей по киберугрозам // АО Бизнес Ньюс Медиа (https://www.vedomosti.ru/technology/articles/2019/05/16/801526-mvd-mozhet-portal). 16.05.2019).***

***

«АНО «Цифровая экономика», реализующая одноименную нацпрограмму, одобрила запуск портала, на котором россияне смогут заявлять о киберпреступлениях…

Информацию подтвердил представитель АНО. По его словам, ожидается, что к июню этого года концепцию утвердит правительство, а прототип платформы разработают до конца 2020 года. Ответственными за проект назначены МВД, ФСБ, Роскомнадзор и Центробанк.

Из документов следует, что задача нового ресурса — собирать данные о киберпреступлениях от граждан, юрлиц, госорганов и упорядочивать их. Сообщить информацию можно будет по телефону, электронной почте, через мессенджер, смс или соцсети.

Портал будет связан с другими госпорталами: Единой биометрической системой, Госуслугами, Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ), Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).

Использовать информацию об угрозах смогут зарегистрированные на платформе пользователи. Для граждан и госорганов доступ к данным будет бесплатным, для юрлиц возможно введение подписки (ее стоимость в концепции не указана).

У ресурса будет несколько уровней доступа: уполномоченный госслужащий (для сотрудников ведомств), доверенный партнер (для компаний-партнеров проекта), подписчик, активный гражданин. Все пользователи должны пройти верификацию, граждане — через Единую биометрическую систему.

GR-директор Group-IB Дмитрий Буянов отметил, что в сотрудничестве с МВД для пополнения базы данных портала заинтересованы несколько крупных компаний из сферы кибербезопасности, в том числе Group-IB. По его мнению, такой инструмент будет полезен как следователям, так и обычным гражданам…» ***(Анна Полякова. В России планируют создать портал для жалоб на кибератаки от граждан // Rusbase (https://rb.ru/news/portal-dlya-zhalob/). 16.05.2019).***

***

Інші країни

«Государственный контролер Йосеф Шапира (Joseph Shapira) опубликовал оценку готовности к кибератакам министерств Израиля, основанную на аудите, проведенном с июля 2017 по июль 2018 года.

Он провел оценку критически важной государственной инфраструктуры (Банк Израиля, нефтеперерабатывающие заводы, Железные дороги Израиля, Управление аэропортов Израиля, Электрическая компания Израиля, Израильское управление портов, Израильское налоговое управление, Израильская ассоциация

интернета и фондовая биржа Тель-Авива), правительственных министерств, вспомогательных подразделений и отраслевых ведомств.

В докладе критика сформулирована осторожно исходя из соображений безопасности. Основной вывод:только некоторые из важнейших государственных инфраструктурных агентств выполнили инструкции, изложенные в доктрине безопасности. Оценка статуса Национального управления по кибернетике "не отражает уровень готовности агентств к противодействию кибератакам".» ***(Государственный контролер: киберзащита Израиля неадекватна // ISRAland (http://www.isra.com/news/229605). 07.05.2019).***

***

«Япония может увеличить расходы для выявления телекоммуникационного оборудования с вредоносными функциями.

Специальная группа при правительстве Японии просит предусмотреть в бюджете-2020 средства для улучшения системы кибербезопасности…

Отмечается, что специальная группа по вопросам кибербезопасности при правительстве Японии обсуждала на заседании в четверг запрет, который министерство торговли США установило американским компаниям на ведение бизнеса с Huawei и связанными с ней структурами в разных странах, в том числе в Японии.

Генеральный секретарь кабинета министров Японии Ёсихидэ Суга указал на то, что нарастает угроза кибератак из-за все более активного слияния реального и виртуального миров. Он призвал членов правительства помочь обществу выработать активные превентивные меры.

Специальная группа решила просить средства для улучшения системы кибербезопасности в части обмена информацией о кибератаках.

На заседании также были представлены инструкции для компаний, предоставляющих ключевые инфраструктурные услуги, прежде всего в сфере электроэнергетики. В частности, их призывают хранить важную информацию на серверах в Японии и создавать базы данных для того, чтобы не допускать их потери при стихийных бедствиях.» ***(В Японии планируют увеличить расходы на кибербезопасность // Телеграф (https://telegraf.com.ua/mir/aziya/5020559-v-yaponii-planiruyut-uvelichit-rashodyi-na-kiberbezopasnost.html). 24.05.2019).***

***

Протидія зовнішній кібернетичній агресії

«Экс-помощник госсекретаря Соединенных Штатов Виктория Нуланд выступила с предложением создать должность «киберцаря» для «защиты от угроз со стороны России».

«Мы должны назначить «киберцаря» в Белом доме для координации национальной и внешней политики (в сфере кибербезопасности)», – сказала

Нуланд во время слушаний комитета по иностранным делам палаты представителей США…

Также она выступила за создание объединенного разведцентра, который сможет «раскрывать, ликвидировать и сдерживать кампании цифрового влияния, манипулирование избирательным процессом»…» ***(Алексей Дегтярев. Нуланд предложила создать должность «киберцаря» в Белом доме // Деловая газета «Взгляд» (https://vz.ru/news/2019/5/2/975994.html). 02.05.2019).***

***

«…Рада ЄС затвердила новий режим санкцій у відповідь на злочинну кібердіяльність. Про це йдеться в повідомленні Ради ЄС. Витік даних, крадіжка інтелектуальної власності, атаки на ІТ-інфраструктуру і викрадення секретної інформації можуть у майбутньому призвести до того, що ЄС накладе санкції на відповідальних за такі дії іноземних юридичних і фізичних осіб.Нові санкції можуть бути спрямовані на тих, хто вправляється в кібердіяльності будь-де, незалежно від їхніх національності і місцезнаходження."Рада створила рамки, що дозволяють ЄС вводити цілеспрямовані обмежувальні заходи щодо стримування і реагування на кібератаки, що несуть зовнішню загрозу для ЄС або його держав-членів, а також на кібератаки проти третіх держав чи міжнародних організацій, де обмежені заходи вважаються необхідними для досягнення цілей Спільної зовнішньої політики і політики безпеки", - йдеться в повідомленні.Кібератаки, охопні сферою застосування цього нового режиму санкцій, є такими, які мають значний вплив і які: або здійснюються з-за меж ЄС, або використовують інфраструктуру за межами ЄС, або здійснюються особами чи установами, створеними чи діяльними за межами ЄС, або здійснюються за підтримки особи чи організацій, що діють за межами ЄС.Спроби кібератак з потенційно значним ефектом також охоплюються цим режимом санкцій.Санкції передбачають заборону на поїздки до ЄС, заморожування активів для фізичних осіб і заморожування активів для суб'єктів господарювання. Крім того, особам і організаціям ЄС буде заборонено надавати гроші підсанкційним суб'єктам.Раніше повідомлялося, що Міністерство юстиції США звинуватило сімох росіян у спробах кіберзломів.» ***(ЄС затвердив механізм введення санкцій за кібератаки // Час Закарпаття (http://chas-z.com.ua/news/73326). 17.05.2019).***

***

«Компанія Huawei вважає, що указ президента США Дональда Трампа, який запроваджує режим надзвичайного стану для захисту інформаційно-комунікаційної інфраструктури США від іноземних загроз таким, що зазіхає на її законні права.

Загалом в компанії нові обмеження Вашингтона назвали "неприйнятними", повідомило видання Agence France-Presse.

Представники Huawei наголосили, що введені обмеження не зроблять США безпечнішою або сильнішою, а навпаки, це призведе до того, що Сполучені Штати будуть обмежені у виборі і їм доведеться використовувати низькоякісні та дорожчі

альтернативи. У компанії додали, що через це рішення США "будуть відставати в розгортанні мережі 5G".

15 травня президент США Дональд Трамп підписав виконавчий указ, що вводить режим надзвичайного стану Трамп запровадив надзвичайний стан у США для захисту комунікаційних мереж для захисту інформаційно-комунікаційної інфраструктури Сполучених Штатів від іноземних загроз. Пізніше стало відомо, що Міністерство торгівлі США внесло китайську компанію Huawei і пов'язані з нею юридичні особи в свій чорний список через загрозу національній безпеці…» ***(Huawei відреагувала на указ Трампа назвавши його неприйнятним // ПрАТ «Телерадіокомпанія "Люкс"» (https://24tv.ua/huawei_vidreaguvala_na_ukaz_trampa_nazvavshi_yogo_posyagannyam_na_yiyi_zakonni_prava_n1153823?utm_source=rss). 16.05.2019).***

***

«Глава МИД Великобритании Джереми Хант уверен, что РФ якобы выискивает слабые места в объектах национальной инфраструктуры в ряде стран. Об этом сообщает ТАСС, ссылаясь на предстоящую речь Ханта в рамках конференции НАТО по вопросам кибербезопасности. С ней он выступит в четверг в Лондоне. Глобальная кампания Москвы, продолжает министр иностранных дел Британии, ставит под угрозу основные правительственные сети. За последние 1,5 года Национальный центр кибербезопасности (NCSC) передал 16 странам-союзницам НАТО свои сведения и оценку о якобы киберактивности России в этих государствах…» ***(Катерина Наумкина. Глава МИД Британии сообщил о киберактивности РФ в ряде стран НАТО // Новости Великобритании на русском языке (https://theuk.one/glava-mid-britanii-soobshhil-o-kiberaktivnosti-rf-v-ryade-stran-nato/). 23.05.2019).***

***

«Президент США Дональд Трамп объявил чрезвычайное положение в США в связи с угрозами для IT-сферы страны со стороны "иностранных врагов"…

Согласно заявлению Белого дома, указ Трампа направлен на "защиту США от иностранных противников, которые все активнее создают и эксплуатируют уязвимости в инфраструктуре и услугах информационно-коммуникационных технологий".

Это предоставляет министру торговли полномочия "запрещать транзакции, представляющие неприемлемый риск для национальной безопасности", - говорится в заявлении…» ***(Трамп обеспокоен угрозами кибербезопасности в США: Ввел ЧП // DsNews (http://www.dsnews.ua/world/tramp-obespokoen-ugrozami-kiberbezopasnosti-v-ssha-vvel-16052019003100).16.05.2019).***

***

«…Внешнеполитическое ведомство Великобритании, предваряя выступления Ханта на конференции НАТО по вопросам кибербезопасности, опубликовало его речь, в которой он утверждает, что российские спецслужбы

занимаются постоянным поиском слабых мест в «критических важных объектах национальной инфраструктуры»…

Также, глава дипломатического ведомства заявил, что за последние полтора года (National Cyber Security Centre, NCSC) довел до сведения 16 стран-союзников НАТО и ряда государств, не являющихся членами альянса, свою оценку кибератиности российских спецслужб в этих странах « Как сообщает www.theuk.one. Свою речь Хант завершил призывом к этим странам быть готовыми применить в отношении России различные варианты ответных действий на любые атаки, которые не дотягивают до порогового уровня применения Пятой статьи Договора о коллективной обороне. Напомним, что президент США Дональд Трамп в одном из интервью телеканалу Fox News признал, что по его разрешению была совершена кибератака в отношении России во время выборов в Конгресс США.» ***(Глава МИД Великобритании призвал ответить на киберугрозы России // Новости Великобритании на русском языке (https://theuk.one/glava-mid-velikobritanii-prizval-otvetit-na-kiberugrozy-rossii/). 23.05.2019).***

***

«Президент США Дональд Трамп в понедельник заявил, что при его администрации была совершена кибератака в отношении России…

"Я бы предпочел этого не говорить, но вы можете быть уверены, что все это произошло - и причем произошло при моей администрации", - сказал президент США.

По словам Трампа, он долгое время не сообщал эти сведения по просьбе разведки США: "Потому что они не любят, когда я говорю.

Речь идет о российской компании "Агентство интернет исследований". В день промежуточных выборов в конгресс США, 6 ноября 2018 года, там пропал интернет. Спецслужбы США считают, что эта организация причастна к вмешательству в президентские выборы США.» ***(Трамп заявил, что США совершали кибератаку против России // NewsOboz (http://newsoboz.org/mir/tramp-zayavil-chto-ssha-sovershali-kiberataku-protiv-rossii-21052019113000). 21.05.2019).***

***

«Армия обороны Израиля 5 мая заявила, что пресекла попытку кибератаки группировки ХАМАС на израильские цели с помощью воздушного удара по зданию в Газе, где якобы работали кибер-оперативники ХАМАСа.

…реакция израильской армии на действия ХАМАСа, озвученная на ее странице в Twitter, знаменует собой первый случай в истории, когда страна ответила военной силой на кибератаку во время активной фазы конфликта.

В начале мая произошла очередная вспышка в военном конфликте Израиля и Палестины: за три дня ХАМАС выпустил более 600 ракет по Израилю, тогда как Армия обороны Израиля нанесла ответные удары по сотням целей, которые она охарактеризовала как военные. По меньшей мере 27 палестинцев и четыре израильских мирных жителя были убиты, а количество раненых превысило 100.

Армейское руководстсво Израиля заявило, что ХАМАС начал кибератаку против Израиля. Какая конкретно была цель атаки, при этом не сообщалось. Израильские СМИ утверждают, что атакующие стремились нанести «ущерб качеству жизни израильских граждан». При этом сообщалось, что атака не была сложной и ее быстро остановили.» ***(Израиль ответил авиаударом на кибератаку из Газы // Олфин (https://allfin.com.ua/news/izrail-otvetil-aviaudarom-na-kiberataku-iz-gazy/). 17.05.2019).***

***

«Компанії Microsoft Corp і Facebook Inc домовилися допомогти підвищити безпеку жовтневих виборів в Канаді, видаливши підроблені акаунти і розправившись з ботами, заявила високопоставлений урядовець Каріна Гулд у понеділок, 27 травня, виступаючи в Палаті громад на Парламентському пагорбі в Оттаві.

У минулому місяці ліберальний уряд прем'єр-міністра Джастіна Трюдо поскаржився на те, що найбільші світові компанії в області соціальних мереж не роблять досить, щоб допомогти в боротьбі з потенційним втручанням іноземців, і заявив, що Оттаві, можливо, доведеться регулювати їх діяльність, повідомляє Reuters.

У відповідь на критику і попередження обидві компанії взяли на себе зобов'язання сприяти чесності виборів, підписавши спільну декларацію.

"Ера Дикого Заходу онлайн не може продовжуватися - бездіяльність не варіант. Дезінформації бути не повинно", - сказала Гулд.

Урядовці побоюються, що зовнішні сили, серед яких називають Росію, втрутяться в вибори.

За словами Гулд, Microsoft і Facebook також домовилися активізувати зусилля по боротьбі з дезінформацією, просуванням заходів безпеки для усунення інцидентів, пов'язаних з кібербезпекою, і роз'ясненням своїх правил прийому політичної реклами.

"Я закликаю інші платформи послідувати їх прикладу найближчими днями", - додала Гулд, звертаючись до Twitter Inc і Google Alphabet Inc…» ***(Microsoft і Facebook будуть стежити за кібербезпекою на виборах у Канаді // Дзеркало тижня. Україна (https://dt.ua/TECHNOLOGIES/microsoft-i-facebook-budut-stezhiti-za-kiberbezpekoyu-na-viborah-u-kanadi-312631_.html). 28.05.2019).***

***

«Кибератаки, о которых заявил британский министр, являются не реально существующей проблемой, а лишь поводом для нагнетания антироссийских настроений, заявил пресс-секретарь посольства РФ в Великобритании

В четверг британский министр иностранных дел Джереми Хант в очередной раз обвинил Россию в проведении кибератак с целью «подорвать критическую инфраструктуру» и «менять результаты выборов» во многих странах. «Фактически глава британской дипломатии обвинил Россию в осуществлении на целый ряд третьих государств кибератак, которые по своему масштабу и потенциальным

последствиям сопоставимы с вооруженными нападениями и потому требуют солидарного ответа союзников по НАТО», — говорится в заявлении российского посольства. В дипмиссии подчеркнули, что российская сторона «неоднократно на различных уровнях предлагала британским партнерам взаимодействие по проблематике киберугроз». Однако до сих пор от Лондона не было никакой реакции. Дипломаты выразили мнение, что новое антироссийского заявление британского министра свидетельствует о том, что российские кибератаки являются для британских властей не проблемой, а поводом «нагнетания антироссийских настроений, в том числе в международном масштабе». В российском посольстве подчеркнули, что подобные заявления «вызывают не только сожаление, но и серьезное беспокойство». При этом там добавили, что у россиян может создаться впечатление, что именно Лондон таким способом прикрывает подготовку к кибернаступлению на Россию. А это «едва ли будет способствовать чьей-либо безопасности».

Россия неоднократно опровергала все обвинения в попытках повлиять на демократические процессы в разных странах

Западные страны неоднократно устраивали нападки на Москву по данному поводу. Ранее, к примеру, госсекретарь Майк Помпео заявил, что Россия вмешивалась в выборы в США «и в 2012, и в 2008, и 2004 году». Каких-либо доказательств своих слов госсекретарь при этом не привел. Российский сенатор Алексей Пушков в ответ обратил внимание на то, что из заявлений Помпео можно сделать вывод, что «Россия вмешивается в выборы в США с тех пор, когда он еще в школу ходил». Обвинения касаются выборов Джорджа Буша-младшего, Барака Обамы и Дональда Трампа. При этом он с иронией отметил, что может быть и самого Помпео выбрала Москва.» ***(Посольство РФ ответило на обвинения со стороны Лондона в кибератаках // Новости Великобритании на русском языке (https://theuk.one/posolstvo-rf-otvetilo-na-obvineniya-so-storony-londona-v-kiberatakax/). 23.05.2019).***

***

Створення та функціонування кібервійськ

«Міноборони Данії та Німеччини шукають солдатів на... ярмарках геймерів. Там військові хочуть підібрати кадри для служби у кібервійськах. Розум та швидка реакція геймерів - бонус, але й фізпідготовки в армії не оминути.

Цю тактику данські військові застосували ще два роки тому. Потенційних солдат кібервійськ вони стали шукати на великих виставках комп'ютерних ігор. Тому не випадково представники міністерства оборони Данії опинилися на виставці для геймерів у Копенгагені. Цим же шляхом, до речі, пішов і німецький Бундесвер, який уже шукав новобранців серед відвідувачів виставки Gamescom у Кельні. На думку данських військових, багато гравців володіють тими навиками, які важливі для потенційних солдатів кібервійськ…» ***(В'ячеслав Юрін, Михайло Малий. Навіщо в армію набирають геймерів? (відео) // Deutsche Welle***

(https://www.dw.com/uk/%D0%BD%D0%B0%D0%B2%D1%96%D1%89%D0%BE-%D0%B2-%D0%B0%D1%80%D0%BC%D1%96%D1%8E-%D0%BD%D0%B0%D0%B1%D0%B8%D1%80%D0%B0%D1%8E%D1%82%D1%8C-%D0%B3%D0%B5%D0%B9%D0%BC%D0%B5%D1%80%D1%96%D0%B2-%D0%B2%D1%96%D0%B4%D0%B5%D0%BE/a-48673901). 09.05.2019).

***

«Японские СМИ со ссылкой на источники в правительстве сообщили о вынашиваемых в Министерстве обороны планах создания (и применения) первого в истории Японии кибероружия.

Законтрактованные правительством сторонние разработчики должны создать новые штаммы вредоносных программ и бэкдоров к концу текущего фискального года. О функциональных возможностях будущего ПО пока ничего не известно.

Также не сообщается о сценариях использования этого кибероружия, однако, на основании опубликованного рисунка можно сделать вывод, что оно создаётся как средство ответного удара — в случае нападения на японские организации. Кроме того, само наличие у Японии такого козыря, по мнению правительственных источников, может стать сдерживающим фактором для иностранных хакеров.

