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

№ 7 (липень)

Київ – 2020

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., 2020– №7 (липень) . – 102 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

«Сьогодні Кабмін прийняв “судьбоносне” рішення: звільнив Голову Держспецзв’язку Валентина Петрова і призначив Юрія Щиголя…

…я не у всьому згоден був з паном Валентином стосовно стратегій та візій розвитку кібербезпеки в країні, але завжди його поважав. Нормальна адекватна людина. З якою не соромно поздоровкатися та навіть десь якось попрацювати.

Звільнений пан Петров з посади Голови ДССЗЗІ був під приводом типово-дурним і абсолютно «лівим»: нібито він, Валентин Петров, не зберіг державні бази даних. Яких в країні понад 340 штук, за безпеку яких відповідають купа різних відомств, в яких працюють або криворуки, або відверті корупціонери, які самі продають ті бази направо і наліво, і вже років так з 20, коли пан Голова ще не був ніяким паном Головою, а просто студентом Валіком.

Тобто до Петрова чисто доколупалися «а чого без шапки». Мабуть, комусь захотілося поставити на його місце свою людинку для виконання специфічних завданнячок.

І хто ж обійняв цю посаду замість Петрова?

Такий собі Юрій Щиголь. Фігура настільки одіозна, що аж мурахи по шкірі.

Восени 2015 року був затриманий на гарячому при отриманні хабара.

Прізвище там не вказано, але якщо покопирсатися у документах та судових рішеннях, а особливо в архіві Управління внутрішньої безпеки СБУ – все знайдеться і підтвердиться. Взяли його під білі рученьки разом з його тодішнім начальником Вадимом Довженцем…

Та справа закінчилася тим, що заявника примусили забрати заяву і провадження прикрили. Хоча теперішній Голова Державної служби спеціального зв’язку та захисту інформації України півроку таки провів на нарах під слідством…

А тепер його самого призначають керувати тим самим відомством, яке (нібито) відповідальне за кібербезпеку країни. Тобто фактичної відповідальності там немає зовсім, зате грошей – просто море-окіян, ще на сто рендж-роверів вистачить, і собі, і дітям, і онукам. І босам, звісно.

Як це все назвати, куди ми котимося, у яку саме прірву і чим (та коли) усе це закінчиться – напишіть вже самі, у мене вже немає на це сили і літературних слів. Офігіватор зламався, проіржавів і розсипався. А для непарламентських обертів є кращі за мене фахівці…». ***(Константин Корсун. Корупціонери керують країною. Тепер офіційно. Щонайменше – кібербезпекою. Здобули // Антикор (https://antikor.com.ua/articles/393169-koruptsioneri_kerujutj_krajinoju._teper_ofitsijno._shchonajmenshe__kiberbezpekoju._zdobuli). 09.07.2020).***

****

«В Інституті законодавства Верховної Ради у дистанційному форматі відбулася науково-практична конференція з нагоди 24-ї річниці Конституції України на тему «Конституційно-правова модель «цифрової України».

До участі залучалися народні депутати України, працівники апарату Верховної Ради України, органів державної влади та місцевого самоврядування, вчені, представники вищих навчальних закладів та наукових установ, міжнародних та громадських організацій.

Для обговорення було запропоновано такі питання: конституційно-правова парадигма цифрової трансформації держави; конституційні засади інформаційного суспільства, конституційно-правове регулювання цифрових прав людини; конституційні засади кібернетичної безпеки України; цифрові трансформації в електронному урядуванні; проблеми впровадження цифрових технологій у демократичні процеси в Україні.

Відкриваючи дискусію, народний депутат України, академік НАН України Олександр Копиленко особливо відзначив, що побудова «цифрової України» стала важливою складовою передвиборчої програми Президента України Володимира Зеленського. Реалізація цього завдання залежить від побудови правової моделі електронної держави, від належного розуміння процесів цифровізації та їх впровадження у систему національного законодавства. На переконання парламентарія, законодавча діяльність Верховної Ради у цій та інших сферах має ґрунтуватися на результатах наукових досліджень. Саме тому заслуговує на підтримку започаткований в Інституті законодавства Верховної Ради України науковий проект «Цифрова держава: правові аспекти». Обмін ідеями та підходами є важливим етапом у підготовці комплексного дослідження з окреслених питань.

В. о. директора Інституту законодавства Верховної Ради України, член-кореспондент НАН України Євген Бершеда наголосив, що можливості інформаційно-комунікаційних технологій дадуть змогу активізувати демократичні засади розбудови суспільства відповідно до Конституції України. Водночас інформатизація може створювати певні ризики — порушення конституційних прав громадян, ухилення від сплати податків, незаконна торгівля, кіберзлочинність. У цих умовах держава має взяти на себе відповідальність щодо регулювання впровадження технологій в усі сфери людської діяльності. Про виділення інформаційного права в окрему галузь у наукових колах йдеться вже давно, а Інститут законодавства Верховної Ради України готовий стати майданчиком для напрацювань у цій сфері.

Завідувач відділу Інституту законодавства, професор Іван Мищак зупинився на питаннях розширення можливостей комунікації влади та суспільства й участі громадян у законотворенні, у тому числі шляхом втілення ініціатив, які висловлюються в електронних петиціях. За результатами аналізу електронних петицій доповідач виділив низку проблемних аспектів, зокрема низький рівень структуризації суспільства щодо захисту своїх прав та законних інтересів. Як наслідок, навіть належним чином сформульовані та слушні пропозиції не отримують достатньої підтримки. Значна частка електронних петицій не містить чітких запитів або пропозицій, має популістський або заполітизований характер, що апріорі не передбачає можливості для реалізації.

Завідувач відділу Інституту законодавства, кандидат юридичних наук Тетяна Гладкова зазначила, що формування електронної демократії — багатовекторних інтерактивних інструментів комунікації між громадянами та владою — стає

стратегічно важливим ціннісним виміром розбудови демократичної держави. З'являються безпрецедентні можливості для громадськості щодо розроблення та реалізації державної політики, а також для моніторингу діяльності влади й контролю за нею.

Підтримуючи висловлену думку, заступник завідувача відділу інституту, кандидат юридичних наук Ірина Костицька зауважила, що необхідність встановлення контролю з боку держави щодо використання сучасних інформаційно-комунікаційних технологій не має порушувати конституційні гарантії прав громадян стосовно участі у суспільному житті, зокрема при прийнятті відповідних рішень органами державної влади та місцевого самоврядування.

Завідувач сектору Інституту законодавства, доктор юридичних наук Ірина Куян зосередила увагу на конституційно-правовій парадигмі цифрової трансформації держави в контексті забезпечення прав людини. На її думку, електронне урядування робить державу більш ефективною у плані кількості та якості пропонованих громадянам публічних (адміністративних) послуг. Але цифровізація публічно-сервісної складової державної влади має й інший аспект.