Расширение гонки вооружений в киберпространство было официально декларировано NATO в июне 2016 г. У Японии, последней из крупнейших держав, уже признавшихся в работе над кибероружием (США, Германия, Великобритания), оно является реакцией на растущую военную угрозу в Дальневосточном регионе со стороны Китая.

Китай, как и Россия, КНДР и Иран, считаются главными инициаторами применения кибервооружений, хотя никто из них формально не заявил об этом.

Это уже вторая попытка Японии создать кибероружие. В 2012 г. на Fujitsu правительством страны была возложена задача разработать ПО для «поиска и уничтожения», но этот проект не принёс желаемых результатов.

В нынешнем году правительство приняло закон, разрешающий сотрудникам Национального института информационных и коммуникационных технологий (NICT) взламывать устройства IoT граждан Японии, использущих стандартные или слабые пароли, в рамках беспрецедентного исследования уровня уязвимости такого оборудования.

Планом предусмотрено составить список небезопасных устройств и передать его соответствующим Интернет-провайдерам для оповещения их клиентов и принятия мер по устранению рисков до начала Олимпиады-2020 в Токио.

Все вышеуказанные проекты родились в новом Департаменте кибербезопасности при Министерстве обороны Японии. Возглавивший его Йошитака Сакурада (Yoshitaka Sakurada), в прошлом году стал мишенью для критики и насмешек, после того как публично признал, что не пользуется компьютерами и вообще в них не разбирается.» ***(В Японии создают средства «ответного удара» в киберпространстве // Goodnews.ua (http://goodnews.ua/technologies/v-yaponii-sozdayut-sredstva-otvetnogo-udara-v-kiberprostranstve/). 06.05.2019).***

***

«Министерство обороны Великобритании выделило 22 млн фунта стерлингов ($27,8 млн) на создание киберцентра, главной задачей которого станет отражение внешних угроз ключевым цифровым коммуникациям страны… Об этом информирует телеканал Sky News со ссылкой на главу оборонного ведомства Пенни Мордонт. Этот объект, по словам министра, будет также поддерживать операции и гуманитарные миссии за рубежом… "Кибератаки могут разрушить нашу национальную инфраструктуру и подорвать демократические институты, - отметила Мордонт. - Наши враги считают, что могут действовать безнаказанно. Мы должны убедить их в обратном". Планируется, что киберцентр начнет работу к 2020 году…» ***(Британия выделила 28 миллионов долларов на создание киберцентра // Новости Великобритании на русском языке (https://theuk.one/britaniya-vydelila-28-millionov-dollarov-na-sozdanie-kibercentra/). 23.05.2019).***

***

Кіберзахист критичної інфраструктури

«…Национальный киберцентр передового опыта (NCCoE) Национального института стандартов и технологий США (National Institute of Standards and Technology) разрабатывает проект рекомендаций для энергетических компаний по обеспечению безопасности устройств IIoT («промышленный Интернет вещей», Industrial Internet of Things).

«Национальный киберцентр передового опыта предлагает проект, который будет концентрироваться на помощи предприятиям в сфере энергетики в обеспечении безопасного обмена информацией распределенных энергетических ресурсов в операционных средах. В связи с ростом числа РЭР, подключаемых к энергетической сети, существует необходимость изучить потенциальные риски кибербезопасности, которые может повлечь эта взаимосвязь», - указывается в сообщении NCCoE.

Проект фокусируется на пяти основных сферах: обмене данными между распределительными объектами и РЭР системами; механизмах и защитных технологиях для идентификации доверенных устройств и коммуникации между устройствами; обнаружении вредоносного ПО и предотвращении атак; обеспечении целостности данных и анализе информации с точки зрения кибербезопасности.

Предварительный вариант документа был опубликован 6 мая нынешнего года. Свои предложения все заинтересованные могут внести до 5 июня.» ***(NIST готовит рекомендации для энергокомпаний по защите IIoT-устройств // SecurityLab.ru https://www.securitylab.ru/news/499044.php). (08.05.2019).***

***

«На хмарній платформі Alibaba Cloud знайшли базу даних мешканців щонайменше двох районів Пекіна, зібрану за допомогою системи розпізнавання облич. Всі дані зберігалися без паролю або іншого захисту.

Цю базу виявив експерт з кібербезпеки Джон Ветінгтон, який розповів про це виданню TechCrunch.

«База містить достатньо даних, щоби точно визначити, куди людина ходила, коли і як багато часу вона витратила. Будь-хто, у кого є доступ до бази, зокрема поліція, міг простежити за повсякденним життям конкретної людини», — зазначає видання.

У відкритому доступі були імена вік, стать, номера ID-карт, національність, зокрема приналежність до таких етнічних груп як ханьці та уйгури. Також журналісти зустрічали такі мітки, як «наркозалежний», «звільнений з в'язниці» тощо.

Крім того, в базі вказаний так званий «соціальний рейтинг» особи. У Китаї запроваджують систему рейтингів, які складають на основі поведінки людей, фінансового стану, порушень тощо. Людей з низьким рейтингом можуть позбавляти деяких прав, а особи з великим зможуть отримувати різні бонуси. Цю систему критикують правозахисники.

Система стеження, до якої отримали доступ журналісти на Alibaba Cloud, здатна стежити за смартфонами і комп'ютерами, які підключені до мережі Wi-Fi. Для цього використовуються датчики китайської компанії Renzixing, які встановлені в усьому районі.

Журналісти звернулися до Alibaba, але там їм сказали, що компанія не несе відповідальності за те, що база зберігалася у відкритому доступі, тому що її розмістив користувач сервісу. Проте через деякий час доступ до цієї бази даних обмежили.

У компанії пояснили, що сповістили клієнта «для вирішення проблеми». Хто цей клієнт, представник Alibaba не розповів…» ***(На Alibaba Cloud виявили персональні дані мешканців Пекіна, отримані системою стеження // Goodnews.ua (http://goodnews.ua/technologies/na-alibaba-cloud-viyavili-personalni-dani-meshkanciv-pekina-otrimani-sistemoyu-stezhennya/). 05.05.2019).***

***

«За останній рік 260 працівників індійської компанії Wipro класифікували мільйони фотографій, постів та іншого контенту з Facebook.

…класифікувати контент Wipro почала з 2014 року. Працівники мали позначати, про що саме пости, пиміром, «селфі», «їжа» чи «тварини».

Деталі такої роботи розповіли працівники компанії на умовах анонімності, але Facebook невдовзі багато з цієї інформації підтвердила. Wipro є однією з двохсот фірм, які замаються такого типу маркуванням контенту.

The Verge зазначає, що Wipro сортує контент з Facebook та Instagram, включаючи оновлення статусу, відео, фотографії, посилання та Stories. Кожен пост перевіряється двома працівниками, щодня опрацьовують приблизно 700 пунктів.

Маркування допомагає «тренувати» програми, які визначають, про що користувачі роблять пости. Надалі ця інформація забезпечує роботу штучного інтелекту, що лежить в основі багатьох функцій соціальних мереж.

Такі практики маркування контенту ставлять нові питання про конфіденційність для Facebook, вважають експерти з правових питань, з якими консультувалася Reuters. Facebook визнав, що деякі повідомлення, які надсилали на опрацювання у Wipro, могли містити імена користувачів.

Юрист Джон Кеннеді (John Kennedy) сказав агентству, що це може порушувати європейські правила захисту даних користувачів (GDPR), оскільки Facebook має просити додаткової згоди на передачу їхніх даних стороннім компаніям.

Але прес-секретар Facebook заявив, що «у їхній політиці щодо даних вони чітко вказують, що використовують інформацію, яку надають люди, аби покращити свій досвід, і що вони можуть працювати з постачальниками послуг, які допомагають в цьому процесі»…» ***(Facebook передає пости користувачів стороннім компаніям, які допомагають навчати алгоритми // MediaSapiens (https://ms.detector.media/web/cybersecurity/facebook_peredae_posti_koristuvachiv_storonnim_kompaniyam_yaki_dopomagayut_navchati_algoritmi/). 06.05.2019).***

***

«Эксперт по кибербезопасности Анураг Сен (Anurag Sen) сообщил о том, что обнаружил базу данных с контактами более 49 миллионов известных Instagram-блогеров в открытом доступе. Она хранилась в облачной платформе Amazon Web Services.

Записи в базе содержали как информацию, которую блогеры сами размещали в профиле, так и скрытые номера телефонов и email-адреса. Помимо этого, в открытом доступе находились сведения о стоимости рекламы в аккаунтах звёзд. Чаще всего, эта цифра выводится из соотношения количества подписчиков и лайков, а также охвата постов.

Скорее всего, база данных принадлежит индийскому маркетинговому агентству Chtrbox, однако, как сообщили блогеры, согласия на использование данных они этой компании не давали и вообще с ней не сотрудничали. Истинность контактных данных звёзды подтвердили.» ***(Контактные данные звезд Instagram оказались в открытом доступе // SmartPhone.ua (http://www.smartphone.ua/news/kontaktnye_dannye_zvezd_instagram_okazalis_v_otkrytom_dostupe_60354.html). 21.05.2019).***

***

«Сделанные в Китае дроны могут отправлять важные данные производителям в Китай, которые, в свою очередь, могут передавать эти данные правительству. Такое предупреждение… выпустило министерство внутренней безопасности США.

Таким образом, утверждают эксперты входящего в МВБ Агентства по кибербезопасности и безопасности инфраструктуры, использование китайских дронов угрожает американским компаниям и организациям. Эти устройства якобы «содержать компоненты, которые могут скомпрометировать ваши данные и разместить вашу информацию на серверах, доступ к которым имеет кто-то помимо компании-производителя».

Хотя в документе не указываются конкретные марки мультикоптеров, 80% продаж таких устройств в США и Канаде приходится на продукцию китайской DJI. При этом на дроны всё чаще полагаются в своей работе и правоохранительные органы США (особенно местная полиция), и компании, обслуживающие объекты инфраструктуры.

Учитывая продолжающуюся торговую войну между США и Китаем, а также введённый на прошлой неделе запрет на сотрудничество американских компаний с китайской Huawei, издание не исключает, что следующей жертвой конфликта может стать DJI. В 2017-м дроны китайского производителя уже запретили использовать американским военным.» ***(США могут запретить китайские дроны // Капитал (https://www.capital.ua/ru/news/127863-ssha-mogut-zapretit-kitayskie-drony). 21.05.2019).***

***

«Управление по защите персональных данных Турции (KVKK) оштрафовало Facebook за халатное отношение к данным. Ошибка в Photo API, о которой мы писали в конце прошлого года, угрожала утечкой фотографий 6,8 млн пользователей соцсети, 300 тыс. из которых были гражданами Турции. Сумма штрафа составила 1,65 млн турецких лир, или $270 тыс.

Детали инцидента стали известны в декабре 2018 года, хотя баг присутствовал в системе с 13 по 25 сентября. В течение почти двух недель около 1500 приложений и 876 разработчиков могли получить доступ к непубличным фото из-за ошибки платформы.

Как пояснил разработчик Facebook Томер Бар (Tomer Bar), «когда кто-то дает приложению разрешение на пользование своими фотографиями на Facebook, мы обычно предоставляем доступ только к тем фото, которыми люди делятся в своей ленте. В данном же случае баг потенциально давал разработчикам приложений доступ к другим фото, например из Marketplace или Историй. Проблема также затронула фотографии, которые люди загрузили на Facebook, но решили не публиковать».

Представители KVKK обвинили разработчиков социальной сети в халатности и в том, что они не уведомили об инциденте власти страны, как того требует законодательство Турции. Большая часть штрафа ($164 тыс.) наложена на Facebook за промедление в устранении уязвимости. Еще $106 тыс. лир компания заплатит за то, что сообщила надзорному органу о проблеме лишь 17 декабря 2018 года, спустя три месяца после обнаружения бага.

Турецкое управление по защите персональных данных продолжает расследование и другой утечки социальной сети, которая также произошла в сентябре прошлого года. Тогда злоумышленники получили доступ к 50 млн

токенов пользователей, в том числе позволяющих авторизоваться через Facebook на сторонних сайтах. Данные еще 40 млн человек оказались под угрозой из-за использования уязвимой функции «Посмотреть как…». ***(Dmitry Nazarov. Власти Турции оштрафовали Facebook за баг в Photo API // Threatpost (https://threatpost.ru/turkey-fined-facebook-for-photo-api-bug/32603/). 13.05.2019).***

***

Кіберзлочинність та кібертерроризм

«Киберпреступные организации соревнуются друг с другом за клиентов, ведут борьбу за лучших менеджеров проектов и даже ищут лидеров, которые выполняют функции генеральных директоров, пишет CNBC. Исследователи из IBM и Google рассказали, как работают киберпреступные группы…

"Мы видим их дисциплину, они активны в рабочее время, у них есть выходные, работают по обычному графику. Все зависит от группы. В организованной преступности, безусловно, есть начальник. Этот человек не обязательно делает всю работу. Они нанимают субподрядчиков", - поделился руководитель отдела аналитики угроз IBM Security Калеб Барлоу. По его словам, важно понимать, как злонамеренные хакеры могут структурировать свои бизнес-операции, поскольку подпольная экономика часто функционирует параллельно с более широкой…

Киберпреступные организации не похожи друг на друга, но типичная структура выглядит следующим образом: лидер, как генеральный директор, наблюдает за более широкими целями организации. Он помогает нанять менеджеров по проектам, выполняющих различные части каждой кибератаки.

Если целью группы является получение денег путем взлома компании и кражи ее информации, менеджеры будут наблюдать в масштабах преступления за различными функциями, которые соответствуют их специализациям…

Криминальные группы не существуют в вакууме. "Если я хороший разработчик, то создам вирусов-вымогателей и продам их так же, как законные компании, которые предлагают программное обеспечение. Тогда я буду поддерживать вредоносное ПО, и, если вы найдете жертв, заразите их и заплатите, я возьму 10% или 20%", - пояснил главный исследователь Alphabet "Other Bet" Хуан Андрес Герреро-Сааде.

В последние годы некоторые из этих поставщиков услуг сократили свои доходы. В первой половине этого десятилетия стало популярным вредоносное программное обеспечение, известное как банковские трояны, которые крадут учетные данные человека для получения денег с его банковского счета. Специалисты, предлагающие услуги по отмыванию средств, пользовались большим спросом. В последние годы этот спрос уменьшился, поскольку вирусы-вымогатели стали более популярными, и преступники смогли напрямую получать деньги.

По словам Герреро-Сааде, у преступных группировок работают "пробивные" продавцы, чтобы вытеснить своих конкурентов путем кражи территории. Это

распространено среди специалистов, которые предлагают атаки типа DDoS. Для одной DDoS-атаки по найму характерно нападать только на компьютеры, которые уже были скомпрометированы конкурентом, а затем использовать эту бот-сеть для собственных целей. Преступники, у которых в ботнете больше компьютеров, более эффективны. Таким образом, DDoS-атаки по найму могут подорвать конкуренцию…

Как заявил руководитель отдела реагирования на инциденты безопасности IBM X-Force Кристофер Скотт, когда компании становятся слишком большими и организованными, их довольно просто идентифицировать - и, таким образом, они уходят из бизнеса.

"Когда вы имеете дело с более бюрократическими организациями, эти действия очень предсказуемы. Одна группа Dyre, специализирующаяся на банковских троянах, стала настолько большой в 2015 году, что ее было очень легко идентифицировать и закрыть. Понимание этих тенденций важно для компаний, которые ведут борьбу с киберпреступниками. Если вы преследуете конкретного противника, вы можете понять, сколько из тех же инструментов, методов и практик они используют", - прокомментировал Скотт.» ***(Ирина Фоменко. CNBC: киберпреступные организации оказались слишком похожи на обычные компании // Internetua (https://internetua.com/cnbc-kiberprestupnuye-organizatsii-okasalis-slishkom-pohoji-na-obuchnuye-companii). 06.05.2019).***

***

«В последние годы киберпространство все больше определяет облик реального мира. Хакерское вмешательство в выборы США, скандал с Facebook и Cambridge Analytica, расследования о российских фабриках троллей, разоблачения Wikileaks и Эдварда Сноудена — все эти события всколыхнули общество и надолго засели в политической повестке дня. И все они, так или иначе, связаны с интернетом. Кибератаки стали привычным инструментом ведения войны. А потому возникает вопрос: может ли кибератака начать Третью мировую? Ответ может вам не понравиться…

Для начала, следует понять, что подразумевается под самим термином “кибератака”. Определений существует множество, но наиболее созвучно вопросам международных отношений то, которое было сформулировано в 2013 году рабочей группой НАТО в “Таллиннском руководстве по ведению кибервойны”. Этот документ определяет кибератаку как “кибероперацию, наступательную или оборонительную, которая, как обоснованно ожидается, приведет к повреждению или смертям людей, либо к повреждениям или разрушениям объектов”.

Здесь важно отметить, что “Таллинское руководство” не является нормативным документом или международным соглашением. Документ, по сути, является частным исследованием группы экспертов. То есть, в международном праве отсутствует точное определение “кибератаки”.

Здесь возникает парадокс: хотя определение отсутствует, физический ответ на кибератаку допускается. Об этом в своей монографии “Кибератаки и легальное обоснование вооруженного ответа” пишет майор армии США Джошуа А. Мендоза. По его словам “существующие источники международного права обеспечивают

юридическое обоснование, требуемое для вооруженного ответа, несмотря на отсутствие в этих источниках кибер терминологии".

Проще говоря, в современном мире каждый волен трактовать понятие кибератаки так, как посчитает нужным. И отвечать так, как сочтет необходимым…

Шанс того, что кибератака спровоцирует вооруженный конфликт, увеличивается по мере того, как растет разрушительная сила кибератак. Вот несколько примеров того, как в течение последних десятилетий кибератаки становились более опасными:

-1976-1984 — первая зарегистрированная кибератака в мире. Советские шпионы установили кейлоггер (программу, регистрирующую нажатия клавиш на клавиатуре) не компьютеры IBM американского посольства в Москве и американского Консульства в Ленинграде (Санкт-Петербург). Это позволило СССР перехватить большой объем конфиденциальных данных и поставить под угрозу национальную безопасность США.

-2007 — в апреле Эстония была поражена массированной DDoS-атакой со стороны России. Это спровоцировало обрушение сетей, отвечающих за различные аспекты общественной жизни: финансы, коммуникацию, вооруженные силы. Атака длилась почти месяц.

-2008 — аналогичную массовую DDoS-атаку Россия использовала во время августовского нападения на Грузию и оккупации Абхазии и Южной Осетии.

-2010 — червь Stuxnet, разработанный США и Израилем, вызвал физическое разрушение 20% ядерных центрифуг Ирана. Атака очень сильно задержала развитие ядерной программы страны.

За последние десять лет интернет-технологии настолько глубоко проникли в наши жизни, что без них уже нельзя представить нормальное функционирование общества и государства. А значит, будущие кибератаки окажутся еще более разрушительными. Достаточно разрушительными, чтобы в ответ начать стрелять…

А две недели назад, 4 мая 2019, кибервойна вообще вышла на принципиально новый уровень. Тогда Армия обороны Израиля впервые в истории ответила на кибератаку террористов ХАМАС в режиме реального времени, и попросту разбомбила предположительное местонахождение вражеских хакеров…

Ситуация в кибербезопасности становится более напряженной, чем когда-либо прежде. Ян Юнгрен, эксперт по кибербезопасности платформы VPNpro, ожидает, что все будет становиться только хуже. "Поскольку не существует никаких правил ведения кибервойны, страны продолжат нападать друг на друга на цифровых фронтах", — говорит Юнгрен.

Конечно, сегодняшняя гонка вооружений в мировом киберпространстве больше напоминает холодную войну, чем полноценный конфликт. Но не стоит забывать, что холодная война продолжается ровно до тех пор, пока кто-нибудь не решится на горячий ответ…» ***(Может ли кибератака начать Третью мировую войну? // Goodnews.ua (http://goodnews.ua/technologies/mozhet-li-kiberataka-nachat-tretyu-mirovuyu-vojnu/). 19.05.2019).***

***

«Facebook удалил 265 аккаунтов, в том числе Instagram, связанных с Израилем

Решение принято в связи с "недостоверным поведением", которое касалось пользователей в Юго-Восточной Азии, Латинской Америке и Африке…

В частности, деятельность с этих аккаунтов была нацелена на Нигерию, Сенегал, Того, Анголу, Нигер и Тунис, а также на Латинскую Америку и Юго-Восточную Азию.

"Люди в этой сети использовали фальшивые учетные записи для просмотра страниц, распространения своего контента и искусственного увеличения вовлеченности", - заявил Натаниэль Глейхер, глава политики кибербезопасности в Facebook.

Он определил израильскую Archimedes Group как источник некоторых из этих действий…

По словам Глейхера, у Archimedes Group было 65 аккаунтов в Facebook, 161 страница, 12 событий и четыре аккаунта в Instagram. Около 2,8 млн аккаунтов в целом были подписаны на одну или несколько страниц.» ***(Facebook удалил 265 аккаунтов из Израиля: Нацелились на Африку, Азию и Южную Америку // Goodnews.ua (http://www.dsnews.ua/world/facebook-udalil-265-akkauntov-iz-izrailya-natselilis-na-afriku--16052019210000). 16.05.2019).***

***

«Эксперты оценили экономику хакерских атак на банки, подсчитав себестоимость работы взломщиков. По данным исследования Positive Technologies, расходы в этом бизнесе окупаются после первого же хищения. Но снижающиеся суммы вывода средств на одну атаку при вложениях в десятки тысяч долларов уже заставляют злоумышленников оптимизировать расходы.

Стартовая стоимость целевой атаки на организации финансовой отрасли составляет около $45–55 тыс., оценивают эксперты Positive Technologies. Около $2,5 тыс. может составить месячная подписка на сервис по созданию документов с вредоносом, инструменты по созданию вредоносных файлов — от $300, исходный код программы-загрузчика вредоноса — от $1,5 тыс., программа по эксплуатации уязвимостей для внедрения — порядка $10 тыс., легальные инструменты, которые могут использовать хакеры, эксперты оценили в $30–40 тыс. (версии программы CobaltStrike использовались группировкой Cobalt).

По оценке директора экспертного центра Positive Technologies Алексея Новикова, вложения киберпреступников окупаются уже после первой же успешной атаки. Однако в последний год доходы атакующих банки хакеров снизились — средняя сумма хищения упала, тогда как расходы на инструментарий остались на прежнем уровне.

Для оптимизации расходов злоумышленникам приходится искать пути повышения результативности атак. В частности, подавляющее большинство атак на банки идет с помощью фишинговых рассылок. С точки зрения расходов они хороши тем, что количество адресатов в рассылке практически не влияет на ее стоимость. «Грубо говоря, был подготовлен шаблон одного письма, а дальше очень

легкая автоматизация для рассылки,— отметил господин Новиков.— То есть разница в отправке одного письма или тысячи только во времени работы сервера».

Главные затраты — это цена самого инструментария и его «упаковки» как для проникновения в кредитную организацию, так и для «продвижения» от компьютера, взломанного первым, далее по внутрибанковской сети. Операционные расходы на рассылку вредоносов незначительны, по оценкам эксперта, они составляют порядка $1 тыс. в месяц. В частности, в компании подсчитали, что примерная стоимость атаки группировки Silence— порядка $55 тыс. Последняя атака, приписываемая группировке — на ИТ-банк в феврале 2019 года, принесла злоумышленникам порядка $380 тыс. (см. “Ъ” от 12 февраля). Другой набор для атаки автоматически меняет стоимость — на взлом ПИР-банка хакерам пришлось потратить порядка $66 тыс., в то время как добыча составила $930 тыс. (см. “Ъ” от 6 июля 2018 года).

Использование не покупных вредоносов, а актуальных уязвимостей позволяет существенно снизить расходы.

Например, в прошлом году эксперты выявили уязвимость в системе Microsoft и предупредили о ней неограниченный круг лиц. Уже через семь часов пошла рассылка — хакеры адаптировали уязвимость для атаки и сэкономили около $10 тыс., рассказывает Алексей Новиков.

Атака из доверенной сети также позволяет повысить ее рентабельность. Подобный подход хакеры использовали в прошлом году при атаке на банк «Юнистрим», с сервера которого рассылались фишинговые письма банкам-партнерам (см. “Ъ” от 21 декабря 2018 года). Одним вредоносом был атакован как сам банк, так и его партнеры.

Об сокращении затрат хакерами говорят и другие эксперты. Так, операционный директор центра мониторинга и реагирования на кибератаки Solar JSOC Антон Юдаков отметил, что киберпреступность сегодня — это в первую очередь бизнес, который сейчас активно оптимизирует расходы. «Существуют целые группы, специализирующиеся на предоставлении конкретных услуг — DDoS-атак, кардинга, написания вредоносного ПО, обналичивания денег, выведенных из банков, и так далее,— отметил он.— Привлечение таких «аутсорсеров» обходится значительно дешевле, чем если бы заказчик атаки создавал собственную группировку с аналогичными функциями». Например, согласно исследованию Positive Technologies, расходы на обнал составляют от 15% до 50% от похищенной суммы. И нижнюю границу цены может дать именно «аутсорсер».

«Кроме того, такая схема обеспечивает большую безопасность и оперативность,— отметил господин Юдаков.— Хакеры также стараются атаковать банки не напрямую, а через более уязвимых контрагентов». Примером тому служат проблемы владельцев карты «Кукуруза» (см. “Ъ” от 15 мая), когда злоумышленники получили доступ к логинам и паролям за счет взлома связанного сервера.» ***(Вероника Горячева. Сколько стоит взлом устроить // Vse.Media (http://vse.media/skolko-stoit-vzlom-ustroit/). 22.05.2019).***

***

«Компания Trend Micro представила первые результаты индекса киберрисков (Cyber Risk Index, CRI), составленного совместно с Ponemon Institute на основе опроса ИТ-компаний. В исследовании приняли участие более 1000 ИТ-специалистов и руководителей организаций, представляющих малый, средний и крупный бизнес США. По итогам опроса самый высокий уровень киберриска оказался у малого бизнеса.

CRI (Cyber Risk Index) состоит из индекса киберподготовленности – CPI (насколько компания готова противостоять угрозам) и индекса киберугроз – CTI (опыт работы с угрозами). Формула расчёта выглядит так: CRI=CPI–CTI. CRI ранжируется в диапазоне от –10 до +10, где –10 – максимальная степень риска. Trend Micro и Ponemon Institute планируют обновлять эти данные каждый полгода.

Кроме того, по итогам исследования представители компаний всех уровней заявили, что их бизнес в течение ближайших 12 месяцев может быть подвержен атакам, которые позволят хакерам проникнуть в сеть – малый (34%), средний (35%) и крупный бизнес (39%) соответственно.

Так, среди респондентов, представляющих малый бизнес, 26% за последний год столкнулись с 3-6 кибератаками, 11% компаний – с 7-10 подобными случаями, а 6% – более чем с десятью такими атаками.

С тремя-шестью кибератаками за прошедшие 12 месяцев столкнулись 19% представителей среднего бизнеса, 14% указали на семь-десять таких инцидентов, а 8% – на более десяти кибератак.

19% опрошенных представителей крупных предприятий стали жертвами трех-шести кибератак, 15% столкнулись с семью-десятью кибератаками, но только 3% сообщили, что у них было более десяти подобных инцидентов.» ***(У малого бизнеса наивысший уровень индекса киберрисков // «Компьютерное Обозрение» (https://ko.com.ua/u_malogo_biznesa_naivysshij_uroven_indeksa_kiberriskov_128787). 20.05.2019).***

***

«В период с января по март участники Антифишинговой рабочей группы (APWG) зарегистрировали 180 768 сайтов-ловушек фишеров — заметно больше, чем в IV и III кварталах 2018 года. В то же время число уникальных фишинговых рассылок сократилось более чем в два раза и составило около 112,4 тыс.

Наибольшее количество атакуемых брендов было зафиксировано в марте — 330. При этом эксперты подчеркнули, что злоумышленников по-прежнему очень интересуют пароли и логины к SaaS-сервисам (ПО как услуга) и веб-почте.

По данным APWG, в I квартале на долю этой объединенной категории мишеней пришлось 36% фишинговых атак, и она обогнала даже платежные системы и службы (27%), не говоря уже о банках и других финансовых организациях (16%). Показатель для облачных хранилищ и файлообменников, напротив, продолжил снижаться и составил лишь 2%, тогда как год назад он превышал 11%.

Процентное соотношение сайтов-ловушек, использующих HTTPS, в отчетный период достигло новой рекордной отметки. «В I квартале SSL-

сертификаты использовали 58% фишинговых сайтов — против 46% в предыдущем, — комментирует Джон Лакур (John LaCour), технический директор PhishLabs. — По нашему мнению, столь значительный рост объясняется двумя причинами: доступностью бесплатных сертификатов и увеличением общего количества сайтов, использующих SSL. Сайты переходят на SSL, так как браузеры стали предупреждать пользователей о его отсутствии, а большинство фишинговых схем полагается на взломанные легитимные сайты».

Заключительный раздел сводного отчета APWG, как всегда, содержит данные по Бразилии, которые охотно предоставляет местный наблюдатель — компания Axur. В I квартале на территории этой страны было зафиксировано 3220 случаев фишинга и 180 случаев использования специализированных вредоносных программ. Все эти атаки были нацелены на пользователей бразильских сервисов или сайтов зарубежных компаний, доступных бразильцам и оформленных на португальском языке.

Эксперты Axur тоже отметили рост количества фишинговых атак в сфере SaaS и почтовом сервисе, в особенности на мобильных платформах. Что касается профильных зловредов, каждый из них в среднем был нацелен на 13 финансовых организаций, обслуживающих жителей Бразилии. Самый большой список, которым оперировали эти трояны, включал 19 позиций.» ***(Maxim Zaitsev. APWG отметила оживление в стане фишеров // Threatpost (https://threatpost.ru/apwg-sees-phishing-sites-number-rising-notably-in-1q2019/32698/). 20.05.2019).***

***

«Ресурсы провайдеров облачных услуг все чаще используются киберпреступниками для организации DDoS-атак. К такому выводу пришли эксперты компании Akamai в результате исследования источников вредоносного трафика. По словам ИБ-специалистов, ежедневно они фиксируют до 30 нападений с IP-адресов, принадлежащих онлайн-сервисам.

Исследователи разработали собственную методику, позволяющую выделить вредоносные пакеты со стороны облачных провайдеров в общем трафике DDoS-кампаний. Специалисты фиксировали количество автономных систем с адресами сетевых сервисов в первые три минуты нападения и их число в такой же период времени за десять минут до атаки.

Аналитики определили, что если в обычных условиях доля трафика, принадлежащего автономным сетям, расположенным в облаке, не превышает 1% от общего числа пакетов, то во время DDoS-атаки этот показатель возрастает до 20% и более. Специалисты также отметили, что рост исходящего трафика за счет вредоносных запросов может варьироваться в зависимости от тематики сетевого ресурса. Так, поток запросов с аккаунтов игровой направленности при нападениях увеличивался более чем в 4 раза.

По мнению экспертов, чтобы получить доступ к профилям облачных хранилищ, киберпреступники используют учетные данные, похищенные на других ресурсах (credential stuffing). В дальнейшем скомпрометированные аккаунты привлекают для участия в DDoS-атаках вместе с IP-адресами, выделяемыми провайдерами в рамках бесплатного пробного доступа к сервису…» ***(Dmitry***

Nazarov. Облачные сервисы становятся источником DDoS-атак // Threatpost (https://threatpost.ru/cloud-services-being-used-for-ddos/32683/). 17.05.2019).

***

«Операторы зловредных кампаний научились манипулировать с защищенными соединениями, чтобы скрывать свою активность от обнаружения. Техника построена на подмене содержимого приветственных сообщений, которые боты отправляют веб-серверам.

Исследователи Akamai назвали обнаруженную технику «трюки с шифрованием» (Cipher Stunting). По их словам, первые случаи ее применения относятся к началу 2018 года, а с сентября популярность метода выросла взрывными темпами. Цель злоумышленников состоит в том, чтобы помешать защитным системам соотнести те или иные пакеты данных с вредоносными клиентами.

Как пояснили эксперты, сегодня подавляющее большинство (82%) кибератак происходит с использованием соединений по протоколам SSL/TLS. Злоумышленники следуют за развитием Интернета в целом — по данным экспертов, к концу 2019 года 90% мирового трафика будет идти по защищенным каналам.

Первое сообщение, которое отправляет клиент серверу при установлении такого соединения — это Client Hello, приветственный пакет с базовой информацией о параметрах коммуникации. Туда входит желаемая версия TLS, список поддерживаемых методов сжатия, возможные методы шифрования (CipherSuites). Все эти данные отправляются в открытом виде, позволяя экспертам снимать и анализировать цифровые отпечатки клиентов, определяя по ним легитимных и вредоносных участников.

Вплоть до августа 2018 года эксперты насчитывали в Интернете чуть менее 19 тыс. таких отпечатков. Столь малое количество объясняется ограниченным набором возможных комбинаций браузера и ОС пользователей, которые в основном и определяют уникальность клиента. Начиная с сентября их количество стало резко увеличиваться — 255 млн в октябре, 1,3 млрд в феврале.

Как показал дальнейший анализ, преступники стали добавлять случайные значения в блок CipherSuites. Это меняет хешированные значения Client Hello и создает лавину уникальных отпечатков. Исследователи связали активность таких клиентов с автоматизированными атаками на сайты авиакомпаний, банков и сервисов онлайн-знакомств.

Эксперты пришли к выводу, что злоумышленники редактируют данные с помощью некой программы на Java. В настоящий момент специалисты научились определять в общем потоке данных отредактированные сообщения Client Hello и блокировать нежелательную активность…» ***(Dmitry Nazarov. Вредоносные боты получили новую технику маскировки // Threatpost (https://threatpost.ru/bots-have-new-camouflage-technic/32655/). 16.05.2019).***

***

«Ежегодный отчет по интернет-безопасности от экспертов SiteLock показал, что в 2018 году количество атак на веб-сайты выросло на 59%, достигнув среднего значения в 62 инцидента в сутки. Криптоджекинг и SEO-спам теряют популярность, а технологии скрытного присутствия, напротив, получают все большее распространение.

По словам экспертов, злоумышленники все чаще не стремятся установить контроль над сайтом, перехватывая лишь отдельные интернет-сессии. В результате они могут надежно закрепиться на скомпрометированном ресурсе, причем обнаружить постороннее ПО можно только с помощью специализированных средств интернет-безопасности.

С другой стороны, многие веб-администраторы ошибочно полагают, что мониторингом их сайтов должны заниматься сторонние контролеры. По их мнению, поисковики отслеживают присутствие вредоносного ПО и автоматически уведомляют зараженные площадки. На самом деле в 2018 году поисковые машины заблокировали лишь 15% зараженных сайтов — на 4 п. п. меньше, чем в 2017-м.

«[Такие сервисы] крайне неохотно пополняют свои черные списки, чтобы не причинять владельцам сайтов лишних неудобств, — поясняют эксперты. — Блокировка может сильно ударить по репутации ресурса, сократить поток посетителей и поступающую прибыль».

Большинство администраторов все же понимает необходимость проактивного подхода к безопасности. Как следствие, количество зараженных площадок на протяжении 2018 года оставалось примерно на одном уровне — около 1% от всех существующих сайтов. В абсолютном выражении это 17,6 млн ресурсов.

На половине из них исследователи обнаружили бэкдоры, shell-зловреды и нелегитимно модифицированные файлы (filehacker). Все эти программы, которые исследователи отнесли к проверенной временем классике, обеспечивают преступникам скрытное присутствие с возможностью модифицировать и красть данные.

Чаще всего преступники используют в своих атаках межсайтовый скриптинг, SQL-инъекции и межсайтовую подделку запросов. Исследователи видят угрозу в растущей популярности свободных CMS WordPress, Joomla! и Drupal, на которых сегодня работает почти 40% сайтов. Эти решения открывают Интернет для неопытных вебмастеров, которые не справляются с настройками безопасности.

«Мы изучили 6 млн ресурсов на базе этих CMS и обнаружили хотя бы одну уязвимость [из трех самых популярных] на 20% WordPress-сайтов, 15% площадок на Joomla! и 2% — на Drupal, — уточняют эксперты. — Проблемы присутствуют даже на последних версиях систем, а значит, простая установка обновлений не гарантирует безопасность».

Специалисты прогнозируют, что в 2019 году преступники будут действовать еще незаметнее, отказываясь от «шумных» атак в пользу скрытных методов проникновения. Веб-администраторам следует самим заботиться о собственной защите, чтобы вовремя блокировать возникающие угрозы.» ***(Dmitry Nazarov. Эксперты насчитали в Интернете 18 млн зараженных сайтов // Threatpost***

(https://threatpost.ru/experts-counted-18m-compromised-websites-online/32629/). 14.05.2019).

***

«Новостное издание ZDNet предупреждает о новых взломах сторонних JavaScript на сайтах с целью хищения информации, вводимой посетителями в веб-формы. На сей раз злоумышленникам удалось модифицировать скрипт веб-аналитики разработки Picreel и сценарий, подгружаемый из CDN-сети в рамках проекта с открытым исходным кодом Alpaca Forms. В настоящее время на их долю совокупно приходится около 4,7 тыс. установок.

Оба случая подмены обнаружил голландский эксперт Виллем де Грот (Willem de Groot). Исследователь полагает, что модификация файлов стала возможной из-за неадекватной защиты доступа к хранилищам AWS S3.

Анализ показал, что вредоносный код крадет данные из веб-форм и отправляет их на сервер, поднятый злоумышленниками в Панаме. Примечательно, что у этого зловреда нет особых предпочтений: он в равной степени проводит сбор информации на страницах авторизации, оформления заказов, оплаты покупок, а также из контактных форм.

По данным де Грота, Picreel и хостер Alpaca Forms уже удалили зараженные скрипты со своих серверов. Тем не менее, киберкампания на этом не закончилась: аналогичные кейлоггеры были найдены также в JavaScript-коде печати доверия Best of the Web. Этот знак обычно устанавливается на сайтах в подтверждение высокого профессионального уровня услуг, безопасности посещений и надежной защиты пользовательских данных. Согласно статистике PublicWWW, соответствующий сниппет установлен на 108 страницах в Интернете…» ***(Maxim Zaitsev. Взломщики изменили скрипты Picreel и Alpaca Forms // Threatpost (https://threatpost.ru/hackers-inserted-malicious-code-into-picreel-alpaca-forms-scripts/32602/). 13.05.2019).***

***

«В этом году в мире также продолжится рост количества случаев мошенничества с использованием технологий социальной инженерии - по итогам 2018 года специалистами Сбербанка уже отмечен рост этого вида преступлений на 6%.

Международными экспертами по кибербезопасности подсчитано, что в 2019 году в мире кибератаки происходят каждые 14 секунд. В 2019 году одним из главных вызовов также станут утечки данных корпораций в результате целевых атак на их сотрудников.

С увеличением числа кибератак возрастает и причиняемый ими ущерб. Если в прошлом году убытки компаний различных секторов экономики составили 1,5 трлн долларов, то в 2019 году, по прогнозу Сбербанка, они достигнут уже 2,5 трлн. К 2022 году, по прогнозу Всемирного экономического форума, сумма планетарного ущерба от кибератак может вырасти до 8 трлн долларов.