У контексті віртуалізації відносин у системі «влада - громадянин» важливо, щоб вони не стали винятково відносинами громадянина з WWW-ботами, що вимагає додаткових гарантій захисту прав людини. Тож захист приватності, персональних даних у зв'язку із зростанням кількості державних реєстрів стає важливою проблемою сьогодення. Загалом охорона й захист таких баз даних має комплексний характер: захист персональних даних, захист даних реєстру від несанкціонованого копіювання, забезпечення нормального функціонування реєстру відповідно до його цільового призначення тощо.

Головний науковий співробітник Інституту законодавства, професор Борис Бабін відзначив, що стрімкий розвиток суспільних відносин зумовлює поступовий відхід від застарілих форм функціонування системи судочинства, які не узгоджуються з темпами технологічного розвитку. У зв'язку з цим відбувається перехід від паперового судочинства до електронного. З'являються нові поняття, категорії та інститути, що потребують правового врегулювання у вітчизняному законодавстві з урахуванням міжнародного досвіду.

Заступник завідувача відділу Інституту законодавства, кандидат юридичних наук Анна Кондратова поінформувала про перспективи імплементації в національне законодавство міжнародних стандартів кібербезпеки згідно з Декларацією цифрової взаємозалежності ООН «Цілі сталого розвитку 2030 та законодавство ЄС». Окрему увагу вона приділила положенням Угоди про Асоціацію між Україною та ЄС, що передбачає обов'язок України ратифікувати окремі директиви ЄС у сфері інформаційної безпеки.

Заступник завідувача відділу Інституту законодавства, кандидат юридичних наук Тарас Скомороха наголосив на важливості конституційного принципу таємного голосування, який закріплений міжнародними стандартами, зокрема статтею 25 Міжнародного пакту про громадянські і політичні права та статтею 3 Першого протоколу до Конвенції про захист прав людини і основоположних свобод. Кодекс належної практики у виборчих справах, ухвалений Венеціанською комісією, визначає його серед основоположних принципів європейського

виборчого доробку. Останнім часом в українському суспільстві обговорюється питання запровадження електронного голосування на виборах і референдумах, що передбачає і розв'язання проблем ідентифікації особи виборця. При підготовці концепції і законопроектів щодо електронного голосування має бути дотриманий загальновизнаний принцип виборчого права стосовно таємного голосування, зарубіжний досвід. Йдеться про правові, експлуатаційні та технічні стандарти електронного голосування, відповідно до яких воно має бути таким самим надійним і безпечним, як демократичні вибори та референдуми, що не передбачають використання електронних засобів.

Завідувач сектору Інституту законодавства, кандидат юридичних наук, старший науковий співробітник Юрій Данилюк зазначив, що розпорядженням Голови Верховної Ради України від 13 січня 2020 року № 2 створено Робочу групу з розробки проектів законів з питань народовладдя, метою діяльності якої є напрацювання, зокрема, законопроекту про народну законодавчу ініціативу. Враховуючи сучасні тенденції, у ньому має бути передбачено максимальне використання новітніх технологій у відповідних процедурах. На думку науковця, розроблення такого законопроекту має ґрунтуватися, зокрема й щодо застосування цифрових технологій, на вивченні кращого зарубіжного досвіду. При цьому заслуговує на увагу досвід Литовської Республіки. Відзначалося, що застосування новітніх цифрових технологій у демократичних процесах передбачає захист і персональних даних, і систем від кібер-втручань.

Завідувач сектору Інституту законодавства Тетяна Кравцова відзначила, що новітні технології (створення електронних реєстрів, електронних кабінетів підприємця та платника податків тощо) сприяють реалізації конституційних економічних прав громадян — права власності, на працю та підприємницьку діяльність, на інформацію в економічній сфері. На її думку, подальший розвиток блок-чейн технологій забезпечить поліпшення бізнес-клімату в країні, більшу відкритість держави та суспільства, зменшення рівня корупції та загальне покращення іміджу України у світі.

Головний консультант Інституту законодавства, кандидат юридичних наук Наталія Ніколаєнко наголосила, що в реаліях сьогодення такі види інноваційної діяльності, як інформатизація та цифровізація, стали узвичаєними атрибутами організації життя соціуму у світі в цілому та в Україні зокрема. Вони потребують напрацювання та впровадження новітнього підходу у питаннях забезпечення й захисту класичних прав і свобод людини, серед яких базовим є конституційне право людини на інформацію. Слід принципово переосмислити традиційні правові моделі гарантування та закріплення на нормативному рівні права людини на інформацію у світлі розвитку цифрових технологій, запровадивши нову парадигму розуміння його юридичної природи, сутності та змістовного наповнення, яка об'єднає філософські, соціологічні і теоретико-догматичні знання про право загалом та здатна запропонувати модерний погляд на розуміння цього фундаментального права людини». ***(Конституційно-правова модель «Цифрової України» // Голос України (http://www.golos.com.ua/article/332823).04.07.2020).***

***

«…2 липня, начальник Департаменту кіберполіції Олександр Гринчак та ректор Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» Михайло Згуровський підписали меморандум про співпрацю та партнерство.

За словами начальника Департаменту кіберполіції, сторони домовилися про проходження практики, стажування, підвищення фахового рівня студентів у підрозділах Департаменту кіберполіції, обміном науково-технічною інформацією та практичним досвідом.

«Кіберполіція приділяє особливу увагу професійній підготовці кадрів, для нас це питання дуже важливе. Тому меморандумом також передбачено направлення співробітників Департаменту кіберполіції для підвищення професійного рівня на відповідні курси в КПІ», - зазначив Олександр Гринчак.

У рамках співпраці також передбачено впровадження в освітній процес передового професійного досвіду та залучення фахівців кіберполіції до викладацької діяльності.

За словами ректора Київського політехнічного інституту, кіберполіція захищає країну від кібернетичних та інформаційних атак. Тому поєднання науки, практичної діяльності та підготовки кадрів у цій сфері є необхідним кроком…». ***(Кіберполіція співпрацюватиме з фахівцями Київського політехнічного інституту в сфері кібербезпеки // СтопКор (https://stopcor.org/zastupnyczya-dyrektora-stolychnogo-komunalnogo-pidpryyemstva-buduye-rozvazhalnyj-park-u-zapovidnij-zoni/). 02.07.2020).***

***

«За перший місяць дії програми пошуку вразливостей Prozorro Bug Bounty система закупівель Prozorro стала більш стійкою до кібератак, 6 баг хантерів знайшли 53 вразливості, які були усунені.

Про це повідомляє прес-служба Prozorro.

"Найбільшу кількість вразливостей знайшли на рівнях P3 і P4, тобто помірної та низької критичності.

Пошук вразливостей відбувався на тестових середовищах системи публічних закупівель Prozorro та трьох електронних майданчиків: Zakupki.Prom.UA, SmartTender, E-Tender", – йдеться у повідомленні.

"Щороку кількість кібератак на державні IT-системи зростає. Ми не можемо стояти осторонь цієї проблеми, і тому вирішили на постійній основі залучати баг хантерів. Ми вдячні за їхній час та зусилля. Лише за перший місяць їхньої роботи система Prozorro та електронні майданчики стали ще більш стійкими до кібератак", – зазначив генеральний директор ДП "Прозорро" Василь Задворний.