Одной из причин ускоренного роста киберпреступности, по мнению специалистов, являются технологические тренды. К 2022 году к интернету будет

подключен один трлн устройств. К 2023-му у 80% людей появится аватар в цифровом мире. При этом более 50% интернет-трафика домохозяйств в 2024-м будут потреблять «умные» устройства и бытовая техника.

Сбербанк ежедневно успешно отражает несколько тысяч атак на свои системы. Поэтому проблемы кибербезопасности для банка являются приоритетными. По инициативе банка уже во второй раз в Москве 20–21 июня 2019 года будет проведен Международный конгресс по кибербезопасности (International Cybersecurity Congress), на котором международное сообщество обсудит глобальные инициативы и основные принципы эффективного взаимодействия…» ***(Кибератаки в 2019 году происходят каждые 14 секунд по всему миру // (ООО "ИКС-МЕДИА"http://www.iksmedia.ru/news/5587604-Kiberataki-v-2019-godu-proisxodyat.html). 21.05.2019).***

***

«Форум OGUser.com, популярный среди хакеров и мошенников, сам подвергся хакерской атаке… Скомпрометированы адреса электронной почты, зашифрованные пароли, IP-адреса и личные сообщения почти 113 000 пользователей форума.

Администратор OGUsers опубликовал заявление 12 мая, что перебои, вызванные отказом жесткого диска, стерли личные сообщения и комментарии на форуме за несколько месяцев. Позже он объяснил пользователям, что восстановил резервную копию с января 2019 года.

Однако администратор не знал, что в то же время хакеры украли пользовательскую базу данных форума и стерли его жесткие диски. Это выяснилось четыре дня спустя, когда администратор конкурирующего хакерского сообщества RaidForums объявил, что загрузил базу данных OGUsers, которую теперь можно скачать бесплатно…

Публикация базы данных OGUser вызвала некоторую обеспокоенность у сообщества, известного привлечением людей, занимающихся кражей телефонных номеров в качестве метода захвата социальных сетей, электронной почты и финансовых счетов жертв. Несколько тем на OGUsers были заполнены комментариями встревоженных пользователей. Многие жаловались на получение фишинговых писем.

В Twitter аналитик Натан Лекс написал, что "эта ситуация больше всего позабавит правоохранительные органы". "Базу данных OGUsers взломали. Скомпрометированы личные сообщения от каждого пользователя до 2018 года. Если эти данные попадут в руки властей, любого пользователя, связанного с деятельностью черных хакеров, будет легко обнаружить", - прокомментировал Лекс.» ***(Ирина Фоменко. IT Pro: хакеры украли у своих конкурентов личные данные более ста тысяч людей // Internetua (https://internetua.com/it-pro-hakery-ukrali-u-svoih-konkurentov-lichnuye-dannye-bolee-sta-tysyacs-lyudey). 21.05.2019).***

***

«Державний телеканал «Кан» зазнав хакерської атаки під час трансляції першого півфіналу 64-го міжнародного пісенного конкурсу «Євробачення-2019», унаслідок якої протягом кількох хвилин на екрані демонстрували повідомлення нібито від імені Армії оборони Ізраїлю (IDF) про загрозу ракетного обстрілу…

Згідно з повідомленням, у двохвилинному відео, з підробленим логотипом IDF, говорилося про нібито небезпеку для людей, які знаходиться в радіусі 1,2 кілометра від місця проведення конкурсу в Тель-Авіві.

«Ізраїль небезпечний, ви ще переконаєтеся», – йшлося в повідомленні.

Як зазначається, ЗМІ Ізраїлю припускають, що за атакою хакерів можуть стояти пропалестинські групи в арабських країнах.

Європейська мовна спілка (організатор конкурсу «Євробачення-2019») та телеканал «Кан» повідомили, що розслідують цю кібератаку…» ***(Ізраїльський телеканал зазнав хакерської атаки під час трансляції півфіналу «Євробачення-2019» // «ДЕТЕКТОР МЕДІА» (https://detector.media/infospace/article/167277/2019-05-15-izrailskii-telekanal-zaznav-khakerskoi-ataki-pid-chas-translyatsii-pivfinalu-evrobachennya-2019/). 15.05.2019).***

***

«Немецкий производитель программного обеспечения TeamViewer признался, что их популярное бесплатное приложение для удаленного доступа к компьютерам было взломано хакерами из Китая при поддержке государства. Это произошло в 2016 году, но о печальном событии компания призналась лишь сейчас немецкой газете Der Spiegel.

"Осенью 2016 года TeamViewer подвергся кибератаке. Подозрительные действия были замечены лишь спустя несколько месяцев, но мы успели предотвратить серьезный ущерб", – заявил представитель компании.

Пресс-секретарь TeamViewer сообщил изданию ZDNet, что в то время было проведено расследование, но они не нашли никаких злоупотреблений со стороны сотрудников…

Der Spiegel утверждает, что китайские хакеры присутствуют в сети TeamViewer с 2014 года. По словам немецкого издания, хакеры, которые проникли в сеть TeamViewer, использовали Winnti – троян-бэкдор, печально известный "инструмент", которым пользуются кибер-злоумышленники из Пекина.

Вредоносная программа была впервые обнаружена в 2009 году и первоначально использовалась только одной группой китайских хакеров, которую исследователи в области ИТ-безопасности также стали называть "группой Winnti". Спустя пять лет все изменилось. Согласно сообщениям ProtectWise 401 TRG и Chronicle, вредоносные программы Winnti начали фиксировать в атаках из Китая, за которыми подозревают поддержку со стороны правительства.

Это делает невозможным, по крайней мере, на данный момент, узнать, какая из множества спонсируемых государством китайских хакерских групп была ответственна за вторжение TeamViewer. Тем не менее, существуют две китайские

хакерские группы, которые соответствуют этому типу атак: APT10 (группа, которая занимается взломом поставщиков облачных услуг) и APT17 (группа, которая занимается атаками по цепочке поставок)…» ***(TeamViewer взломали: разработчики скрывали правду три года // AOinform (https://www.aoinform.com/news/teamviewer_vzlomali_razrabotchiki_skryvali_pravdu_tri_goda/2019-05-20-29749). 20.05.2019)/***

***

«Хакеры взломали веб-сайт Сингапурского Красного Креста (SRC), а личные данные более 4000 потенциальных доноров крови — включая имена, группы крови и контактные телефоны — были скомпрометированы в результате последней кибератаки на город-государство…

SRC сообщил о нарушении властям в тот же день, и полиция начала расследование. "SRC серьезно относится к этому инциденту", — заявили в организации, добавив, что "внешние консультанты" помогают в расследовании.

Предварительные результаты показали, что "слабый пароль администратора" мог сделать сайт уязвимым. Генеральный секретарь SRC Бенджамин Уильям заявил, что организация связывается с пострадавшим от кибератаки.

В июле прошлого года в результате крупнейшего в истории взлома данных хакеры получили доступ к правительственной базе данных и украли учетные данные 1,5 млн сингапурцев, включая премьер-министра Ли Сянь Луна.

Официальный запрос выявил множество недостатков, в том числе слабых мест в компьютерных системах, а также неадекватную подготовку персонала и ресурсы. Власти полагают, что за этой атакой стояло государство.

В январе Сингапур объявил, что конфиденциальная информация о 14 200 человек, у которых диагностирован вирус, вызывающий СПИД, была размещена в Интернете, причем большинство из них пострадали от иностранцев. Власти обвинили Михи Фаррера Брочеза, ВИЧ-положительного американца, который был заключен в тюрьму в городе-государстве и депортирован в 2018 году.

В марте Управление здравоохранения сообщило, что личные данные 800 000 человек, которые с 1986 года сдали или зарегистрировались для сдачи крови в Сингапуре, были ошибочно размещены в сети более двух месяцев…» ***(Хакеры взломали сайт Красного Креста и слили данные в сеть // Goodnews.ua (http://goodnews.ua/technologies/xakery-vzlomali-sajt-krasnogo-kresta-i-slili-dannye-v-set/). 17.05.2019).***

***

«В среду, 15 мая, председатель совета директоров израильской телекомпании Kan Эльдад Кобленц обвинил исламистское движение ХАМАС в проведении хакерской атаки во время прямой трансляции первого полуфинала песенного конкурса «Евровидение-2019», который в этом году проходит в Тель-Авиве. Хакеры нанесли удар вечером 14 мая.

На протяжении двух минут на экранах телевизоров, расположенных в радиусе 1,2 километра от места проведения конкурса, держалась предупреждающая надпись «Угроза ракетной атаки. Пожалуйста, уйдите в укрытие». Она

сопровождалась воем сирены. Надпись сменилась видео ракетного удара, снятом из космоса. Затем появилась еще одна надпись: «В Израиле небезопасно, вы увидите это».

Кобленц подчеркнул, что Национальный директорат кибербезопасности в кратчайшие сроки отбил хакерскую атаку. «Не думаю, что эти надписи видели многие зрители. Это была самая быстрая победа Израиля над ХАМАС», — добавил он с легкой иронией.

Пока официальные лица отказываются объяснять, как хакерам удалось попасть в прямой телеэфир. Однако они подчеркивают, что методы, которые были использованы киберпреступниками в ходе атаки, не угрожают национальной безопасности.

Ранее пропалестинские активисты угрожали любыми способами сорвать проведение «Евровидения» в Тель-Авиве. Это не испугало десятки тысяч иностранных туристов приехать в Израиль, чтобы побывать на песенном конкурсе…» ***(Палестинские хакеры провели атаку на "Евровидение-2019" (видео) // «Факты и комментарии®» (https://fakty.ua/305367-palestinskie-hakery-proveli-ataku-na-evrovidenie-2019-video). 15.05.2019).***

***

«Группа под названием Shadow Brokers в 2017 г. заполучила набор инструментов для взлома, что привело к массовым атакам по всему миру, включая печально известные вымогательства WannaCry. Хотя группа утверждала, что похитила инструменты из Агентства национальной безопасности США (АНБ), было загадкой, как именно им удалось это сделать. Теперь же исследование Symantec показало, что источником могли быть агенты китайской разведки, которые перехватили инструменты, когда АНБ атаковало их компьютеры.

Symantec обнаружила, что подрядчик Министерства государственной безопасности Китая, известный под кодовым именем Buckeye, использовал украденные инструменты АНБ по крайней мере за год до Shadow Brokers. Symantec считает, что группа захватила инструменты во время атаки АНБ, а затем переделала их для создания собственной версии.

…АНБ считает, что это один из самых опасных китайских подрядчиков. Он был ответственен за нападение на американские компании космической и спутниковой отрасли, а также работающих в области ядерной энергии. Symantec заявляет, что Buckeye использовали модифицированные инструменты АНБ для проведения кибератак на исследовательские организации, образовательные учреждения и другую инфраструктуру в Бельгии, Люксембурге, Вьетнаме, на Филиппинах и в Гонконге. По крайней мере, в одном случае группа получила доступ к миллионам записей частных переписок из крупной телекоммуникационной сети.

Если Buckeye действительно передала инструменты Shadow Brokers, то группа также косвенно ответственна за атаки, предпринятые северокорейскими и российскими хакерами, которые также использовали эти инструменты. Атаки вымогателей WannaCry нанесли вред Национальной службе здравоохранения

Великобритании и затронули цепочку поставок вакцин. Российские хакеры также вывели из строя критически важные украинские службы, в том числе почтовую систему, аэропорты и банкоматы.» ***(Китайские шпионы могли передать украденные инструменты АНБ создателям WannaCry // «Компьютерное Обозрение» (https://ko.com.ua/kitajskie_shpiony_mogli_peredat_ukradennye_instrumenty_anb_sozdatelyam_wannacry_128679). 08.05.2019).***

***

«Хакер понял, что за ним следят. Шпионское программное обеспечение, которое он хотел использовать против правительства Украины, проникло не в ту машину. И теперь аналитик компании из США разбирал на куски программу под названием RatVermin, пытаясь понять, как она работает… хакер работал на так называемую ЛНР - самозваную «республику» на Востоке Украины. Он сначала пытался запустить злокачественный вирус под названием Hidden Tear, чтобы зашифровать файлы на компьютере, в который злоумышленник ошибочно проник. Вирус вывел бы компьютер из строя, показав американскому аналитику насмешливое сообщение: «Ваши файлы были зашифрованы. Отправьте мне Bitcoin или шаурму. И я не люблю ночные клубы, десерты или напиваться». Но аналитик заблокировал работу вируса. А затем в течение нескольких часов 20 марта 2018 года длилась виртуальная версия «рукопашного боя». Хакер пытался удалить программное обеспечение, которое американец использовал для «вскрытия» RatVermin… Эта беседа была описана в отчете, который был опубликован в прошлом месяце американской компанией FireEye. Она иллюстрирует хакерскую кампанию против Украины, которую ведут от имени так называемой ЛНР. В ее рамках применяют как специально написанное программное обеспечение, так и публично доступные образцы шпионских программ, которые нацеливают против украинских министерств для похищения данных. Хакер из Луганска, которого загнали в тупик в прошлом году, не смог достичь своей цели. Но кампания, в которой он принимал участие, иллюстрирует, как кибератаки, доступные в прошлом только хорошо профинансированным разведывательным управлениям, теперь стали инструментом даже для боевиков. Распространение такого оружия позволяет отдельным хакерам и их союзникам проводить разведывательные операции для своих псевдоправительств …успех российских хакеров на Донбассе трудно оценить. Однако, они активно работают против Киева с 2014 года, на что указывают данные FireEye. Можно допустить, что за эти годы российские боевики могли получить определенные победы. «Список целей включает широкий спектр украинских военных, политиков и СМИ. И в случае успеха атаки против них могут иметь серьезные последствия», - говорит научный сотрудник Wilson Center Нина Янкович. «Даже если успеха не было достигнуто, они могут посеять сомнения общества относительно украинских кибервозможностей, а также возможностей правительства», - добавила она. Россия предоставляет ключевую поддержку так называемым «республикам» на Востоке Украины. Однако, аналитики говорят, что не заметили пока убедительных доказательств того, что хакерские атаки так называемой ЛНР ведут актеры из России. Поэтому вероятно, что террористы в

Луганске создали собственное подразделение кибербразведки. По словам Халтквиста, если все действительно так, это может указывать на то, что буквально любой в мире может стать кибершпионом.» ***(Foreign Policy: после войны в Украине кибершпионов в мире станет больше // информационный портал "ua.today" (http://ua.today/news/incidents/foreign_policy_posle_vojny_v_ukraine_kibershpionov_v_mire_stanet_bolshe). 06.05.2019).***

***

«За последние несколько лет хактивисты значительно сократили свою активность вплоть до фактической остановки DDoS-атак к настоящему моменту. По мнению экспертов IBM X-Force, причины следует искать в успехах правоохранительных органов и попытках хакеров уйти от публичности.

Исследователи проанализировали известные эпизоды хактивизма за период с 2015 по 2019 годы. Кампания признавалась идеологически мотивированной, если ее организаторы сами объявляли ее таковой. Вторым условием для включения в подборку был существенный ущерб для пострадавшей стороны.

Как выяснилось, за последние годы популярность хактивизма упала на 95% — с 35 инцидентов в 2015-м до двух в 2018-м. В нынешнем году под критерии исследования не попала ни одна кампания. С другой стороны, такие масштабные истории, как взлом сетевого оборудования Ubiquiti, не пополнили статистику из-за отсутствия финансовых потерь.

Основная часть (45%) атак 2015–2018 гг. приходилась на движение Anonymous. Еще 35% поделили между собой Lizard Squad, LulzSec и другие группировки.

По словам экспертов, ведущую роль в падении хактивизма сыграли проблемы внутри движения Anonymous. Его участники не смогли договориться о позиции по американским выборам 2016 года — одни стремились сохранить аполитичность, другие хотели атаковать ресурсы кандидатов. Кроме того, члены сообщества все чаще оказываются на скамье подсудимых, где получают реальные тюремные сроки и крупные штрафы.

Исследователи подсчитали, что с 2011 года власти Великобритании, США и Турции арестовали более 60 хактивистов. Эта цифра включает лишь те случаи, которые освещали СМИ. Реальный объем операций против таких группировок может быть гораздо больше.

Исследователи призывают аудиторию не хоронить хактивизм раньше времени. По их словам, нынешнее затишье может означать, что «благородные» взломщики ищут способ вести атаки с меньшими рисками для себя. С другой стороны, недавние атаки на сайты эквадорского правительства и СМИ в Саудовской Аравии доказывают, что некоторые активисты не отказываются и от прежних методов борьбы.» ***(Dmitry Nazarov. В 2019 году противники хактивизма могут праздновать победу // Threatpost (https://threatpost.ru/hacktivism-is-no-longer-a-threat-in-2019/32711/). 20.05.2019).***

***

«Эксперты Expert Security Center компании Positive Technologies (PT ESC) обнаружили кибергруппировку предположительно с азиатскими корнями. Злоумышленники атаковали более 30 организаций из различных отраслей, включая промышленность, энергетический и нефтегазовый секторы России, СНГ и других странах. При этом значительное число жертв находилось в России и СНГ.

Главная цель группы — кража конфиденциальной информации организаций. Группа действует на протяжении как минимум нескольких лет: обнаружены следы активности TaskMasters начиная с 2010 года.

Группа использовала необычный метод закрепления в инфраструктуре: участники создавали специфические задания (таски) в планировщике задач (поэтому группировка получила название TaskMasters). Планировщик задач позволяет выполнять команды ОС и запускать ПО в определенный момент времени, указанный в задаче. Используемый кибергруппировкой планировщик AtNow позволяет выполнять задачи не только локально, но и на удаленных компьютерах сети, и делать это независимо от временных настроек этих узлов. Кроме того, эта утилита не требует установки. Все это упрощает автоматизацию атаки.

«После проникновения в локальную сеть злоумышленники исследуют инфраструктуру, эксплуатируют уязвимости, загружают на скомпрометированные узлы вредоносные программы и удаленно используют их для шпионажа, — рассказывает Алексей Новиков, директор экспертного центра безопасности Positive Technologies. — Обнаружить подобные атаки можно с помощью специализированных средств защиты, в том числе PT Network Attack Discovery, а для анализа атак и их предотвращения необходимо привлекать профессионалов в расследовании киберинцидентов».

Эксперты Positive Technologies предполагают, что члены группы TaskMasters могут быть жителями стран Азии. В коде используемых ими инструментов встречаются упоминания китайских разработчиков, во время некоторых атак были зафиксированы подключения с IP-адресов из Китая, а ключи для некоторых версий программ можно обнаружить на форумах, где общаются жители этой страны. Помимо этого, многие утилиты из пакета TaskMasters содержат сообщения об ошибках и другую отладочную информацию, написанные на английском языке с ошибками, что указывает на то, что он не является для разработчиков родным языком…» ***(Кибергруппировка TaskMasters атакует организации в России и СНГ // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5585679-Kibergruppirovka-TaskMasters-atakue.html). 13.05.2019).***

***

«В первом квартале 2019 года русскоговорящие кибергруппировки в основном ушли в тень. Лишь немногие из них вели себя активно — например, Sofacy и Turla.

Такие выводы сделала «Лаборатория Касперского» на основании мониторинга данных об APT-атаках в первые три месяца 2019 года. Эксперты предполагают, что, возможно, затишье связано с изменениями в этих структурах.

Самой «громкой» кампанией прошедшего периода стала операция ShadowHammer — сложная целевая атака на цепочки поставок.