"Програма Prozorro Bug Bounty діє на постійній основі, тому запрошуємо баг хантерів протестувати систему публічних закупівель на стійкість до кібератак, а електронні майданчики, підключені до системи Prozorro, долучатися до програми", – додали у компанії…». ***(У Prozorro розповіли про перші результати роботи "білих" хакерів // Рубрика (https://rubryka.com/2020/07/08/u-prozorro-rozpovily-pro-pershi-rezultaty-roboty-bilyh-hakeriv/). 08.07.2020).***

***

«Влітку хакери не відпочивають. РНБО лише за останній місяць заявляла про низку загроз для українських користувачів. Це були не лише нові форми інтернет-атак, йшлося і про витік даних з реальними адресами багатьох сайтів. Усі загрози відслідковують у Національному координаційному центрі кібербезпеки. І наші журналісти поспілкувалися з тими фахівцями, які протидіють кіберзагрозам. Докладаніше – у сюжеті "5 каналу".

Вертолітний майданчик Віктора Януковича, місце зборів партії "Слуга народу". До певного часу конгресно-виставковий центр "Парковий" асоціювався винятково з політикою. Але віднедавна біля входу з'явився банер із чотирма літерами НКЦК. Тепер тут працюють ті, хто відповідає за кібербезпеку країни.

За складною довгою назвою ховається установа, створена ще в 2016 році. Утім до активної роботи стала лише цього літа.

"Центр фактично є основним робочим органом, який є в державі, що відповідає за кібербезпеку. Це і взаємодія між різними органами, і збір інформації, аналіз, уніфікація вимог до того, як ми будуємо в країні кібербезпеку", – каже Сергій Прокопенко, керівник управління забезпечення діяльності НКЦК РНБО України.

У перспективі планують, що тут зможуть взаємодіяти фахівці з кібербезпеки з різноманітних державних установ.

"Основне приміщення, де збираються фактично всі аналітики і представники суб'єктів кібербезпеки. Тут оформлені робочі місця для всіх. Нацбанк, прикордонники і так далі. Тут розміщаються наші робочі місця", – говорить Сергій Прокопенко, керівник управління забезпечення діяльності НКЦК РНБО України.

Поки що центр комплектується спеціалістами, яких тут має працювати з кілька десятків. У працівників, що вже потрапили до штату, роботи вистачає.

"Це аналітика, це аналіз кіберінцидентів, подій, про які нам звітують основні суб'єкти кібербезпеки. Основний фокус зараз – це залучення щодо звітування кіберінцидентів у приватному секторі", – розповідає Каріна Горбань, провідна інспекторка Національного координаційного центру кібербезпеки РНБО України.

У ситуаційній кімнаті одна зі стін складається з ряду моніторів. Серед низки карт з інформацією – розташування пристроїв, з яких атакували інфраструктурні об'єкти. Найбільше – на території окупованого сходу.

Тут накладаються не тільки ті пристрої, які використовувалися для стандартних атак, а й ті, що використовувалися для спроб проникнення на об'єкти критичної інфраструктури: перебір паролів, використання експлоітів", – розповідає Олександр Галущенко, провідний інспектор Національного координаційного центру кібербезпеки РНБО України.

Секретар РНБО каже – Центр комплектують найкращими фахівцями.

"Основне – це люди, які тут працюють. Ми покладаємося головно на них. Питання заробітної плати, ми вважаємо, що це другорядне питання. Питання якості цих людей – а вона в нас дуже і дуже висока", – говорить Олексій Данілов, секретар РНБО України.

За місяць активної роботи працівники центру вже кілька разів повідомляли про випадки кіберзагроз. Зокрема – про нові типи атак та масштабний витік

реальних IP-адрес інтернет-сайтів з усього світу». ***(Петро Троць, Анна Несевра. Витік даних: як Центр з кібербезпеки при РНБО протидіє загрозам // 5 канал (https://www.5.ua/suspilstvo/vytik-danykh-iak-tsentr-z-kiberbezpeky-pry-rnbo-protydiie-zahrozam-siuzhet-220675.html). 31.07.2020).***

***

«Проблеми з роботою сайтів президента та Служби безпеки України не пов'язані з недільним повідомленням про витік реальних IP-адрес, який виявили фахівці РНБО…

Кажуть, що більшість фігурантів зі списку уже встигли відповідно відреагувати на застереження і посилити безпеку сайтів. Але не всі.

"Навіть сьогодні, готуючись до інтерв'ю, ми перевіряли, і декілька ресурсів, там вебсайт міста-мільйонника і декілька банків та великі промислові групи, вони все ще не встигли оновити свої IP-адреси", – заявив Сергій Прокопенко, керівник управління забезпечення діяльності НКЦК…» ***(У координаційному центрі кібербезпеки прокоментували збої в роботі сайтів президента та СБУ // 5 канал (https://www.5.ua/suspilstvo/u-koordynatsiinomu-tsentri-kiberbezpeky-prokomentuvaly-zboi-v-roboti-saitiv-prezydenta-ta-sbu-220501.html). 29.07.2020).***

***

«Рада національної безпеки вдруге за місяць заявляє про кіберзагрози. Фахівці повідомили про витік інформації з реальними IP-адресами сайтів, які користувалися послугами компанії "Клаудфлер" чимало з яких належать урядового домену або мають стосунок до критичної інфраструктури. В компанії заявили, що витоку інформації не фіксували, але офіційного заперечення поки не було. Кореспондент "5 каналу" Петро Троць дізнавався, наскільки серйозною є така загроза.

Витік даних, який несе загрозу для безпеки державних та приватних ресурсів. У РНБО повідомили: їхні фахівці виявили у прихованій мережі Даркнет дані майже трьох мільйонів сайтів, які користуються сервісом "Клаудфлер" для захисту від кібератак. Ця компанія допомагає інтернет-сторінкам пережити напади з великої кількості комп'ютерів: коли на певну адресу одночасно заходять багато відвідувачів, це може заблокувати роботу сайту.

"Опублікований перелік містить реальні IP-адреси сайтів, що створює загрози спрямованих на них атак. Зокрема, серед таких адрес 45 записів із доменом "gov.ua" та більше 6,5 тисяч із доменом "ua", зокрема, ресурси, що належать об’єктам критичної інфраструктури", – йдеться у повідомленні РНБО.

Власників українських ресурсів, згаданих у списку, повідомили про небезпеку.

"Такі атаки робляться не тільки якимись там чорними хакерами, вони бувають спровоковані цілими державами в рамках геополітичних протистоянь. І те, що зараз відбувся витік такої інформації, ці адреси, що були поза "Клаудфлер", вони є вразливими точками, і зловмисники можуть бити по цих точках, по айпішниках", – говорить Єгор Аушев, співзасновник школи "білих хакерів" Cyber School.