В январе, феврале и марте APT-атаки были нацелены преимущественно на жертвы, расположенные в Юго-Восточной Азии. Оставались активными и китайскоговорящие группировки, которые проводили в первом квартале кампании разного уровня сложности. Например, CactusPete, ведущая свою деятельность с 2012 года, внедряла новые варианты загрузчиков и бэкдоров, а также перекомпонованные эксплойты для уязвимости нулевого дня в движке VBScript, ранее использовавшиеся участниками группы DarkHotel.

По данным «Лаборатории Касперского», основным драйвером APT-атак в первом квартале была геополитика. Также злоумышленники довольно часто интересовались криптовалютами. Кроме того, атаки часто проводились с помощью коммерческого шпионского ПО: в первые три месяца года были обнаружены, к примеру, новый вариант программы FinSpy и операция LuckyMouse, для реализации которой использовались утекшие в сеть разработки компании Hacking Team…» ***(Русскоговорящие кибергруппировки затаїлись // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5585070-Russkogovoryashhie-kibergruppirovki.html). 07.05.2019).***

***

Вірусне та інше шкідливе програмне забезпечення

«В рейтинге наиболее опасных вредоносных программ, которые продемонстрировали повышенную активность в апреле текущего года, оказались стразу три вируса-майнера. Соответствующий список составили специалисты по кибербезопасности из компании Check Point.

Что касается о вирусах-майнерах, то речь идет о Cryptoloot, XMRig и Jsecoin. Первая программа использует мощности CPU/GPU жертв и необходимые ресурсы для майнинга.

В обзоре аналитиков компании отмечается, что Cryptoloot выступал основным конкурентом Coinhive, но он запрашивал существенно меньше дохода с сайтов.

Вторая вредоносная программа-майнер XMRig построена с открытым исходным кодом, ее хакеры используют для поражения компьютеров жертвы и добычи монет Monero. Впервые об этом вирусе стало известно в мае 2017 года.

Третье вредоносное программное обеспечение Jsecoin представляет собой JavaScript-майнер, который может встраиваться в веб-сайты. Вирус запускается в интернет-браузере в обмен за виртуальную валюту и другие вознаграждения.

Кроме этих вредоносных программ специалисты по кибербезопасности отметили растущее влияние банковского трояна Trickbot и вируса-шифровальщика Badrabbit.

«Растущая активность троянов говорит о стремлении преступников извлечь максимальную финансовую выгоду после ликвидации ряда популярных ресурсов для майнинга и падения стоимости криптовалют», – говорится в исследовании.

По словам главы подразделения по исследованию интернет-угроз компании Check Point Майи Хоровец, в последнее вредоносное ПО концентрируется не столько на краже персональных данных, сколько на распространении вымогателей Ryuk.» ***(В ТОП-10 вредоносных программ попали три вируса-майнера // «LetKnow OÜ» (https://letknow.news/news/v-top-10-vredonosnyh-programm-popali-tri-virusa-maynera-23178.html). 16.05.2019).***

***

«Британская фирма кибербезопасности Sophos зарегистрировала в конце прошлой недели вспышку активности со стороны нового штамма ransomware под названием MegaCortex.

Как и Ryuk, Bitpaymer, Dharma, SamSam, LockerGoga или Matrix, MegaCortex относится к категории программ, используемых только для тщательно спланированных целевых вторжений в сети крупных предприятий.

Эта тактика «охоты на крупного зверя» на протяжении последних шести месяцев была преобладающей в применении ransomware.

Данное ПО впервые было замечено в январе 2018 г., когда его образец был кем-то загружен на сервис сканирования вирусов, VirusTotal. С тех пор количество атак MegaCortex постепенно росло, но в середине прошлой недели произошла резкая эскалация: Sophos насчитала 47 инцидентов, составивших две трети от общего числа известных ей атак MegaCortex (76).

Согласно опубликованному в пятницу заявлению Sophos, ей удалось блокировать атаки, исходившие из корпоративных сетей в США, Канаде, Нидерландах, Ирландии, Италии и Франции. Однако, британский провайдер антивирусных сервисов отметил, что часть атак — из мест, не охваченных его мониторингом, могли остаться незамеченными.

Сама Sophos не смогла с полной достоверностью установить, как ПО MegaCortex попадало в инфицированные сети, но ряд других экспертов компьютерной безопасности утверждают, что для этого используется загрузчик вредоносного кода, Rietspoof.

Это новый подход, другие целевые атаки ransomware осуществлялись либо путём грубого взлома конечных точек через слабозащищенные соединения RDP (Remote Desktop Protocol), либо загрузкой на рабочие станции, предварительно инфицированные троянами Emotet или Trickbot.

Сообщается, что MegaCortex представляет значительную опасность: с его помощью хакеры могут быстро захватить контроль над контроллером домена, что позволит им устанавливать ransomware на рабочие станции во внутренней сети корпорации.

Пострадавшие могут определить MegaCortex по произвольному 8-символьному расширению, которое добавляется к зашифрованным файлам, а также по характерному требованию выкупа (как оно выглядит, показано на снимке экрана).

В качестве профилактической меры исследователи из Sophos рекомендуют компаниям настроить двухфакторную аутентификацию для своих внутренних сетей и, в особенности, для серверов центрального администрирования.» ***(Новый***

вид ransomware активизировал атаки на корпоративный сектор // «Компьютерное Обозрение» (https://ko.com.ua/novyj_vid_ransomware_aktiviziroval_ataki_na_korporativnyj_sektor_128655). 07.05.2019).

***

«По оценке «Лаборатории Касперского», в I квартале количество DDoS-атак, проводимых с ботнетов, увеличилось на 84%, а их средняя продолжительность — более чем в 4 раза. Рост активности дидосеров стал особенно заметным во второй половине марта; отдельный всплеск был зарегистрирован также в середине января.

Оживлению на этом фронте предшествовал довольно долгий период затишья, которому, по мнению экспертов, способствовали репрессивные меры против купли-продажи DDoS-услуг. Теперь опустевшая ниша, по всей видимости, снова стала заполняться.

Согласно свежей статистике, список стран — источников мусорного трафика по-прежнему возглавляет Китай; за минувший квартал его доля выросла до 67,89%. Второе место сохранили США, хотя их показатель уменьшился до 17,17%; на третью ступень поднялся Гонконг (4,81%).

Вклад DDoS-инцидентов длительностью более 1 часа продолжает расти и за отчетный период увеличился в два раза. Тем не менее, самая затяжная атака продолжалась 289 часов (чуть больше 12 суток), тогда как в предыдущем квартале этот показатель был выше — 329 часов (почти 14 суток).

Из векторов DDoS наиболее часто применялся SYN flood, доля которого вновь повысилась и составила 84,1%. UDP flood остался на втором месте, хотя его вклад сократился с 31,1 до 8,9%. TCP flood тоже значительно снизил свой показатель (до 3,1%) и оказался на четвертой позиции, пропустив вперед HTTP flood (3,3%).

Основной мусорный поток создавали Linux-ботнеты; в I квартале на их долю пришлось 95,71% DDoS-атак — против прежних 97,11%. Небольшое снижение показателя, как отметили исследователи, вызвано отнюдь не ростом популярности Windows-сетей у дидосеров, а сокращением числа командных серверов Mirai-подобных зловредов, в особенности Darkai. В итоге мусорный поток, генерируемый этими ботами, уменьшился в среднем в три раза, а в случае Darkai — даже в семь раз.

Как и ранее, ботоводы предпочитают размещать C&C-серверы в США (34,10% находок). Второе место в этом рейтинге заняли Нидерланды (12,72%), на третье с седьмого поднялась Россия (10,40%).» ***(Maxim Zaitsev. Эксперты фиксируют рост DDoS-активности // Threatpost (https://threatpost.ru/kaspersky-lab-sees-ddos-activity-up-in-1q2019/32737/). 22.05.2019).***

***

«Bleeping Computer предупреждает о появлении нового Windows-вымогателя, который распространяется через вредоносную рекламу с

использованием эксплойтов из набора RIG. К счастью, исследователи уже изучили опасную находку и выпустили бесплатный декриптор.

На запуск GetCrypt требуется согласие пользователя, так как обход службы контроля учетных записей его авторы не предусмотрели. После активации зловред прежде всего проверяет языковые настройки системы. Если жертва использует украинский, белорусский, русский или казахский язык, он завершает свои процессы и отказывается от шифрования.

В противном случае программа продолжает свою работу: отыскивает идентификатор производителя ЦП (CPUID) и использует его для создания строки из четырех символов, которая впоследствии будет добавляться к имени зашифрованных файлов. После этого GetCrypt удаляет теневые копии, используя Windows-утилиту vssadmin.exe, и приступает к шифрованию.

При поиске подходящих объектов вымогатель оперирует списком папок, которые следует обходить стороной:

:\$Recycle.Bin
:\ProgramData
:\Users\All Users
:\Program Files
:\Local Settings
:\Windows
:\Boot
:\System Volume Information
:\Recovery
AppData

Для преобразования файлов жертвы используются потоковый шифр Salsa20 и RSA с 4096-битным ключом. Зашифрованным файлам присваивается упомянутое четырехзначное расширение и в каждую папку с ними помещается записка # decrypt my files #.txt. Это сообщение написано на английском языке, но с орфографическими ошибками, и не окончено. Более полный текст выводится на экран в виде изображения, заменяющего обои рабочего стола. Сумма выкупа не оговаривается; для восстановления файлов жертве предлагают отослать письмо на адрес @cock.li, а в случае отсутствия отклика — на резервный @tutanota.com, прикрепив файл encrypted_key.bin из папки %AppData%.

Отыскивая файлы для шифрования, зловред пытается также добраться до сетевых папок общего пользования. Если такой ресурс недоступен, он использует список ходовых логинов и паролей для взлома и в случае успеха подключается к папке, используя функцию WNetAddConnection2W. Исследователи отмечают, что с подобной особенностью шифровальщика они столкнулись впервые.

У жертв GetCrypt имеется возможность вернуть данные без уплаты выкупа: эксперты Emsisoft создали специальную утилиту, которой можно воспользоваться, если сохранился оригинал хотя бы одного зашифрованного файла. Декриптор пока загружают с сайта компании, но она является участником онлайн-проекта No More Ransom, и можно ожидать, что в скором времени этот инструмент будет доступен и там.» ***(Maxim Zaitsev. Зашифрованные GetCrypt файлы можно вернуть без***

выкупа // Threatpost (https://threatpost.ru/getcrypt-ransomware-analysis-yields-free-decryptor/32761/). 23.05.2019).

***

«Киберпреступники используют ссылки с переадресацией, чтобы обмануть жертву и загрузить на ее компьютер модульный троян Trickbot. К такому выводу пришли ИБ-специалисты после изучения спам-рассылок, маскирующихся под сообщения об отправке товара из интернет-магазина. Злоумышленники прикрываются легитимными доменами, чтобы обойти фильтры безопасности и доставить полезную нагрузку на устройство получателя.

Вредоносная ссылка содержится в письме, имитирующем стандартное сообщение об отправке заказа. Оно выглядит довольно убедительно: стиль подачи информации соответствует подобным документам, в послании есть номер для трекинга посылки, сроки доставки и даже иконки соцсетей.

Чтобы запутать получателя, киберпреступники воспользовались функцией переадресации Google. Ссылка в письме выглядит как hxxps://google[.]dm:443/url?q=<адрес целевого сайта> и служит для перенаправления жертвы на этот адрес. Однако и пользователь, и спам-фильтры видят домен Google и считают URL легитимным.

При переходе по ссылке жертве показывается предупреждение о переадресации. Если пользователь ничего не заподозрит и откроет вредоносный сайт, он увидит фальшивую страницу просмотра заказа. Эта страница содержит скрипт для фоновой загрузки зловреда Trickbot.

Опасный троян в зависимости от состава подключенных к нему модулей может быть использован для кражи паролей, данных банковских карт и сведений для доступа к криптокошелькам. Вредоносную программу впервые обнаружили осенью 2016 года, и с тех пор авторы регулярно добавляют в нее новые функции.

Так, в апреле прошлого года ИБ-специалисты обнаружили в дикой природе вариант трояна, блокирующий экран зараженного устройства. Эксперты предположили, что создатели Trickbot решили сделать из него вымогатель, однако позже выяснили, что такая уловка необходима для кражи учетных данных в новых версиях Windows.

Аналитики отмечают, что киберпреступники и ранее использовали спам-рассылки для доставки зловреда, однако впервые применили механизм переадресации для маскировки ссылок на свои ресурсы.» ***(Julia Glazova. Trickbot скрывается от спам-фильтров с помощью переадресации // Threatpost (https://threatpost.ru/trickbot-uses-redirect-urls-to-trick-spam-filters/32734/). 21.05.2019).***

***

«Исследователи из компании Chronicle провели детальный анализ Linux-версии трояна Winnti, ранее ускользавшей от внимания ИБ-специалистов. По их мнению, функции этого штамма во многом совпадают с возможностями вредоносной программы, подробно описанной экспертами «Лаборатории Касперского» еще в 2013 году. Как утверждают аналитики, зловред

создан китайской проправительственной кибергруппировкой, использующей новый вариант приложения для целевых атак.

Вредонос состоит из двух модулей: один обладает базовыми функциями бэкдора, другой отвечает за маскировку действий программы в зараженной системе. Полезная нагрузка доставляется на компьютер в зашифрованном виде и декодируется путем гаммирования. Возможности приложения libxselinux соответствуют Windows-варианту Winnti 2.0 и включают в себя работу с тремя командными серверами, чьи адреса жестко зашиты в код зловреда.

Троян использует протоколы ICMP, HTTP, а также собственные реализации TCP и UDP, чтобы получать дополнительные модули из центра управления. Как отмечают специалисты, киберпреступники также способны напрямую подключаться к зараженной системе, если командные серверы Winnti окажутся недоступны. Конечные функции вредоносного приложения определяются набором плагинов, которые могут варьироваться в зависимости от целей атаки.

Руткит libxselinux.so отвечает за сокрытие действий Winnti на инфицированной машине. Программа представляет собой доработанный вариант утилиты Azazel, доступной на GitHub. Скрипт назначает основным функциям зловреда буквенные коды и модифицирует их отклик на запросы, чтобы не допустить срабатывания антивирусных сканеров.

Разработчики Winnti добавили в Azazel оператор Decrypt2, который применяется для расшифровки конфигурационных файлов модуля libxselinux.so. Кроме того, авторы зловреда включили в код утилиты уникальные идентификаторы портов и процессов, задействованных трояном. В дальнейшем эти имена используются при обработке команд из центра управления.

Linux-версия Winnti обнаружилась при изучении деталей атаки на фармацевтическую компанию Bayer. Эксперты нашли троян на серверах организации в начале прошлого года, однако намеренно не удаляли его из системы, чтобы изучить работу вредоносного ПО. В ходе исследования выяснилось, что первые проникновения с применением Linux-варианта бэкдора датируются 2015 годом.» ***(Egor Nashilov. Эксперты рассказали о Linux-варианте трояна Winnti // Threatpost (https://threatpost.ru/winnti-for-linux-discovered/32731/). 21.05.2019).***

***

«Два ИБ-исследователя обнаружили вредоносное ПО, которое маскируется под легальный VPN-сервис. По словам Лоуренса Абрамса (Lawrence Abrams), утилита под названием Pirate Chick VPN загружает на компьютер жертвы троян AZORult. Эксперт установил это совместно с Майклом Гиллеспи (Michael Gillespie) и его командой MalwareHunter.

Мошенники распространяли программу через поддельное обновление Adobe Flash Player и вредоносную рекламу. В последнем случае при переходе по ссылке человек попадал на типичную с виду продающую страницу, где помимо описания утилиты размещались FAQ, политика конфиденциальности и пользовательские соглашения. Посетителю предлагалось скачать пробную версию утилиты на три месяца. Исполняемые файлы также выглядели убедительно, поскольку были подписаны сертификатом британской компании ATX International Limited.

После открытия Pirate Chick VPN связывался с удаленным сервером, а затем загружал в папку %Temp% полезную нагрузку в виде .txt-файла и декодировал ее, превращая в исполняемый файл AZORult, который запускался в фоновом режиме.

Этот шпион предназначен для кражи логинов и паролей, данных кредитных карт и криптокошельков, истории браузера, файлов cookie и других сведений. Кроме того, он может служить загрузчиком для других зловредов.

Согласно исследованию «Лаборатории Касперского», наибольшей популярностью AZORult пользуется среди российских продавцов и покупателей вредоносного ПО. При этом программа постоянно дорабатывается и совершенствуется, а злоумышленники находят все новые способы ее доставки на устройства своих жертв.

Так, в текущем году они маскировали ее под службу обновления сервисов Google и утилиту для чистки дискового пространства G-Cleaner, а также внедряли в клиент криптовалюты Denarius.

Интересно, что в данном случае разработчики прописали для зловреда три условия, при которых он не начинает свою деятельность.

Если в системе запущен любой из этих процессов — ImmunityDebugger, Fiddler, Wireshark, Regshot или ProcessHacker. Все это утилиты для мониторинга системных служб, анализа HTTP-трафика, системного реестра и вредоносного ПО.

Если IP-адрес жертвы находится в России, Украине, Беларуси или Казахстане.

Если пользователь работает в виртуальной среде VMWare, VirtualBox или HyperV.

На данный момент сайт Pirate Chick VPN по-прежнему функционирует, однако программа после установки скачивает обфусцированную копию procmon.exe.

«Прежде полезной нагрузкой был троян AZORult, — пояснил Абрамс. — Однако сейчас это утилита для отслеживания активности запущенных процессов Process Monitor, которая может быть всего лишь временной заменой до запуска другой кампании».» ***(Egor Nashilov. Мошенники продвигали AZORult под видом VPN Pirate Chick // Threatpost (https://threatpost.ru/fake-vpn-pirate-chick-propagates-azorult/32610/). 14.05.2019).***

***

«Эксперты Национального центра кибербезопасности США (National Cybersecurity and Communications Integration Center, NCCIC) обнаружили новый зловред в арсенале APT-группировки Hidden Cobra. Программа под названием Electricfish представляет собой продвинутый сетевой шлюз, позволяя злоумышленникам выгружать данные из закрытых инфраструктур.

На счету группировки Hidden Cobra, также известной как Lazarus, множество кампаний, включая взлом азиатских финансовых организаций и запуск эпидемии шифровальщика WannaCry. В 2019 году преступников заподозрили в атаках на российские предприятия.

Специалисты NCCIC не раскрывают, как они получили доступ к зловреду. Известно лишь, что ПО обнаружено при расследовании ФБР и Министерством

внутренней безопасности США неких атак Hidden Cobra, что позволило однозначно установить связь программы с группировкой. Позже на VirusTotal нашлись еще три версии программы, которые загрузили на сайт в августе — октябре 2018 года.

Как рассказали эксперты, Electricfish создает канал для передачи данных между жертвой и атакующими. Операторы зловреда выставляют необходимые настройки через командную строку: указывают IP-адреса и порты для передачи информации от зараженной машины на управляющий сервер, прописывают данные прокси. После этого Electricfish открывает TCP-подключение, по которому и направляет трафик.

Зловред использует специально разработанный протокол, что позволяет действовать незаметно для стандартных систем мониторинга. Использование собственного прокси-сервера обеспечивает злоумышленникам возможность обойти системы аутентификации.

По данным центра кибербезопасности Вьетнама (Vietnam Computer Emergency Response Center, VNCERT), несколько месяцев назад зловред использовали в атаках на банки и критическую инфраструктуру этой страны. На момент публикации в открытых источниках нет подробностей об этих инцидентах.

Специалисты NCCIC опубликовали индикаторы, по которым можно отследить заражение Electricfish (XML-файл). Эксперты также призывают администраторов проверить актуальность ПО и настройки сетевого доступа на подконтрольных им компьютерах, включить брандмауэры и ограничить пользователям возможность установки стороннего ПО.