У липні фахівці Національного координаційного центру кібербезпеки при РНБО уже повідомляли про нові типи кібератак. Цього разу загроза могла стосуватися роботи інтернет-сторінок, пов'язаних із діяльністю об'єктів критичної інфраструктури – аеропортів, атомних станцій, банків. А якої шкоди тут можна наробити добре пам'ятають ті, хто в 2017 мав проблеми із вірусом Petya, що заблокував роботу низки українських установ.

"Люди не розуміють загрози, вони з нею не стикалися, думають, що нікому не потрібні, через це загроза збільшується. Вона актуалізується і пересічному громадянину чи державному органу не вийде сказати, що нас це не стосується або я нікому не потрібен", – розповідає Павло Бєлоусов, експерт Школи цифрової безпеки DSS380.

Кіберзагроза стосується також і простих громадян. У травні поліція порушила кримінальне провадження через поширення персональної інформації українців через один із телеграм-каналів. Фахівці ж радять: ускладнити роботу зловмисникам можуть самі користувачі – за допомогою унікальних паролів та двофакторної перевірки.

"Вони вже не такі складні для втілення як були 5 років тому. Коли треба було комп'ютерним генієм, щоб дещо налаштувати, і люди звичайні не лізли в ці налаштування, зараз все просто: два кліки і все працює. Але до цього треба прийти, цим треба зайнятися, і не сьогодні, а ще вчора", – говорить Павло Бєлоусов, експерт Школи цифрової безпеки DSS380.

У питанні кібербезпеки ніхто не може гарантувати постійний спокій. І якщо сьогодні ви поза підозрілим списком, це не запорука, що завтра зранку ваша інтернет-сторінка чи особисті дані не будуть зламані зловмисниками. Але цю ситуацію можна порівняти зі здоров'ям ваших зубів: якщо ви стабільно відвідуєте стоматолога, тобто дбаєте про інформаційну безпеку, то і шанси мати серйозні проблеми у вас знижуються». ***(Петро Троць, Анна Несевра. Кібербезпека держави: чому це важливо та стосується навіть простих громадян // 5 канал (https://www.5.ua/suspilstvo/kiberbezpeka-derzhavy-chomu-tse-vazhlyvo-ta-stosuietsia-navit-prostykh-hromadian-siuzhet-220414.html). 28.07.2020).***

****

«Кіберфахівці Служби безпеки України перевірили ймовірність ризиків витоку даних із сервісу CloudFlare, яким користуються держслужбовці, і не виявило загрози для державних ресурсів і критичної інфраструктури.

«Виявлено, що IP-адреси вебресурсів, які з’явилися в інтернеті, є узагальненою базою загальнодоступних даних. Тобто оприлюднені доменні імена з IP-адресами доступні у мережі за допомогою стандартних запитів DNS. Загалом були опубліковані майже 2,6 млн таких записів», - йдеться у повідомленні.

Тож оприлюднення цих даних не несе додаткових ризиків для роботи вебресурсів, які обслуговує CloudFlare, зокрема, українських органів державної влади та об’єктів критичної інфраструктури, запевняють фахівці.

До перевірки залучалися Ситуаційний центр забезпечення кібербезпеки СБУ та Державний центр кіберзахисту Держспецзв’язку. Дані для проведення діагностики надала компанія «Cloudflare Inc».

Напередодні сайт президента України та форма подання електронних декларацій не працювали майже п’ять годин. У Держспецзв’язку причиною називали аварію та знеструмлення технічного майданчику на вулиці Юрія Іллєнка у Києві.

26 липня в Раді національної безпеки і оборони повідомили, що хакери викрали і виклали в даркнет (приховану від пересічних користувачів частину мережі - ред.) базу даних сервісу CloudFlare, яким користуються багато українських державних і приватних закладів.

У списку опинилися 45 сайтів, зареєстрованих на домені gov.ua, яким користуються українські органи влади. А також понад 6,5 тисяч сайтів на українському домені .ua. Зокрема сайти об'єктів критичної інфраструктури. Попри те, що більшість даних вже застаріли, є й актуальна інформація». ***(Ольга Чекис. У Службі безпеки підбили підсумки перевірки витоку даних з CloudFlare // Дзеркало тижня. Україна (https://zn.ua/ukr/UKRAINE/u-sluzhbi-bezpeki-pidbili-pidsumki-perevirki-vitoku-danikh-z-cloudflare.html). 28.07.2020).***

***

«…Не успели пользователи полноценно освоить новую редакцию Закона о государственных закупках, как команда Прозорро, во главе с генеральным директором предприятия Василием Задворным, внедряет новые современные изменения. Уже с 1 июня заработала новая прогрессивная инициатива Bug Bounty, которая никак не касается шоколадных жуков, а заключается в выявлении уязвимых мест системы перед кибернетической угрозой в современном мире.

Прозрачность использования государственных средств, удаление коррупции и безопасность всех участников процесса госзакупки - были, есть и всегда будут главными приоритетами неуемной команды Задворного. А потому, уже фильтрованный опыт таких мировых акул большого бизнеса, как Google, Амазон или Фейсбук, активно внедряется в нашей экономической среде с целью удаления заскорузлой ??плесени экономических преступлений.

Кибербезопасность госзакупок

В сентябре прошлого года был впервые проведен мониторинг системы ведущими хакерами. Тогда не было выявлено ни одного недостатка в функционале центральной базы данных и аукционном модуле, а только исправлены незначительные ошибки и улучшен интерфейс для более комфортной коммуникации. Ранее к подобной практике в Украине приходили только частные компании, тогда как большинство государственных учреждений, в основном, работали с программами, оставшимися с советских времен, которые по своей природе не устойчивы к требованиям современной кибернетической среды.

Еще с 2013 года во время массовых протестов было сообщено о первых атаках на частные предприятия и государственные учреждения, когда пострадала энергосистема, стали очевидными недостатки, недочеты и необходимость укрепления информационных баз и повышения безопасности киберпространства. 6 декабря 2016 хакерская атака на правительственные ресурсы, в том числе Госказначейство, а также 14 апреля и 27 июня 2017 были проведены масштабные атаки на украинские системы, когда хакеры получили доступ к 80% предприятий

путем автоматизированного обхода стандартных процедур аутентификации и удаленного доступа к технике. Тогда произошло вирусное поражение иностранных касательных систем, что привело к поражению порядка пятисот тысяч компьютеров по всему миру.

Bug bounty в мире

Из-за вынужденной готовности к кибернетическим атакам государственных предприятий по всему миру все больше внедряется принцип bug bounty. К примеру, Пентагон в 2016 году основал собственный регулярный мониторинг и выплатил «белым» хакерам более 330 тыс. долл. вознаграждения за идентификацию более трех сотен «дыр» в безопасности. Сингапур практикует такой поиск недостатков с 2018 года, а за 26 найденных багов прошлого года было выплачено вознаграждения 11 750 тыс. долл. Что касается украинской практики, то за июнь 2020 командой из семи БагХантеров было обнаружено и успешно устранено 53 угрозы различного уровня опасности. Наиболее продуктивным был поиск Вадима Шовкуна, БагХантера по прозвищу Jarvis, что за свою валидную работу получил ценные подарки. Поиски проходили в тестовой среде системы Прозорро, что никак не нарушало прав пользователей и основ конфиденциальности, а сама система работала в обычном режиме. Руководство решило оставить Bug Bounty в постоянном применении, а потому к регулярному участию приглашаются талантливые кибер-аудиторы.