Ранее аналитики сообщили о появлении у Lazarus многофункционального трояна HOPLIGHT, который позволяет преступникам загружать на компьютеры стороннее ПО и вмешиваться в системные процессы.» ***(Egor Nashilov. Группировка Hidden Cobra вооружилась новым зловредом // Threatpost (https://threatpost.ru/hidden-cobra-arms-up-with-electricfish/32597/). 13.05.2019).***

***

«Компания ESET зафиксировала новую вредоносную кампанию группировки BlackTech. Злоумышленники распространяют бэкдор Plead, используя скомпрометированные цифровые сертификаты ASUS Cloud Corporation, которые маскируют угрозу под легитимное ПО и помогают обходить защиту.

Схема атаки выглядит следующим образом: облачное хранилище ASUS направляет запрос на легитимный сервер для получения бинарного файла с последней версией обновления системы. На этом этапе злоумышленники подставляют собственный URL-адрес, ведущий на вредоносный файл.

Загрузка файла происходит с сервера, который имитирует название легитимного сервера ASUS. После загрузки вредоносный файл сохраняется в ОС и запускается при каждом входе пользователя в систему.

ESET не исключает, что подмена сертификатов могла происходить в рамках атаки на цепочку поставок. Другим вариантом представляется атака через посредника (man-in-the-middle) — злоумышленники компрометируют роутер, пользуясь уязвимостями облачного хранилища ASUS WebStorage.

Вредоносная активность зафиксирована на территории Тайваня в конце апреля. Как полагают эксперты ESET, за ней стоит группировка BlackTech, которая известна кибершпионажем в странах Азии.

ESET связалась с ASUS Cloud Corporation и сообщила об угрозе.» ***(Обнаружена новая атака группировки BlackTech // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5587167-Obnaruzhena-novaya-ataka-gruppirovk.html). 20.05.2019).***

***

«Эксперты по безопасности обнаружили в сети Tor сервис под названием Inpivx, который позволяет даже не самым технически подготовленным желающим конструировать шифровальщики-вымогатели и использовать их для атак.

В последнее время в даркнете встречается немалое количество ресурсов, предлагающих шифровальщики как услугу (RaaS), где от клиента вообще не требуется никаких или почти никаких технических знаний. Однако Inpivx работает по иному принципу.

За $500 клиенту предлагается исходные коды для процедур шифрования в различных вариациях и для панели управления будущим вредоносом.

Таким образом потенциальные киберпреступники получают возможность использовать эти компоненты для сборки или написания своей уникальной вымогательской программы - уже с готовыми инструментами управления…

Вредоносная программа написана на C++ и работает на всех версиях Windows, начиная с XP. Панель управления написана на PHP. В ней присутствуют все нужные потенциальному злоумышленнику компоненты - управление размерами требуемых от жертв выплат, вывод статистики по заражениям (с детализацией по операционным системам и географическому расположению атакованных машин и т.д.), простой чат для общения с жертвами и так далее…» ***(Начались продажи троянов в исходном коде с учебником для тех, кто не умеет программировать // ООО "ИКС-МЕДИА" (http://www.iksmedia.ru/news/5585210-Nachalis-prodazhi-troyanov-v-isxodn.html). 07.05.2019).***

***

«Дослідниця в галузі кібербезпеки, відома під ніком SandboxEscaper, виявила кілька нових вразливостей в системі Windows. Не минуло й тижня, як у новому травневому оновлення ОС WIndows 10 виявили нову уразливість. Тепер же корпорації доведеться випустити ще одне невелике оновлення заради усунення нової уразливості.

Одна з проломів дозволяє користувачам отримувати доступ до файлів, якими володіє адміністратор, не маючи відповідних прав. Ще один виявлений фахівцем дефект операційної системи дозволяє копіювати файли у папки, доступ до яких обмежений. Судячи з усього, користувачі знову під загрозою, але їм вже не звикати.

Фахівці з кібербезпеки припускають, що Windows усуне дефекти 11 червня, коли вийде наступне оновлення. Настійно не рекомендуємо залишати свій ноутбук або комп'ютер без нагляду до 11 червня…» ***(Виявлено нову вразливість у Windows 10: не минуло й тижня // znaj.ua (https://znaj.ua/techno/235283-viyavleno-novu-vrazlivist-u-windows-10-ne-minulo-y-tizhnya). 27.05.2019).***

***

«Інтернет-митець Гуо О Донг створив одну із найбільш незвичних інсталяцій у світі. Це звичайний ноутбук, а цінним його роблять шість найбільш небезпечних вірусів. Вони цілком працездатні, досить лише під'єднати лептоп до Wi-Fi або вставити в нього USB-диск. Творча інсталяція отримала назву «Існування Хаосу», і її продають за $1 200 749 на момент написання цієї замітки…

Основою інсталяції став 10,2-дюймовий нетбук Samsung NC10-14GB. Це бюджетний апарат на базі першого покоління процесорів Intel Atom N270 (відоме своєю низькою продуктивністю), екраном 1024×600 пікселів, 1 ГБ оперативної пам'яті та 160 ГБ жорстким диском. Девайс постачався з Windows XP Home.

Митець інсталював в ноутбук шість найбільш руйнівних вірусів усіх часів для ОС Windows. За оцінками митця, загальні збитки від цих шести вірусів складають щонайменше $95 трильйонів. В ноутбуці розмістили:

Вірус ILOVEYOU, що відправляється по електронній пошті, заразив близько 500 000 систем, сума збитку склала $15 мільярдів, з них $5,5 мільярда в першу тиждень

MyDoom, один з найбільш швидко поширюваних черв'яків, руйнівна діяльність оцінюється в $38 мільярдів

SoBig з властивостями «хробака» і трояна, що відправляється по електронній пошті як вірусний спам. Торкнувся сотень тисяч ПК, фінансові втрати від його дій склали приблизно $37 мільярдів

WannaCry – програма-вимагач, яка також створювала бекдори в системах. Атака торкнулася більше 200 000 комп'ютерів в 150 країнах і завдала шкоди в розмірі $100 мільйонів

DarkTequila — шкідливий софт, націлений в першу чергу на користувачів з Латинської Америки. Краде банківські та корпоративні дані навіть в автономному режимі, обійшовся в мільйони доларів багатьом компаніям

BlackEnergy 2 — руткіт, використаний при кібератаці, яка викликала масштабне відключення електроенергії в Україні в грудні 2015-го.» ***(Євген Корольов. Виставили на продаж ноутбук із 6 найнебезпечнішими вірусами, ціна – понад $1,2 млн // Tech Today (https://techtoday.in.ua/news/vystavyly-na-prodazh-noutbuk-iz-6-najnebezpechnishymy-virusamy-czina-ponad-1-2-mln-114903.html). 27.05.2019).***

***

«Компания ESET напоминает пользователям о глобальной атаке вируса WannaCryptor (или WannaCry), ставшего всемирно известным в связи с масштабами заражения два года назад. Такая колоссальная атака была вызвана эксплойтом EternalBlue, который был общедоступным, чем и воспользовались

киберпреступники. С тех пор использование эксплойта в злонамеренных целях растет с каждым днем.

EternalBlue был якобы похищен из «Агентства национальной безопасности» (NSA) в 2016 г., а 14 апреля 2017 г. известная группа киберпреступников Shadow Brokers распространила эксплойт в интернет-сети. Программа нацелена на уязвимость реализации протокола Server Message Block (SMB) через порт 445. Уязвимость была обнаружена и исправлена корпорацией Microsoft еще до начала атаки WannaCryptor в 2017 г.

По данным Shodan, на сегодня существует около миллиона устройств, использующих устаревший протокол SMB v1 во время подключения к общественному Интернету. Большинство этих устройств находятся в США, Японии и России. Возможными причинами проникновения EternalBlue в интернет-сеть являются плохо развита система безопасности и отсутствие исправлений.

На основе данных телеметрии ESET, попытки атаки, связанные с EternalBlue, достигают исторических вершин, причем сотни тысяч случаев заражений блокируются каждый день.

Кроме злонамеренного использования, распространение данного эксплойта растет в системах внутренней безопасности предприятий. Например, отделы технической безопасности различных компаний используют его как средство для поиска уязвимостей в корпоративных сетях.

Кроме WannaCryptor, EternalBlue стал причиной большинства известных кибератак. Эксплойт также использовался в 2017 г. во время атаки Diskcoder.C (также известная как Petya, NotPetya и ExPetya) и программы-вымогателя BadRabbit, которая была нацелена на сеть Wi-Fi одного из отелей. Также с помощью эксплойта распространялись трояны и программы для майнинга криптовалют в Китае.

Все кибератаки, связанные с данным эксплойтом, подтверждают важность своевременного исправления уязвимостей с помощью надежных решений безопасности, осуществляющих всестороннюю защиту устройства и обнаружения вредоносных программ на нем.» ***(Распространение эксплойта EternalBlue достигает новых висот // Компьютерное Обозрение (https://ko.com.ua/rasprostranenie_jeksplojta_eternalblue_dostigaet_novyh_vysot_128879). 28.05.2019).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Влада Нідерландів екстрадувала до США громадянина України, звинуваченого в злочинах в кіберпросторі. Про це йдеться в заяві, опублікованій в п’ятницю на сайті Міністерства юстиції США…

Як випливає з документа, йдеться про 31-річного Олексія Іванова. Влада США вважає, що він і його спільники розповсюджували в інтернеті шкідливі

програми для отримання доступу до комп'ютерів користувачів. Далі вони за гроші надавали іншим особам можливість частково контролювати ці ПК.

За даними Мін'юсту США, Іванов причетний до здійснення кібератак, які торкнулися мільйонів комп'ютерів. Більше сотні з них перебували на території штату Нью-Джерсі.

Українець був затриманий владою Нідерландів в жовтні 2018 року в рамках розслідування, ключову роль в якому грала Секретна служба США. Американська влада висунула йому звинувачення в грудні минулого року, тоді вони були засекречені. Іванов був екстрадований в США 2 травня.

Планується, що українець постане перед судом у Ньюарку (штат Нью-Джерсі) протягом доби. Йому відмовлено у звільненні під заставу…» ***(Олексій Супрун. Нідерланди екстрадували українця до США, якого звинувачують в кібератаках // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1797932-niderlandi-ekstraduvali-ukrayintsya-v-ssha-yakogo-zvinuvachuyut-v-kiberatakakh). 04.05.2019).***

***

«Минюст США предъявил обвинения китайской хакерской группировке, которую считает ответственной за взлом в 2015 году базы медицинской страховой компании Anthem и хищение данных 78 млн человек, сообщил помощник генпрокурора США Брайан Бенчковски.

По его словам, группировка базируется в Китае и действует «с чувством безнаказанности». Она «осуществила один из наихудших компьютерных взломов в истории», который был «исключительно сложным».

Хакеры получили доступ к именам, телефонам, электронным адресам, информации о занятости и доходах, номерам социального страхования американцев…

Кроме Anthem пострадали еще как минимум три крупных фирмы.

Об арестах кого-то из хакеров не сообщалось.

Еще в 2015 году следователи, занимающиеся этим делом, заявляли, что власти Китая могут оказывать поддержку организаторам хакерской атаки.» ***(Антон Антонов. США обвинили китайцев в крупной кибератаке // Деловая газета «Взгляд» (https://vz.ru/news/2019/5/10/976983.html). 10.05.2019).***

***

Технічні аспекти кібербезпеки

«…примерно каждый второй человек с "умным" устройством, которым можно управлять с помощью смартфона, не меняет исходный пароль после покупки.

Этот пароль по умолчанию легко взломать, и, по данным Немецкой ассоциации технических инспекционных агентств (VdTUV), 47% пользователей с готовностью признают, что никогда не меняли его.

Надежный пароль состоит как минимум из восьми символов, включая заглавные и строчные буквы, цифры и специальные символы. Он также не должен быть нормальным словом из словаря.

Вам следует продумать, какие устройства действительно должны полностью подключаться к Интернету и внешнему миру. Возможно, достаточно просто интегрировать их в домашнюю сеть и управлять ими только внутри здания через смартфон или планшет (а не с работы, например). Это затрудняет доступ хакеров к сети.

Если вы действительно любите "умные" домашние устройства, то рассмотрите создание только для этих девайсов отдельной сети WLAN, которая не имеет связи с компьютерами и планшетами, где хранятся ваши личные данные.

По мнению экспертов, устройства, которые особенно важны для безопасности, такие как сетевые системы сигнализации или камеры видеонаблюдения, должны быть подключены только с помощью кабеля, если это возможно, и не должны иметь доступ к беспроводной сети.

Кроме того, при выборе устройства следует убедиться, что все отправляемые им данные зашифрованы. Это обеспечивает более безопасную связь между фактическим гаджетом, маршрутизатором и приложением на вашем смартфоне…» ***(Ирина Фоменко. The Star Online: половина пользователей оставляют свои "умные" устройства уязвимыми для хакеров // Internetua (https://internetua.com/the-star-online-polovina-polzovatelei-ostavlyauat-svoi-umnye-ustroistva-uyazvimymi-dlya-hakerov). 13.05.2019).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Исследователи в области безопасности обнаружили новый класс уязвимостей в чипах Intel, которые могут использоваться для кражи конфиденциальной информации непосредственно из процессора…

Ошибки напоминают Meltdown и Spectre. Спекулятивное выполнение помогает процессорам предсказать в определенной степени, что может понадобиться приложению или операционной системе в будущем, благодаря чему приложение будет работать быстрее и эффективнее. Процессор выполнит свои прогнозы, если они понадобятся, или откажется от них, если они не нужны.

В случае с Meltdown и Spectre произошла утечка секретных данных, хранящихся в процессоре, включая пароли, секретные ключи и токены учетных записей, а также личные сообщения.

"ZombieLoad", как его называют, - это побочная атака, нацеленная на чипы Intel, позволяющая хакерам эффективно использовать недостатки разработки, а не внедрять вредоносный код. В Intel заявили, что ZombieLoad состоит из четырех ошибок, о которых исследователи сообщили производителю всего месяц назад.

Почти все компьютеры с чипами Intel с 2011 года подвержены уязвимостям. Микросхемы AMD и ARM не входят в это число.

ZombieLoad берет свое название от количества данных, которые процессор не может понять или обработать должным образом, заставляя процессор запрашивать помощь у микрокода процессора для предотвращения сбоя. Приложения обычно могут видеть только свои данные, но эта ошибка предполагает утечку информации. Исследователи заявили, что ZombieLoad будет пропускать любые данные, загруженные в настоящее время ядром процессора.

Уязвимости могут использовать для того, чтобы увидеть, какие веб-сайты посещает человек в режиме реального времени, но их можно легко перенести, чтобы получить пароли или токены доступа для входа в учетную запись жертвы.

Подобно Meltdown и Spectre, ZombieLoad поражает не только ПК и ноутбуки, но и облака. ZombieLoad может запускаться на виртуальных машинах, которые должны быть изолированы от других виртуальных систем и их хост-устройств.

Один из исследователей Даниэль Грусс сообщил, что ZombieLoad "работает так же, как на ПК, и может считывать данные с процессора". Это потенциально серьезная проблема в облачных средах, где виртуальные машины разных клиентов работают на одном и том же серверном оборудовании.

Пользователям, по словам Грусса, необходимо установить исправления. Intel выпустил микрокод для исправления уязвимых процессоров, включая чипы Intel Xeon, Intel Broadwell, Sandy Bridge, Skylake и Haswell. Также это касается микросхем Intel Kaby Lake, Coffee Lake, Whiskey Lake, Cascade Lake и всех процессоров Atom и Knights.

Но другие технологические гиганты, такие как производители потребительских ПК и устройств, также выпускают патчи в качестве первой линии защиты от возможных атак. Apple, Microsoft и Google уже выпустили исправления.

"Обновления микрокодов, как и предыдущие патчи, будут влиять на производительность процессора. Большинство исправленных потребительских устройств могут в худшем случае потерять 3% производительности и до 9% в среде центра обработки данных", - заявил представитель Intel. Ни Intel, ни Грусс и его команда не выпустили код эксплойта, поэтому прямой и непосредственной угрозы для обычного пользователя нет.» ***(Ирина Фоменко. Обнаружена уязвимость практически в каждом чипе Intel с 2011 года // Internetua (https://internetua.com/obnarujena-uyazvimost-prakticseski-v-kajdom-csipe-intel-s-2011-goda). 15.05.2019).***

***

«…Во вторник, 14 мая, Financial Times (FT) сообщила об уязвимости в мессенджере WhatsApp, которая позволяла при помощи голосовых звонков устанавливать на смартфон программу-шпион. Представитель WhatsApp заявил, что атака имела все признаки того, что над ней работала «частная компания, сотрудничающая с правительствами в области разведки». WhatsApp сообщил об инциденте в министерство юстиции США и в ирландскую комиссию по защите данных (Data Protection Commission).

WhatsApp пока не оценивал, сколько из 1,5 млрд пользователей мессенджера пострадали от уязвимости, которой подвержены смартфоны как с Android, так и с iOS. Последнее обновление, устраняющее уязвимость, мессенджер выпустил в понедельник. Эксперты по кибербезопасности описали, как защититься от угрозы.

Чаще всего на смартфон устанавливалась шпионская программа Pegasus. Ее разработала израильская NSO Group, которая специализируется на создании софта для спецслужб. Троян имеет модульную структуру и способен загружать недостающие компоненты, чтобы читать sms-сообщения или прослушивать звонки, делать скриншоты, записывать нажатия клавиш, получать доступ к контактам истории браузера и т. д., перечисляет руководитель департамента аудита информационной безопасности компании «Инфосекьюрити» Сергей Ненахов.

Пользователю стоит проверить историю звонков: если поступали звонки с неизвестных номеров, возможно, совершалась атака, указывает руководитель группы исследований безопасности мобильных приложений Positive Technologies Николай Анисеня. Также нужно проверить, не появилось ли на устройстве новых или дублирующих приложений (например, второй браузер Google Chrome), указывает он. А еще следует проверить версию мессенджера, говорит Ненахов. Уязвимость затрагивает WhatsApp для Android (до выпуска 2.19.134) и iOS (до 2.19.51), а также необновленные версии WhatsApp Business и версии мессенджера для WindowsPhone (до 2.18.348) и операционной системы Tizen (до 2.18.15)…» ***(Алена Сухаревская. Reuters: уязвимость WhatsApp угрожает меньшинству пользователей // АО Бизнес Ньюс Медиа (https://www.vedomosti.ru/technology/articles/2019/05/14/801345-uyazvimost-whatsapp). 14.05.2019).***

***

«…Основатель соцсети «ВКонтакте» и приложения Telegram раскритиковал мессенджер WhatsApp из-за проблем с безопасностью данных пользователей. По его мнению, администрация WhatsApp умышленно запутывает коды своих приложений, чтобы специалисты по безопасности не смогли их изучить.

«Каждый раз, когда WhatsApp приходится исправлять критическую уязвимость в своем приложении, на ее месте появляется новая. Все их проблемы безопасности работают как бэкдоры», - написал Дуров в своем блоге.

Он также предположил, что WhatsApp и его материнская компания Facebook сотрудничают с ФБР, внедряя бэкдоры в приложение.

«Я понимаю, что силовые структуры оправдывают установку бэкдоров антитеррористическими усилиями. Проблема в том, что такие бэкдоры могут также использоваться преступниками и авторитарными правительствами. Неудивительно, что диктаторы, похоже, любят WhatsApp. Отсутствие безопасности позволяет им шпионить за своими людьми», - подчеркнул Дуров.