Водяные знаки

С 19 июня 2020 при загрузке пакета документов в систему электронных закупок можно использовать функцию нанесения диагонального полупрозрачного «водяного» знака на сканкопию. Функция рекомендована к использованию для повышения уровня защиты персональных данных участников закупочного процесса. Информация такого маркера может включать код ЕГРПОУ поставщика и надпись «Для участия в закупках», что в свою очередь, сделает невозможным использование копий документов вне системы в мошеннических целях.

Такие водяные знаки - это обыденная практика аналогичных европейских систем закупок и, отныне, в ответ на запрос пользователей системы по защите открытых данных, они включены и в ЕСЗ Прозорро и сопутствующих площадок. Важно, что Закон о публичных закупках никоим образом не исключает использования подобных пометок на страницах пакета тендерной документации, а потому администрация ресурса призывает включить в постоянную практику такое нововведение.

Так что новая редакция Закона никоим образом не регулирует сбор, защиту и обработку персональных данных участников, доступ к которым имеют все любопытные пользователи сети, сторона поставщика всегда может обоснованно обжаловать требование заказчика предоставить сканкопию паспорта и идентификационного кода, к примеру. Заказчик обязан предоставить обоснованный ответ по существу такого запроса личных данных и преувеличенной необходимости таких документов в составе тендерного пакета. Согласно Закону Украины «О защите персональных данных» в плоскости электронных коммерческих отношений, предприниматели, предоставляющие сканкопию личных документов путем их публикации, автоматически дают согласие на их

использование. Исходя из этого, предприниматели должны своевременно и внимательно анализировать условия и состав тендерной документации и реагировать на превышение регламента со стороны заказчика.

Аналитика со стороны площадок

В этом году также включены дополнительные механизмы аналитики и прослеживания коррупционных схем в отношениях между участниками закупок в системах некоторых площадок. Возможность спрогнозировать не только возможных конкурентов будущего аукциона и их ценовое предложение, но и шаги понижения во время раундов аукциона, отныне позволит более продуктивно планировать работу и лучше готовить ценовое предложение. Изучая репутацию фирмы-поставщика или заказчика и причинно-следственные связи уже устоявшихся отношений, можно глубже понять рынок, эффективнее оценивать свои возможности и тактически маневрировать, как активный пользователь системы.

Поэтому отныне, госзакупки онлайн будут проходить в условиях повышенной безопасности, которая регулярно совершенствуется не только на уровне компьютерных систем и технологий, но и благодаря законодательным инициативам». ***(Повышение безопасности государственных закупок // Мост (http://most.ks.ua/news/type/1/url/povyshenie_bezopasnosti_gosudarstvennyh_zakupok). 29.07.2020).***

***

Національна система кібербезпеки

«Учасники засідання Національного координаційного центру кібербезпеки обговорили питання щодо організації захисту систем Центральної виборчої комісії під час місцевих виборів у 2020 році. Про це УНН повідомляє з посиланням на прессслужбу Ради національної безпеки і оборони України.

Так, учасники засідання обговорили питання щодо організації захисту систем ЦВК під час місцевих виборів у 2020 році, а також перспективи та потенційні ризики впровадження у виборчий процес онлайн-голосування та інших електронних сервісів.

Як зазначив заступник секретаря Ради нацбезпеки і оборони Сергій Демедюк, РНБО "готова протистояти загрозам з кіберпростору, які очікувано надходитимуть від нашого північного сусіда".

"Це не лише кібератаки, а й спроби маніпулювання суспільною свідомістю, поширення фейків з метою загострення суспільно-політичної ситуації всередині країни та дискредитації України на міжнародній арені", - зазначив Демедюк.

За результатами обговорення учасники засідання Національного координаційного центру кібербезпеки запропонували заходи щодо недопущення зриву виборчого процесу внаслідок кібератак…

Окрім того, під час обговорення питання щодо онлайн-голосування наголошувалося, що впровадження такої ініціативи потребує ґрунтовного підходу.

"У цьому контексті зацікавленим міністерствам і відомствам запропоновано розробити попереднє технічне завдання, модель потенційних загроз та техніко-економічне обґрунтування впровадження онлайн-голосування у виборчий процес в Україні для подальшого всебічного вивчення та обговорення", - зазначено в повідомленні…». ***(Анна Мурашко. У РНБО обговорили питання кіберзахисту систем Центрвиборчкому під час місцевих виборів // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1879685-u-rnbo-obgovorili-pitannya-kiberzakhistu-sistem-tsentrviborchkomu-pid-chas-mistsevikh-viboriv). 09.07.2020).***

***

«Ситуаційний центр забезпечення кібербезпеки Служби безпеки України оновив національну платформу Malware Information Sharing Platform "Ukrainian Advantage" (MISP-UA) для ефективної протидії кіберзагрозам і обміну даними…

У відомстві розповіли, що MISP-UA – це платформа, яка в режимі реального часу забезпечує обмін даними про кіберризики, атаки та інциденти на об'єктах критичної інфраструктури, установах і підприємствах, державних електронних інформаційних ресурсах.

"За своїм функціональним наповненням платформа дозволяє зміцнити стан кібербезпеки різних секторів державного управління та економіки України. З її допомогою відбувається державно-приватна взаємодія для спільного захисту інформаційного та кіберпростору держави загалом. На платформі MISP-UA вже зареєстровані понад 300 користувачів, серед яких державні і приватні підприємства", – інформують в СБУ.

Користувачі MISP-UA надають відомості про ознаки можливого ураження технологічних і комунікаційних систем, що надає можливість кіберфахівцям СБУ передбачати шляхи атак, потенційні загрози та інструменти нейтралізації.

Додамо, що СБУ розпочала впровадження MISP-UA у 2018 році, використовуючи досвід країн ЄС та НАТО. Наразі СБУ використовує цю платформу як один із елементів забезпечення національної безпеки у кіберпросторі…». ***(Тарас Джміль. СБУ оновила платформу MISP-UA для ефективної протидії кіберзагрозам // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1880887-sbu-onovila-platformu-misp-ua-dlya-efektivnoyi-protidiyi-kiberzagrozam). 16.07.2020).***

***

«В пресс-службе Национальной полиции Украины обнародовали любопытную информацию. Теперь украинцы знают, сколько денег ежемесячно получают люди, которые оберегают порядок и покой целого государства.

…оклад киберполицейских в Украине весьма внушительный – около 45 тысяч гривен.

Об этом рассказал заместитель министра внутренних дел Украины Антон Геращенко. Причина столь высоких окладов специалистов киберполиции проста –

нехватка квалифицированных кадров, которые бы согласились работать за 15 тысяч гривен.

«У нас постоянно идет процесс реформирования киберполиции. Несколько лет назад мы повысили зарплату и сделали так, что у нас там зарплата одна из самых высоких в полиции - 40-45 тыс. грн - именно потому, что киберспециалисты по кибербезопасности... нам сложно было вообще найти людей на зарплату 15 тыс. грн. Потому что системные администраторы в обычных небольших компаниях зарабатывают минимум 20-25 тыс. грн, а серьезные специалисты получают 2-3 тыс. долларов США, наверное, даже больше. Поэтому сейчас у нас в киберполиции специальное подразделение, где получают большие относительно других зарплаты, именно для того, чтобы защищать интересы граждан и государства в киберпространстве», - рассказал заместитель Арсена Авакова». ***(Зарплаты полицейских: в МВД озвучили оклады правоохранителей в Украине // Антикор (https://antikor.com.ua/articles/396964-zarplaty_politsejskih_v_mvd_ozvuchili_oklady_pravoohranitelej_v_ukraine). 22.07.2020).***

***

Кібервійна проти України

«3 липня, "Укроборонпром" відбив чергову атаку хакерів.

Про це повідомила пресслужба концерну…

Хакери намагалися заразити систему "Укроборонпрому" вірусом типу "троян" через електронні скриньки працівників.

Зазначається, що електронна адреса, з якої відбувалася атака, розміщена на серверах одного американського телекомунікаційного провайдера.

Всю інформацію щодо даного інциденту вже передали до Національного Координаційного центру кібербезпеки РНБОУ.» ***(Хакери атакували "Укроборонпром" // СтопКор (https://stopcor.org/hakery-atakuvaly-ukroboronprom/). 04.07.2020).***

***

«Система кіберзахисту державних інформресурсів та об'єктів критичної інфраструктури за тиждень (1-7 липня) зафіксувала на 18% більше підозрілих інцидентів, ніж минулого тижня.

Про це повідомляє прес-служба Держспецзв'язку.

"Переважна більшість зафіксованих підозрілих подій стосується спроб мережевого сканування (52%), застосування нестандартних протоколів (24%), виявлення мережевого ШПЗ (11%), веб-атак (8%) та спроб отримання прав адміністратора (4%).

Система захищеного доступу державних органів до мережі Інтернет заблокувала 1888 різних видів атак. Переважна більшість (80%) - це мережеві атаки прикладного рівня. Також заблоковано 9 DDoS-атак, переважна більшість - на веб-ресурси Офісу президента", - йдеться у повідомленні.

Зазначається, що урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA у цей період зареєструвала та опрацювала 19 514 кіберінцидентів.

"Переважна більшість опрацьованих інцидентів належить доменній зоні UACOM (близько 99%). Основна кількість інцидентів стосується розповсюдження ШПЗ (73% від загальної кількості) та фішингу (26%)", - додали у відомстві». ***(Зросла кількість кібератак на державні сайти – Держспецзв'язку // Економічна правда (https://www.epravda.com.ua/news/2020/07/8/662725/). 08.07.2020).***

***

«Если Россия решится на наступление, Украине следует готовиться к мощным кибератакам, которые приведут к полной блокаде Азовского моря.

Об этом в интервью изданию Тиждень заявил бывший командующий ВС США в Европе, эксперт Центра анализа европейской политики (CEPA) Бен Ходжес.

Эксперт заявил, что ожидает полной блокады Азовского моря.

Он также предполагает возможность многочисленных общественных протестов в Украине, организованных российскими спецслужбами в различных социальных группах.

«Их цель - максимально отвлечь внимание, поэтому это будут разные города во всех областях Украины, не только на юге. Они создадут Киеву немало проблем», - считает Ходжес.

По его мнению, для России осенью будут все благоприятные предпосылки - политические, экономические и военные - для наступления на Украину.

«Если Кремль сочтет, что со стороны Запада реакция будет минимальной, то это создает определенные риски. Такие расчеты могут повлечь атаку определенного типа», - отметил эксперт, добавив, что все упомянутые предпосылки для наступления «не обязательно означают, что атака будет, однако предпосылки есть», - добавил Ходжес» ***(Экс-командующий ВС США допустил усиление наступления России на Украину // ООО «ИЗДАТЕЛЬСКИЙ ДОМ «МЕДИА-ДК» (https://nv.ua/world/geopolitics/rossiya-mozhet-atakovat-ukrainu-ekspert-ssha-poslednie-novosti-50099272.html). 10.07.2020).***

***

«Протягом першого півріччя 2020 року Служба безпеки України нейтралізувала понад 300 кібератак на об'єкти критичної інфраструктури, викрила майже 20 хакерських угруповань, значну частину яких контролювали з РФ. Про це повідомляє пресцентр СБУ…

В відомстві зазначили, що заблокували механізм фінансування незаконних збройних формувань "ЛНР" через системи електронних платежів.

"Група громадян на окупованій частині Луганщини під кураторством так званого "МДБ ЛНР" і ФСБ РФ створила псевдофінансову установу "Перший комерційний центр". Ця структура забезпечувала проведення в ОРЛО операцій з поповнення та зняття коштів з банківських платіжних карт України та РФ,

валютно-обмінних операцій, грошових переказів через міжнародні платіжні системи, обіг електронних коштів у заборонених Україною ресурсах", – йдеться в повідомленні.

Також була заблокована діяльність організованої групи мешканців Києва та Житомира, які за допомогою програмного забезпечення здійснювали підміну номерів і видавали міжнародний трафік псевдооператорів “Фенікс” і “Лугаком” з окупованої території Донбасу і Російської Федерації за місцеві телефонні розмови українських абонентів.

"СБУ запобігла розсилці листів на тему COVID-19 начебто від імені Центру громадського здоров’я МОЗ України. Завдяки спільній спецоперації СБУ і Державної податкової служби заблоковано податкову схему, котра щомісяця завдавала збитки державі на 2 мільярди гривень. Загалом за цей період викрито та припинено 219 фактів протиправного використання електронних платіжних систем і систем розрахунків, “криптовалют” і “криптовалютних технологій”, – поінформували в СБУ.

Для захисту кібербезпеки України було розпочато 295 кримінальних проваджень, у тому числі 82 – за несанкціоноване втручання у роботу комп’ютерів, 17 осіб притягнуто до кримінальної відповідальності.

Окрім того, за півроку СБУ припинила діяльність 2,7 тис. спільнот у соцмережах, 375 вебресурсів, 431 інтернет-агітатора і 10 ботоферм, які поширювали фейки та деструктивну інформацію.