Создатель Telegram напомнил, что пользователи WhatsApp постоянно сталкиваются с проблемами и утечками и призвал переходить на более безопасные мессенджеры…» ***(Создатель Telegram обвинил WhatsApp в сотрудничестве с ФБР // SecurityLab.ru (https://www.securitylab.ru/news/499120.php). 16.05.2019).***

***

«…Компания Google сообщила об отзыве аппаратных ключей безопасности Titan Security Key в связи с обнаруженной уязвимостью, связанной с сопряжением по Bluetooth. Согласно информации в блоге компании, баг позволяет злоумышленнику, находящемуся на расстоянии примерно 9 м от устройства, взамодействовать с ключом или гаджетом.

Проблема вызвана некорректной конфигурацией протоколов сопряжения по Bluetooth в Titan Security Key и затрагивает только Bluetooth Low Energy (BLE)-версию решения. Версия, работающая через USB и NFC, уязвимости не подвержена.

Как отмечается, баг достаточно сложно проэксплуатировать, для этого атакующему потребуется иметь доступ к учетной записи жертвы и суметь подключиться к аппаратному ключу до того, как к нему подключится устройство пользователя.

Компания пообещала бесплатно заменить все уязвимые ключи.

Titan Security Key - аппаратное решение, предназначенное для надежной аутентификации и авторизации с применением устройств USB или Bluetooth.» ***(Google отзывает ключи безопасности Titan из-за уязвимости // SecurityLab.ru (https://www.securitylab.ru/news/499117.php). 16.05.2019).***

***

«Процессоры Intel подвержены четырем вновь выявленным очень опасным уязвимостям. Информацию об этом компания пыталась скрыть путем подкупа исследователей, обнаруживших их…

Компания Intel предприняла попытку подкупа исследователей в области кибербезопасности Амстердамского свободного университета (Vrije Universiteit Amsterdam, VU) с целью сокрытия информации о новых уязвимостях в ее процессорах. Речь про класс уязвимостей Microarchitectural Data Sampling (MDS), основанных на технологии спекулятивного исполнения команд и включающий в себя как минимум четыре уязвимости, в том числе RIDL (Rogue In-Flight Data Load).

RIDL обнаружил студент VU Стефан ван Шайк (Stephan van Schaik), за что университету полагалось финансовое вознаграждение в рамках программы Intel по ограничению распространения информации об уязвимостях в ее продуктах. Максимальный размер награды за выявление столь серьезной угрозы составляет $100 тыс., но Intel предложила искусственно снизить степень ее значимости и официально выплатить университету всего $40 тыс. За согласие на это условие чипмейкер предложил исследователям VU дополнительные $80 тыс., но получил отказ. Информацию о случившемся опубликовал голландский ресурс NRC.

По словам Intel, ее программа выплаты вознаграждений позволяет ограничивать распространение сведений о выявленных уязвимостях. Снижение темпов распространения информации дает Intel время на разработку необходимого обновления до того, как все подробности попадут в общий доступ и станут известны, в том числе, и злоумышленникам…

Не сумев подкупить исследователей, Intel признала факт существования уязвимостей класса MDS в своих процессорах. Примечательно, что технологию спекулятивных команд, дающую процессору возможность предугадывать, какие данные понадобятся приложению или ОС, с целью повышения производительности эксплуатируют не только MDS-уязвимости, но и ранее выявленные атаки Meltdown и Spectre.

В класс MDS вошли атаки ZombieLoad, Fallout, RIDL и STLF (Store-to-Leak Forwarding), и им подвержены все процессоры Intel, выпущенные с 2011 г. С целью обеспечения их защиты Intel выпустит «заплатку» для микрокода, которая, по ее словам, может незначительно снизить производительность чипов. Точные значения компания не приводит…

По оценке экспертов Apple и Google, одного патча безопасности для микрокода будет недостаточно: для более надежной защиты от уязвимостей MDS они предлагают отключить технологию многопоточности Hyper-Threading. Это действие тоже может отразиться на производительности процессора – она может снизиться на 40%.

Обе компании уже выпустили апдейты собственных продуктов, нивелирующие действие атак MDS. В частности, Google начала распространение «заплаток» для Chrome OS-устройств на чипах Intel, браузера Chrome и собственной облачной инфраструктуры. Apple в свою очередь выпустила обновление macOS Mojave 10.14.5 для всех Mac и MacBook, выпущенных с 2011 г. по 2019 г. Компания отметила, что после установки обновления пользователи падения производительности не заметят.

Компания Microsoft тоже подготовила патч безопасности – KB4494441 для Windows 10 1809 и KB4500109 для 1903. В Linux-среде необходимые обновления уже получили дистрибутивы Ubuntu, FreeBSD, RHEL и NetBSD, а также ядро Linux – изменения внесены в версию 5.1.2…» ***(Intel пыталась подкупить исследователей, чтобы скрыть уязвимости в своих процесорах // Goodnews.ua (http://goodnews.ua/technologies/intel-pytalas-podkupit-issledovatelej-chtoby-skryt-uyazvimosti-v-svoix-processorax/). 18.05.2019).***

***

«Компания Microsoft выпустила срочное обновление для операционных систем Windows. Программисты признались, что программное обеспечение имеет критическую уязвимость, хотя и заверяют, что злоумышленники им никогда не пользовались. По крайней мере пока.

Как рассказали в компании, хакеры могли воспользоваться этой прорехой в безопасности ОС, чтобы получить удаленный доступ к компьютеру незаметно для пользователя, то есть, по признанию программистов Microsoft, проблема «создавала громадную червоточину».

Патч с кодом, который закроет брешь и инструкций о том, как можно обезопасить свою систему, выпустили даже для версий Windows, которые официально перестали поддерживать больше 5 лет назад: архивы с заплатками для Windows XP и Windows 2003 появились на сайте одновременно с исправлениям для более новых и частично поддерживаемых Windows 7 и Windows 2008, то есть

уязвимость существует как минимум 16 лет. При этом исправление для современных ОС придут без вмешательства пользователя. Главное – не запрещать системе установить "обновку".

Обновить старые операционные системы Microsoft решил впервые с мая 2017 года, когда крипточервь-вымогатель WannaCry поразил за несколько дней более 300 тыс. компьютеров. Брешь в защите операционной системы обнаружили, правда, не разработчики Microsoft – как признал IT-гигант, на уязвимость им указали сотрудники Национального центра кибербезопасности Великобритании.» ***(Во всех версиях Windows обнаружили опасную уязвимость // Goodnews.ua (http://goodnews.ua/technologies/vo-vsex-versiyax-windows-obnaruzhili-opasnuyu-uyazvimost/). 16.05.2019).***

***

«Разработчики Mozilla выпустили новую версию браузера Firefox для Windows, macOS, Linux и Android. В релизе 67.0 обозревателя исправлена 21 уязвимость, а также добавлена функция блокировки встроенных криптомайнеров и скриптов, скрытно отслеживающих пользователя по цифровым отпечаткам.

Две бреши признаны критическими, так как они позволяют злоумышленнику выполнять вредоносные действия без привлечения пользователя. Эксплуатация CVE-2019-9814 и CVE-2019-9800 может привести к выполнению на устройстве стороннего кода через нарушение целостности памяти. Множественные ошибки при работе с памятью были выявлены командой разработчиков Mozilla и устранены с выпуском обновления.

Еще одиннадцати проблемам присвоен высокий уровень опасности. Шесть из них связаны с ошибкой Use-After-Free, возникающей при работе различных компонентов браузера. Некорректное использование динамической памяти может привести к прекращению работы Firefox, отказу в обслуживании или выполнению стороннего кода за пределами песочницы. Уязвимости получили следующие идентификаторы:

CVE-2019-9818 вызвана возможностью состояния гонки в сервере аварийного завершения работы.

CVE-2019-9820 проявляется при вызове обработчика ChromeEventHandler в компоненте DocShell.

CVE-2019-9821 связана с неправильной работой функции AssertWorkerThread.

CVE-2019-11691 допускает использование потока XMLHttpRequest после завершения работы цикла.

CVE-2019-11692 возникает при удалении работающего в данный момент слушателя событий из менеджера процессов браузера.

CVE-2019-7317 обнаружена в операторе png_image_free библиотеки libpng.

Несколько независимых исследователей сообщили разработчикам о проблеме с многопоточностью при обработке JavaScript-сценариев в Firefox для macOS. Уязвимость, допускающая атаки типа Spectre, была исправлена в релизе 10.14.5 операционной системы Apple и теперь получила заплатку в коде браузера. Патч для

CVE-2019-9815 позволяет отключить поддержку технологии Hyper-threading в приложениях, которые выполняют потенциально опасный код.

Некорректная обработка типов используемых объектов в компоненте UnboxedObjects могла привести к манипулированию сценариями JavaScript и обходу процедур безопасности. Добавив заплатку для CVE-2019-9816, создатели Firefox отметили, что уязвимый модуль по умолчанию отключен во всех актуальных релизах браузера.

Ошибка, идентифицированная как CVE-2019-9817, допускает чтение изображений, созданных при помощи HTML-функции canvas и расположенных на стороннем ресурсе. Недостаток нарушает правило ограничения домена и может быть использован для кражи графических данных.

Серьезный баг исправлен в FetchAPI, предоставляющем сторонним приложениям интерфейс для использования ресурсов браузера. Как сообщают разработчики, эксплуатация CVE-2019-9819 может вызвать несовпадение разделов JavaScript и привести к аварийному завершению работы браузера.

Еще одна заплатка связана с переполнением буфера в компоненте WebGL для Linux. По информации специалистов, проблема кроется в функции bufferdata и может привести к зависанию вкладки с вредоносным содержимым. Уязвимость, найденная ИБ-исследователем с псевдонимом crixer, получила идентификатор CVE-2019-11693.

Остальные исправления относятся к ошибкам среднего и низкого уровня опасности. Новый релиз доступен для всех пользователей Firefox через функцию автоматического обновления интернет-обозревателя. Предыдущая версия браузера вышла в середине марта и также содержала патчи для 21 уязвимости.» ***(Maxim Zaitsev. В новый Firefox добавлена блокировка криптомайнеров // Threatpost (https://threatpost.ru/firefox-67-features-cryptominer-blocking-ability/32751/). 22.05.2019).***

***

«**Эксперты Google Project Zero, команды специалистов по уязвимостям нулевого дня, опубликовали базу собранных по открытым источникам 0-day и призвали сообщество к совместной работе.** Случаи эксплуатации были обнаружены при расследовании атак таких сильных группировок, как APT3 (также известна как Buckeye), APT28 (Sofacy, Fancy Bear), Equation Group.

Архив представляет собой таблицу со справочной информацией по каждой уязвимости, включая дату обнаружения, затронутые продукты, ссылки на описание, аналитику и рекомендации безопасности. Эксперты не ставили себе целью создать всеобъемлющую базу — материалы собираются по тем продуктам, которые Project Zero изучает в рамках своей основной деятельности. Это решения таких компаний, как Adobe, Apple, Facebook, Google, Microsoft. Системы, поддержка которых закончилась на момент обнаружения уязвимости, также не попали в архив…

Эксперты также поделились некоторыми выводами. Так, чаще всего действия злоумышленников направлены на порчу данных в памяти. С такими ошибками

связано 68% уязвимостей в базе. Подробное техническое описание есть у 86% всех багов в архиве.

В среднем в кибератаках новые 0-day появляются каждые 17 дней. Разработчики, как правило, закрывают брешь в течение 15 дней после обнаружения.

Эксперты отмечают, что публикация этих материалов вовсе не означает поощрение киберпреступности, а данные приводятся исключительно в информационных целях. Исследователи также напоминают, что фактически им удалось изучить лишь проваленные кампании — по ним не стоит судить о поведении всех киберпреступников…

В опубликованной базе есть и уязвимость WhatsApp, которая применялась в недавних шпионских атаках. Дыра в системе звонков позволила неизвестным злоумышленникам внедрить вредоносный код в смартфоны журналистов и правозащитников.» ***(Dmitry Nazarov. Google собирает материалы об эксплуатации 0-day уязвимостей // Threatpost (https://threatpost.ru/google-creates-0day-database/32678/). 17.05.2019).***

***

«Уязвимость протокола RDP в операционных системах Windows может быть использована злоумышленниками для кибератак и нуждается в немедленной установке обновлений безопасности. К такому выводу пришли ИБ-специалисты, разработавшие PoC эксплуатации CVE-2019-0708 и инструменты для обнаружения проблемных устройств.

Критический недостаток, получивший название BlueKeep, допускает удаленное выполнение кода с системными привилегиями и не требует от злоумышленника авторизации на целевой машине. Microsoft оценила баг как критический и 14 мая выпустила патч для своих операционных систем. Производитель не раскрывал технические детали ошибки, чтобы не провоцировать атаки на пользователей, которые не установили апдейты.

Тем не менее ИБ-специалист под псевдонимом Valthek заявил, что сумел создать PoC для получения административных привилегий и дистанционного запуска стороннего скрипта через RDP-доступ. Исследователь отказался обнародовать подробности, сославшись на высокий уровень опасности эксплойта. Работоспособность программы подтвердили сторонние эксперты, заявившие, что она допускает удаленное выполнение кода в среде Windows XP.

Аналитик «Лаборатории Касперского» Борис Ларин опубликовал анимированное изображение, которое демонстрирует возникновение «синего экрана смерти» на виртуальной машине с запущенной Windows XP. Специалист заявил, что компания создала инструмент, который поможет обнаружить и предотвратить эксплуатацию бага и готова поделиться им с заслуживающими доверия представителями индустрии.

Принципиальную возможность эксплуатации CVE-2019-0708 подтвердил также ИБ-эксперт проекта Zerodium Чауки Бекрар (Chaouki Bekrar). Исследователь отметил, что проблема затрагивает хосты, работающие на базе Windows Server 2008, Windows 7, Windows 2003 и Windows XP. Как заявил специалист, не

авторизованный в системе злоумышленник может получить root-права для удаленного доступа к устройству. Две последние ОС уже не поддерживаются производителем, однако все равно получили критически важный патч.

Знакомые с проблемой аналитики указывают, что в ближайшее время эксплойт для атаки Windows-машин через RDP смогут создать и злоумышленники. Для предотвращения нападений ИБ-специалисты рекомендуют немедленно обновить операционную систему или отключить на ней использование службы Remote Desktop Services.» ***(Dmitry Nazarov. Специалисты прогнозируют атаки с использованием BlueKeep // Threatpost (https://threatpost.ru/experts-are-waiting-for-bluekeep-exploit-attacks/32747/). 22.05.2019).***

***

«Исследователь Дэвид Уэллс (David Wells) из Tenable обнаружил в Slack 3.3.7 уязвимость, которая позволяла получить доступ к скачанным на устройство файлам. Проблема затронула десктопное приложение для Windows. Эксперт сообщил разработчикам о найденном баге, и они уже исправили его в новой версии 3.4.0.

Проблема была связана с тем, как приложение обрабатывало внутренние ссылки вида slack://… Атакующий мог создать специальный адрес, который не отличается от обычного внешне и изменяет путь сохранения файлов. В качестве директории злоумышленник мог указать в том числе удаленный сервер. Помимо это, баг позволял менять некоторые другие настройки.

Уэллс также обнаружил, что атакующий может изменять скачанные файлы. Таким образом, злоумышленник способен встроить в документ вредоносный код, который автоматически запустится, когда жертва откроет вложение.

Несколько усложняет задачу преступникам запрет создавать гиперссылки в сообщениях Slack — получатель всегда видит URL и вряд ли рискнет переходить по незнакомому адресу. Однако это ограничение можно обойти, заменив в специальном поле значение «текст» на «вложение». В результате злоумышленник может замаскировать URL под любой текст, например https://www[.]google[.]ru/, и тем самым ввести в заблуждение жертву.

Вредоносная ссылка могла быть отправлена в личном сообщении или в канал, к которому атакующий имеет доступ. Однако опасность может исходить не только от участников беседы. Уэллс указывает, что даже неавторизованный злоумышленник способен изменить место сохранения файлов с помощью RSS-потоков на сторонних сайтах.

Если канал использовал RSS-потоки с внешнего ресурса, то жертве достаточно было кликнуть по ссылке на этом ресурсе. При этом злоумышленник может изменить настройки, даже если у него нет доступа к рабочему пространству пользователя…» ***(Dmitry Nazarov. Уязвимость Slack позволяла красть данные из списка загрузок // Threatpost (https://threatpost.ru/slack-vulnerability-allows-to-sreal-downloaded-files/32722/). 20.05.2019).***

***

«**Сотни тысяч маршрутизаторов TP-Link уязвимы из-за ошибки, которую можно использовать для удаленного управления устройством…** Компании потребовалось более года, чтобы опубликовать исправления на своем веб-сайте.

Уязвимость позволяет любому неопытному злоумышленнику удаленно получить полный доступ к маршрутизатору. Для работы эксплойта используется пароль по умолчанию, который многие не меняют.

В наихудшем сценарии преступник может устраивать масштабные хакерские атаки на маршрутизаторы, используя механизм, аналогичный тому, как работают ботнеты, например, Mirai.

Эндрю Маббитт, основатель британской компании Fidus Information Security по кибербезопасности, впервые обнаружил и раскрыл ошибку удаленного выполнения кода для TP-Link в октябре 2017 года. TP-Link выпустил исправление через несколько недель для уязвимого маршрутизатора WR940N. В январе 2018 Маббитт снова предупредил TP- Link об уже другом проблемном роутере, TP-Link WR740N.

TP-Link сообщает, что уязвимость быстро исправили на обоих маршрутизаторах. Но при проверке оказалось, что прошивка для WR740N не была доступна на сайте. Представитель TP-Link заявил, что обновление "в настоящее время доступно по запросу технической поддержки", но не объяснил, почему.

Маршрутизаторы давно славятся проблемами безопасности. В основе сети любой недостаток, влияющий на роутер, может иметь катастрофические последствия для каждого подключенного устройства.

Получив полный контроль над маршрутизатором, злоумышленник может нанести ущерб сети. Изменение настроек роутера влияет на всех, кто подключен к одной и той же сети, например, на изменение настроек DNS, чтобы обманом заставить пользователей посетить фейковую страницу и украсть их учетные данные.

В TP-Link отказались сообщить, сколько именно потенциально уязвимых маршрутизаторов было продано. WR740N сняли с продажи в 2017 году. После проверки двух поисковых систем на наличие открытых устройств и баз данных, Shodan и Binary Edge, каждый сайт подтвердил, что число уязвимых маршрутизаторов составляет от 129 000 до 149 000.

"TP-Link обязаны предупредить пользователей об обновлении, если тысячи устройств по-прежнему уязвимы, вместо того, чтобы надеяться, что они обратятся в службу технической поддержки компании", - заявил Маббитт.

В США в скором времени будут требовать от компаний продавать устройства с уникальными паролями по умолчанию, чтобы бот-сети не могли захватывать подключенные к Интернету устройства и использовать их общую пропускную способность для отключения веб-сайтов в автономном режиме.» ***(Ирина Фоменко. TechCrunch: сотни тысяч маршрутизаторов оказались уязвимы для хакерских атак // Internetua (https://internetua.com/Techcrunch-sotni-tusyach-marshrutizatorov-okazalis-uyazvimy-dlya-hakerskih-atak). 23.05.2019).***

***

«Компания ESET предупреждает об уязвимости BlueKeep в службах удаленного рабочего стола (RDP), которая вскоре может стать новым вектором для распространения киберугроз. В случае использования уязвимости киберпреступники смогут получить доступ к компьютеру жертвы без необходимых учетных данных или взаимодействия с пользователем.

Стоит отметить, исправление от компании Microsoft для операционных систем доступно с 14 мая…

В связи с потенциальной опасностью специалисты ESET подготовили рекомендации для защиты от атак с использованием этой уязвимости:

Применить обновления операционной системы. Программное обеспечение Windows должно быть обновлено до актуальной версии. При использовании Windows XP или Windows 2003 исправления нужно загрузить и применить как можно быстрее.