“Велику роль для захисту національного інформпростору відіграло продовження санкцій проти російських соцмереж “ВКонтакте” і “Одноклассники”, а також продуктів “Яндекс”, “Mail.ru”, “Доктор Веб”, “Касперский”, “1С”, “Парус”, – зазначили в СБУ…». ***(Наталія Затуливітер. За півроку на об’єкти критичної інфраструктури України здійснено понад 300 кібератак // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1881682-sbu-vidzvituvala-pro-neytralizatsiyu-300-kiberatak-na-obyekti-kritichnoyi-infrastrukturi). 21.07.2020).***

****

«Працівники Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України зафіксували перші спроби нового типу DDOS-атак на найбільш ранньому їх етапі. Про це повідомив заступник Секретаря Ради національної безпеки і оборони України Сергій Демедюк, передає УНН з посиланням на повідомлення пресслужби РНБО.

“Вже тоді ми зрозуміли серйозність загрози — всього за кілька днів хакери успішно атакували десятки провайдерів по всьому світу, включно з Україною. Аналіз зібраних нами даних показав, що більшість інцидентів на перших етапах були лише підготовкою до великої скоординованої атаки, направленої на блокування доступу до сегментів інтернету на глобальному рівні. Тому ми одразу попередили українських провайдерів, відповідних суб’єктів кібербезпеки та зарубіжних партнерів про загрозу та надали рекомендації щодо реагування на подібні атаки”, — зазначив Демедюк.

З його слів, згодом цей прогноз НКЦК підтвердився — у червні 2020 року одна з DDOS атак нового типу стала найбільшою в історії, досягнувши значення майже 780 Гбіт/сек. Саме вона стала причиною короткострокового відключення 15% всього світового інтернету та ряду магістральних провайдерів.

Повідомляється, що джерелом атак цього типу є мережа скомпрометованих пристроїв "розумного дому" (IoT). При цьому у більшості випадків доступ до цих пристроїв здійснювався шляхом зламу стандартних паролів. Зловмисники отримували доступ до віддаленого керування, після чого атакували.

"Особливістю цих атак є спрямованість безпосередньо на інфраструктуру провайдерів. Відтак, у разі її вдалої реалізації функціонування всього національного сегменту мережі інтернет є під загрозою", — зазначив заступник Секретаря РНБО, додавши, що лише в Україні нині виявлено майже 10 тисяч пристроїв, які потенційно можуть використовуватися для здійснення такої DDoS-атаки.

За словами Демедюка, "такої кількості цілком достатньо, щоб відключити від мережі на час атаки майже всю країну"…». ***(Саша Картер. Майже вся країна може залишитись без інтернету: у РНБО заявили про новий тип DDOS-атак // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1881150-mayzhe-vsya-krayina-mozhe-zalishitis-bez-internetu-u-rnbo-zayavili-pro-noviy-tip-ddos-atak). 17.07.2020).***

****

«Спеціалізований структурний підрозділ з реагування на кіберінциденти Державної служби спеціального зв'язку та захисту інформації України CERT-UA в період з 22 до 28 липня заблокував 49 125 кібератак на державні органи влади.

Це у 60 разів більше, ніжу попередный тиждень.

3% атак – це кіберзлам паролю шляхом перебору всіх можливих варіантів ключа;

3% зламів за технікою, яку використовують спамери для злому електронної пошти;

93% – мережеві атаки прикладного типу.

Також служба Держспецзв'язку заблокувала 3 DDoS-атаки (хакерська атака на обчислювальну систему з метою довести її до відмови) на сайт Офісу президента України…» **(Майже 50 тис. за тиждень: хакери збільшили атаки на сайти держорганів // ФАКТИ. ICTV (https://fakty.com.ua/ua/proisshestvija/20200728-majzhe-50-tys-za-tyzhden-hakery-zbilshyly-ataky-na-sajty-derzhorganiv/). 28.07.2020).**

****

«В середине июля Совет национальной безопасности и обороны Украины выступил с сообщением о новом типе DDOS-атак на телекоммуникационные сети. Их особенностью стало то, что под удар попали десятки провайдеров по всему миру, в том числе, украинские.

Но главный месседж СНБО заключался в следующем – успешные атаки могут обрушить работу национального сегмента интернета. Другими словами, отключить Украину от сети…

По словам заместителя секретаря СНБО Сергея Демедюка, в июне 2020 одна из DDOS-атак нового типа стала крупнейшей в истории, достигнув значения почти 780 Гбит/с. Как результат – краткосрочное отключение 15% всего мирового интернета и ряда магистральных провайдеров.

Зарубежные медиа писали об июньской атаке на один из европейских банков, имя которого не раскрывали из соображений конфиденциальности. Ее мощность на пике составила 809 млн пакетов в секунду, что ставит ее в один ряд с крупнейшими бот-атаками в истории.

Поразила и невероятная скорость, так как трафик от нормального показателя до более 400 Гбит/с вырос всего за несколько секунд, а пиковых значений достиг спустя еще две минуты. Специалисты компании Akamai полагают, что за ней стоит новый ботнет (зараженная сеть). В процесс было вовлечено большое количество IP-адресов, не замеченных ранее в подобных операциях. Но, скорее всего, эта атака не связана с выявленной в СНБО.

DDOS-атаки («отказ в обслуживании») направлены на блокирование доступа к веб-сайту или приложению для конечных пользователей. Обычно хакеры генерируют большое количество пакетов или запросов для перегрузки работы целевой системы, используя множество взломанных источников, которые могут быть объединены в ботнет.

В целом для Украины атаки типа DDOS не являются чем-то новым. По данным Центра кибербезопасности при Нацкомиссии по регулированию в сфере связи и информатизации (НКРСИ), во II квартале 2020 года они стали причиной 46% киберинцидентов в государственном секторе. В негосударственном секторе – всего 1%.

В комментарии РБК-Украина Сергей Демедюк рассказал, что отличие нового типа атаки заключалось в использовании не мощностей зараженных устройств, а стримингового видеопотока для нагрузки на IP-адрес.

«Такой тип атаки был использован в украинской сети впервые. Атака имела целью блокирование работы провайдеров», – подчеркнул он.

Атаки были многократными и продолжались от 40 минут до 1,5 часа несколько дней подряд. В общей сложности, под удар попала десятая часть всей сети в Украине

Источники атак – наши роутеры и веб-камеры

Источником атак нового типа стала сеть скомпрометированных устройств «умного дома» (IoT). В большинстве случаев доступ к ним получали путем взлома стандартных паролей, после чего хакеры брали на себя удаленное управление для дальнейших действий.

Центр кибербезопасности НКРСИ уточняет, что очевидными мишенями в этих случаях являются роутеры и веб-камеры. Наиболее уязвимое место – использование пароля по умолчанию или вообще его отсутствие.

Злоумышленники взламывают их при помощи программного обеспечения, которое перебирает самые распространенные варианты. Как правило, этот процесс занимает мало времени.

Конкретно в этой атаке использовались взломанные веб-камеры. «Их дефолтные настройки (например, login: admin, password: admin) были одной из основных причин получения несанкционированного доступа к удаленному управлению. Еще интересно, что атака осуществлялась не на конкретный адрес, а целыми диапазонами, что, собственно, выглядело как массивный перебор информации или поиск конкретной цели», – сказали изданию в СНБО.