Отключить протокол удаленного рабочего стола. Несмотря на то, что RDP не является уязвимым, Microsoft рекомендует организациям выключить его, пока не будут применены актуальные обновления. Кроме этого, для минимизации вероятности атаки удаленный рабочий стол должен быть включен только на тех устройствах, где протокол действительно нужен.

Правильно настроить протокол удаленного рабочего стола (RDP). Если организации нужно использовать RDP, избегайте доступа к публичной сети Интернет. Только устройствам в локальной сети или благодаря доступу через VPN можно устанавливать удаленный сеанс. Другим вариантом является фильтрование доступа к удаленному рабочему столу с помощью брандмауэра, который дает разрешение определенному диапазону IP. Если это невозможно, следует использовать многофакторную аутентификацию.

Применить аутентификацию на уровне сети (NLA). Таким образом, перед установкой удаленного сеанса пользователь должен осуществить аутентификацию. Однако, как добавляет компания Microsoft, системы все еще могут быть уязвимыми, если киберпреступник имеет актуальные данные для входа в учетную запись, которые можно использовать для успешной аутентификации.

Используйте многоуровневое решение для обнаружения и предотвращения атак, которые используют уязвимости на уровне сети.» ***(Обнаружена опасная уязвимость в службах удаленного рабочего стола // Компьютерное Обозрение (https://ko.com.ua/obnaruzhena_opasnaya_uyazvimost_v_sluzhbah_udalennogo_rabochego_stola_128868). 27.05.2019).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Компания Microsoft анонсировала решение для электронных урн для голосования. Система Microsoft 365 for Campaigns призвана защитить

волеизъявление американских граждан на выборах и будет представлена уже в июне 2019 года.

Продукт построен на базе сервиса Microsoft AccountGuard, который был запущен в 2018 году в рамках программы по защите демократии от кибератак. За прошедшее время к AccountGuard подключились 12 европейских стран, включая Бельгию, Германию и Францию.

Второй компонент нового решения — открытый SDK ElectionGuard. Набор инструментов предполагает внедрение в информационные избирательные системы технологии сквозной верификации и вместе с тем позволяет привлекать контролирующие организации для проверки результатов.

В компании подчеркивают, что новые системы не предполагают переход на интернет-голосование и не заменяют традиционные избирательные урны. Решение лишь укрепляет существующие практики, чтобы сделать их более прозрачными и устойчивыми к вмешательствам.

Так, избиратели смогут в любой момент удостовериться, что их голоса учтены правильно. Для этого система будет выдавать им трекер с уникальным кодом, по которому можно будет авторизоваться на специально созданном портале. После окончания выборов на этой площадке граждане смогут убедиться, что их голос действительно достался верному кандидату.

При необходимости ElectionGuard позволяет любому желающему создать собственные средства для проверки электоральных результатов. По замыслу разработчиков, такие сторонние утилиты будут сверять данные в ходе голосования и сделают невозможными скрытые манипуляции при подсчете голосов. Правозащитные и контролирующие организации смогут таким образом отслеживать чистоту процедур, не угрожая течению процессов и анонимности волеизъявления, поскольку все операции проводятся только с зашифрованными данными.

За последнюю часть отвечает технология гомоморфного шифрования, позволяющая проводить математические операции с данными без их преобразования в открытый формат. По словам Microsoft, применение открытых технологий и в этом случае позволят сторонним участникам в любой момент проконтролировать легитимность исполнения процедур.

Для дополнительной проверки новое решение позволяет сверить случайно выбранные бюллетени. Система соотносит их электронные записи с бумажными аналогами, чтобы контролеры могли удостовериться в совпадении данных. Эксперты указывают, что этот механизм повысит доверие к результатам и сократит трудозатраты комиссии по подсчетам голосов.

Все компоненты решения будут опубликованы на GitHub, чтобы разработчики систем электронного учета голосов в других странах могли встроить новые компоненты в свои продукты. Microsoft уже объявила о партнерстве с компаниями, которые поставляют в США более половины машин для голосования. В ближайшие месяцы корпорация планирует запустить систему отзывов, которая позволит будущим участникам процессов ближе познакомиться с возможностями нового решения.» ***(Dmitry Nazarov. Microsoft поможет американцам провести***

честные выборы // Threatpost (https://threatpost.ru/microsoft-will-help-americans-protect-elections/32548/). 07.05.2019).

***

«Спеціалістка з кібербезпеки Стефані Ванроелен проаналізувала п’ять найпопулярніших антивірусів для смартфонів і зрозуміла, що краще обійтися без них.

Бельгійка Стефані Ванроелен (Stephanie Vanroelen) працює в компанії Nviso, яка, зокрема, займається тим, що шукає прогалини в безпеці IT-систем. На конференції з кібербезпеки NoNameCon у Києві (16-17 травня) вона розповіла про своє свіже дослідження антивірусів для смартфонів…

Для аналізу вона взяла безплатні версії п’яти антивірусів зі списку найбільш популярних для Android: Kaspersky Mobile Antivirus, Avast Mobile Security, Norton Security & Antivirus, Sophos Mobile Security, Security Master.

Далі вона проаналізувала, які дозволи просили надати ці додатки, як використовували трафік мережі і якими даними ділилися із серверами.

Перше, що здивувало Стефані Ванроелен, — ці програми доволі великі. Якщо зазвичай мобільні застосунки важать близько 15 мегабайтів, то, приміром, Kaspersky — 45 мегабайтів.Постало питання: чим виправданий такий розмір?

«Деякі додатки запитували IP-адресу, хоча невідомо, навіщо це антивірусу. Інший додаток розбирався із даними мого Wifi: як він використовується, які імена користувачів. Але не відомо, для чого такі дані збирає антивірус на смартфоні. Багато даних, які беруть ці програми, виглядають цікавими для дослідження, але вони зашифровані», — каже дослідниця.

Також антивіруси просять до 96 дозволів, тимчасом як звичайний додаток запитує про близько 15 дозволів. Деякі з цих прав використовуються для того, щоб антивірус міг провести необхідні тести. Проте є й такі дозволи, які доволі важко пояснити. Серед них — згода на здійснення дзвінків…

Ба більше, вони запитують і про можливість встановлювати додаткові пакети програм на телефон. Хоча невідомо, чому компанії не можуть припасувати все необхідне в один оригінальний додаток. Також вони хочуть право змінювати параметри телефону, форматувати картку пам’яті й доступ до управління акаунтами…

«Детектору медіа» Стефані Ванроелен сказала, що так і не змогла дійти висновку, який із цих додатків вона може порекомендувати — значущих відмінностей серед них немає…

Для свого смартфону на IOSя не використовую ці додатки. Як на мене, ґаджет і так достатньо захищений: регулярно оновлює програмне забезпечення, за чим я стежу. Тож антивірус не дає мені ніякої додаткової цінності.

На Android так само: якщо ви оновлюєте ПЗ і стежите за якістю того, що встановлюєте, завантажуєте лише офіційні додатки, то маєте бути у відносній безпеці. На 100 % вас і так нічого не захистить…» ***(Володимир Малинка. Який антивірус обрати для смартфона? Жодного // MediaSapiens (https://ms.detector.media/web/cybersecurity/yakiy_antivirus_obrati_dlya_smartfona_zhodnogo/). 24.05.2019).***

***

«Компания "HP Inc.", американский производитель компьютеров и принтеров, установит программное обеспечение на основе искусственного интеллекта, разработанное израильской фирмой по кибербезопасности "Deep Instinct", на свои компьютеры следующего поколения, чтобы защитить их от кибератак.

Десятки миллионов компьютеров "HP" по всему миру будут защищены программным обеспечением, говорится в заявлении "Deep Instinct" во вторник. О сделке не сообщалось никаких финансовых данных, но веб-сайт "Calcalist" оценил ее в 150 миллионов долларов на четыре года.

"HP" работает вместе со стартапом в Тель-Авиве, который использует глубокое обучение для прогнозирования киберугроз и расширенных атак, чтобы запустить программное обеспечение "HP Sure Sense" и "обеспечить постоянную защиту против самых передовых киберугроз", говорится в заявлении "HP".» ***("HP" установит израильское программное обеспечение на компьютеры нового поколения // ISRAland (http://www.isra.com/news/230465). 28.05.2019).***

***

«Bittium — финская компания с более чем 30-летним опытом в области передовых технологий радиосвязи и обработки биосигналов, создания продуктов для тактической связи, предоставления мобильных устройств и решений для кибербезопасности, сертифицированных для использования войсками на полях сражений.

На днях она представил свой последний смартфон под названием Bittium Tough Mobile 2, который, по ее словам, является «самый безопасным в мире» и подходит как для профессионального, так и для личного использования.

Новинка имеет «многоуровневую структуру безопасности», основанную на усиленной операционной системе Android 9 Pie, с функциями защиты информации и программным обеспечением, интегрированными в исходный код. Это обеспечивает максимально эффективную защиту как данных, хранящихся в устройстве, так и передаваемых данных.

Телефон поставляется с несколькими функциями шифрования, аутентификации и управления ключами, проверкой безопасности при загрузке и во время выполнения программы, защищенной от несанкционированного доступа платформой защиты информации, и режимом конфиденциальности. Последний отключает микрофоны, камеры и Bluetooth, а также снижает точность датчиков одним нажатием кнопки. Tough Mobile 2 совместим с программным обеспечением Bittium Secure Suite, которое позволяет удаленно управлять телефонами и передавать зашифрованные данные.

Компоненты и программные решения проверены для использования органами власти и сертифицированы для безопасного использования государственными чиновниками. Bittium также обещает «лучшую доступность обновлений безопасности по сравнению с обычными смартфонами». Телефон

поддерживает использование нескольких изолированных и безопасных рабочих пространств, что обеспечивает безопасность и конфиденциальность.

Что касается характеристик, Bittium Tough Mobile 2 имеет 5,2-дюймовый сенсорный дисплей с разрешением FullHD, процессор Snapdragon 670, 4 ГБ оперативной памяти, 64 ГБ памяти eMMC с возможностью расширения с помощью mciroSD карт, 12-Мп заднюю и 5-Мп фронтальную камеры, два фронтальных динамика, поддерживает двухдиапазонный Wi-Fi, Bluetooth 5.0 и NFC, а также имеет сертификат защиты от воды и пыли IP67 и MIL-STD-810G от ударов и падений.

Телефон оснащен слотом для двух SIM-карт, батареей емкостью 3000 мАч, а также специальными кнопками для режима конфиденциальности, экстренного вызова и push-to-talk.

Устройство уже доступно для предварительного заказа на сайте Bittium за 1550 евро.» ***(Bazelas. Bittium Tough Mobile 2 — «самый безопасный смартфон в мире» // iLenta (https://ilenta.com/news/smartphone/news_25009.html). 29.05.2019).***

***

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

Алексєєв М. М. Протидія кібернетичним загрозам в Польщі: досвід для України / М. М. Алексєєв // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. - 2018. - № 3. - С. 49-53.

Розглянуто кроки збройних сил Республіки Польща щодо формування захисту кіберпростору та ставлення керівництва Міністерства національної оборони Польщі до цієї проблеми. Приділено увагу нормативно-правовій базі, що визначає основи забезпечення захисту національних інтересів України в кіберпросторі, основним цілям, напрямам та принципам державної політики у сфері кібербезпеки, а також повноваженням державних органів у цій сфері, основним принципам координації їх діяльності щодо забезпечення кібербезпеки.

Шифр зберігання НБУВ: Ж73897

***

Воробієнко П. П. Кіберосвіта : монографія / Воробієнко П. П., Даник Ю. Г., Телелим В. М. - Одеса : ОНАЗ ім. О. С. Попова, 2018. - 207 с.

Розкрито сутність, зміст та взаємозв’язок кібернетичної та інформаційної безпеки. Проаналізовано формування і розвиток кіберосвіти в Україні та у світі. Запропоновано шляхи формування компетенцій з основ кібербезпеки у закладах вищої освіти. Розроблено варіант реалізації організації системи освіти з питань кібербезпеки.

Шифр зберігання НБУВ: ВА831123

***

Єрменчук О. П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монографія / О. П. Єрменчук. - Дніпро, 2018. - 178 с.

Здійснено комплексний аналіз теоретичних і практичних проблем пов'язаних із організацією захисту критичної інфраструктури в Великобританії, Франції, Німеччині, Іспанії, Данії. Розглянуто еволюційні процеси та апробований досвід спільної діяльності залучених державних органів та партнерів з приватного сектору різних держав і їх повноважень, основні складові елементи ієрархічної системи важливі для її побудови та функціонування.

Шифр зберігання НБУВ: ВА830439

***

Збірник тез наукових доповідей науково-практичного семінару «Забезпечення кібербезпеки: правові та технічні аспекти», 8 листопада 2018 року. - Харків, 2018. - 112 с.

Зі змісту:

- Харченко В.С. Людина, система, кіберпростір: без пекові складові для правового аналізу;
- Торяник В.В. Анализ кибербезопасности систем мониторинга на основе интернета дронов;
- Колісник М.О. Індустрія 4.0: кібербезпека і правові засади;
- Фесенко Г.В. Потенційні кіберзагрози для системи управління БПЛА;
- Цуранов М.В. Цілісність інформації як засіб протидії кіберзлочинам;
- Кальченко В.В. Інформаційна безпека та кібербезпека, визначення та терміни;
- Пєвнєв В.Я., Кальченко В.В. Правові та технічні питання кібербезпеки в Україні;
- Стєбєлєв А.М. Конституційні права і свободи людини і громадянина в механізмі забезпечення кібербезпеки;
- Павликівський В.І., Селевко В.Б. Кіберзлочинність та обмежені можливості традиційного кримінального та кримінального процесуального права;
- Каткова Т.Г. Адміністративна відповідальність за порушення законодавства у сфері кібербезпеки;
- Золотарьов С.О. Судова комп'ютерно-технічна експертиза та її роль у захисті кібербезпеки держави;
- Верьовкіна Д.І. Право на захист персональних даних як об'єкт кібербезпеки;
- Глушенко В.І. Суб'єкти національної системи кібербезпеки;
- Ямпольська А.І. Забезпечення кібербезпеки в процесі державної реєстрації на нерухоме майно.

Шифр зберігання НБУВ: ВА830725

***

Карабут Н. О. Засоби підвищення безпеки даних в корпоративних мережах / Н. О. Карабут, Д. В. Швець // Вісник Криворізького національного університету. - 2018. - Вип. 46. - С. 122-125.

Проаналізовано існуючі засоби підвищення безпеки даних в корпоративних мережах. Виявлено найбільш вразливі ланки в програмному та апаратному забезпеченні, що можуть нести загрозу безпеці даних в корпоративній мережі та її функціонуванню в умовах можливих хакерських атак. Запропоновано методи підвищення безпеки зберігання та передачі даних в корпоративних мережах.

Шифр зберігання НБУВ: Ж72501

***

Кондратюк М.В. Комп'ютерна безпека як правова категорія / Кондратюк М.В. // Науковий вісник Херсонського державного університету. Сер. : Юридичні науки. - 2018. - Вип. 5. - С. 58-61.

Запропоновано авторське визначення терміна «комп'ютерна безпека». Проаналізовано, систематизовано і узагальнено зміст комп'ютерної безпеки на основі публікацій науковців та нормативних документів. Розглянуто ряд принципів, що визначають сферу комп'ютерної безпеки. Окреслено специфічні особливості кібербезпеки.

Шифр зберігання НБУВ: Ж73149/юр.

***

Лисиця Д. О. Метод тестування безпеки програмного забезпечення для захисту інформації з використанням технологій реверсної інженерії : автореф. дис. ... канд. техн. наук : 05.13.21 / Лисиця Дмитро Олександрович ; Держ. ун-т телекомунікацій. - Київ, 2019. - 20 с.

Проаналізовано основні вимоги щодо безпеки програмних засобів комп'ютерних систем, наявних методологій тестування безпеки ПЗ та факторів, що впливають на цей процес. Розроблено комплекс математичних моделей технологій генерації та реалізації засобів «тесту на проникнення», що складається з GERT-моделі початкової генерації коду кібератаки несанкціонованого доступу до інформаційних ресурсів та GERT-моделі процесів активного аналізу системи управління ресурсом і впровадження в комп'ютерну систему. Обґрунтовано практичні рекомендації щодо застосування методів та засобів тестування безпеки програмного забезпечення комп'ютерної системи.

Шифр зберігання НБУВ: РА439336

***

Матеріали ІІІ Міжнародної науково-практичної конференції «Актуальні проблеми реформування сучасного законодавства» (14-15 вересня 2018 р.). - Харків, 2018. - 111 с.

Зі змісту:

- Коліса Я.Ю. Розвиток правової охорони комп'ютерних програм.

Шифр зберігання НБУВ: ВА831059

***

Матеріали ІІІ Міжнародної науково-практичної конференції «Україна в умовах реформування правової системи: сучасні реалії та міжнародний досвід» (20-21 квітня 2018 р.) : тези наук. доп. - Тернопіль, 2018. - 407 с.

Зі змісту:

- Юркевич І.І. Кіберзлочинність як загроза інформаційній безпеці.

Шифр зберігання НБУВ: ВА830729

***

Матеріали науково-практичної конференції «Сучасні трансформації розвитку правової системи України», 26 квітня 2018 року. - Черкаси : Пономаренко, 2018. - 121 с.

Зі змісту:

- Харченко Т.О. Актуалізація проблем кіберзлочинності на сучасному етапі в Україні.

Шифр зберігання НБУВ: ВА830789

***

Петрів М.В. Поняття та ознаки кіберсквотингу / Петрів М.В. // Науковий вісник Ужгородського національного університету. Серія : Право. - 2018. - Вип. 52(1). - С. 127-130.

Проаналізовано поняття та ознаки «кіберсквотингу». Розглянуто судову практику. Установлено, що кіберсквотинг є єдиним правопорушенням, яке зумовлює виникнення доменних спорів. Доведено необхідність спеціального правового регулювання відносин використання комерційних позначень у цифровому середовищі.

Шифр зберігання НБУВ: Ж68850/пр.

***

Протидія злочинам у сфері використання інформаційних технологій : інтегр. навч.-практ. посіб. - Харків : Право, 2019. - 186 с.

Розкрито питання кримінально-правової кваліфікації та кримінального забезпечення досудового розслідування «комп'ютерних» злочинів.

Шифр зберігання НБУВ: ВА830517

***

Федоров М.П. Проблеми протидії кіберзлочинності в Україні / Федоров М.П. // Вісник Львівського торговельно-економічного університету. Юридичні науки. - 2018. - Вип. 7. - С. 218- 231.

Досліджено державно-правовий механізм протидії кіберзлочинності в Україні. Проаналізовано основні положення чинних законодавчих та інших підзаконних актів, що регламентують відносини у сфері захисту прав та законних інтересів держави, юридичних та фізичних осіб від злочинних посягань у інформаційно-цифровій сфері. Обгунтовано пропозиції щодо вдосконалення чинного законодавства України у сфері кіберзахисту.

Шифр зберігання НБУВ: Ж69765/юрид.

***

Шевченко А. В. Управління функціональною стійкістю інформаційних систем на основі оптимізації видатків на захист / А. В. Шевченко // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. - 2018. - № 3. - С. 90-96.

Проаналізовано стан, напрями та основні причини зростання кількості інцидентів інформаційної безпеки. Побудовано моделі залежності збитків від інцидентів, як функцій від видатків на інформаційну безпеку. Знайдено загальну залежність оптимальних видатків на інформаційну безпеку залежно від рівня критичності інформаційних ресурсів організації.

Шифр зберігання НБУВ: Ж73897

***