Что касается уязвимости провайдеров к DDOS-атакам с применением устройств «умного дома», то известный под ником «Шон Таунсенд» сооснователь «Украинского киберальянса» Андрей Баранович в комментарии изданию заявил, что в этом нет ничего принципиально нового.

«Любой оператор с квалифицированными инженерами на самом деле знает, как бороться с DDOS-атаками. Это неприятно, но не смертельно. То, что Национальный координационный центр кибербезопасности при СНБО заметил эту атаку и предлагает свою помощь, неплохо. Но я полагаю, что это отнюдь не самая насущная проблема украинской информационной безопасности», – подчеркнул он.

По оценкам СНБО, на сегодня в стране насчитывается почти 10 тысяч устройств, через которые могут быть осуществлены атаки на инфраструктуру провайдеров. Заместитель секретаря Сергей Демедюк заявлял, что этого вполне достаточно, чтобы на время парализовать украинский сегмент интернета.

В свою очередь, Баранович считает преувеличенной опасность подобных атак, даже с мощностью под 800 Гбит/с.

«Это довольно много и может на какое-то время «уложить» провайдера, и даже провайдера провайдера, но Украину как государство «отключить от Интернета» не получится. Много независимых операторов, и не те объемы», – добавил эксперт.

Тем не менее при первых подозрениях того, что кто-то получил доступ к роутеру и другим устройствам «умного дома», украинцам рекомендуют сбросить их к заводским настройкам, сменить пароли на более стойкие, по возможности включить двухфакторную аутентификацию и регулярно обновлять ПО.

Что говорят провайдеры

Из крупнейших украинских провайдеров за последние несколько недель о массовой DDOS-атаке заявила только компания «Воля». В течение трех дней фиксировались атаки на абонентские подсистемы, которые также перешли на инфраструктуру провайдера в Харькове. В результате более 100 тысяч абонентов испытали проблемы с доступом к интернету, IPTV и телевидению.

Атаки проводились с десятков тысяч разных IP адресов по всему миру – США, Малайзия, Тайвань, Вьетнам и т. д. Всю информацию провайдер передал киберполиции, но компания не уверена, что атаки не повторятся снова, хотя и делает все, чтобы этого избежать.

Другие крупные провайдеры, такие как «Киевстар» и «Укртелеком», не фиксировали DDOS-атаку на свои сети в июне. Однако подчеркивают, что кибератаки периодически имеют место.

Директор департамента корпоративных коммуникаций «Укртелекома» Михаил Шуранов в комментарии РБК-Украина рассказал, что почти ежедневно службы провайдера отслеживают и блокируют потенциальные угрозы.

«Например, в прошлом месяце была заблокирована очередная атака злоумышленников с помощью почтовых вложений с внешних адресов – очень популярная форма кибератаки», – отметил Шуранов.

По словам директора по кибербезопасности «Киевстара» Юрия Прокопенко, атаки происходят время от времени, но негативного влияния на системы провайдера не было. В том числе благодаря постоянному улучшению системы противодействия.

«Благодаря этому, например, «Киевстар» был одной из немногих крупных компаний, которые не пострадали от вируса Petya в 2017 году. Хотя наша инфраструктура также подвергалась активному нападению», – добавил он.

Провайдеры подчеркивают, что постоянно сотрудничают с киберполицией и Ситуационным центром обеспечения кибербезопасности СБУ. Они делятся опытом и наработками в этой сфере для защиты информационных систем в Украине.

Кроме того, на сегодня Украина синхронизирует законодательство с европейскими нормами по кибербезопасности. Согласно им, провайдеры обязаны предоставить клиентам достаточный уровень защиты. И если ресурсы крупных операторов не вызывают сомнений, то возможности более мелких локальных провайдеров, которые обслуживают более 50% рынка, остаются под вопросом.

Настораживающая тенденция

По последним данным, СБУ за первое полугодие 2020 в общей сложности нейтрализовала более 300 инцидентов, целью которых были объекты критической инфраструктуры. К ним причастны почти 20 хакерских группировок, и значительную часть их контролировали из Российской Федерации (фашистское государство, страна-агрессор — согласно Закону Украины от 20.02.18). Чего нельзя пока сказать о месте, откуда совершалась DDOS-атака нового типа.

«Сейчас мы работаем над тем, чтобы зафиксировать все цифровые следы этой атаки и собрать информацию в различных частях мира, где были зафиксированы такие атаки. Имея достаточное количество необходимой информации, мы сможем сделать выводы о месте ее осуществления. У нас уже есть определенные наработки, однако разглашать их рано – пока дело находится в компетенции одного из правоохранительных органов киберзащиты», – рассказал замсекретаря СНБО Сергей Демедюк.

Он добавил, что уже началась работа над созданием системы обнаружения таких атак на ранних стадиях.

При этом за весь 2019 год специалисты СБУ отразили более 480 кибератак, и это дает основание полагать, что Украина сохраняет свою привлекательность для хакеров. А это, в свою очередь, означает, что в дальнейшем перед нами будут возникать все новые угрозы в сети.

В подтверждение этого на прошлой неделе стало известно о DDOS-атаках на сайт Офиса президента Украины, а также сообщалось, что число подозрительных инцидентов в сети выросло на 22% по сравнению с предыдущим периодом.

Кроме того, Национальный координационный центр кибербезопасности выявил масштабную утечку из сервиса Cloudflare, который специализируется на защите от кибератак. В так называемом DarkNet опубликовали данные 3 млн сайтов с реальными IP-адресами, в том числе ресурсов с доменами gov.ua и ua.

Часть этих данных принадлежит объектам критической инфраструктуры Украины. Поэтому владельцам скомпрометированных ресурсов порекомендовали сменить IP-адреса размещения сайтов и усилить мониторинг кибератак». ***(СНБО: на Украину совершена // Антикор (https://antikor.com.ua/articles/397565-snbo_na_ukrainu_sovershena_krupnejshaja_v_istorii_ddos-ataka). 28.07.2020).***

***

Боротьба з кіберзлочинністю в Україні

«Сотрудники киберполициях в Черновицкой области совместно со следователями Шевченковского отделения полиции и Черновицкой местной прокуратурой разоблачили преступные действия 17-летнего черновчанина.

Правоохранители выяснили, что подросток осуществлял несанкционированное вмешательство в автоматизированные системы международных компаний, занимающихся электронной коммерцией. Используя вредоносное ПО, парень завладел конфиденциальной информацией интернет-пользователей, которую потом продавал на хакерском форуме и через один из мессенджеров.

Сотрудники полиции провели дома у нарушителя обыск и изъяли компьютерную технику, смартфоны и накопители информации. Результаты судебной компьютерно-технической экспертизы подтвердили факты несанкционированного вмешательства в автоматизированные системы. Также было обнаружено более 300 тыс. текстовых файлов, содержащих персональные данные нескольких миллионов интернет-пользователей со всего мира.

Следователи Шевченковского отделения полиции сообщили злоумышленнику о подозрении в совершении преступлений, предусмотренных частями 1 и 2 статьи 361-2 (несанкционированный сбыт или распространение информации с ограниченным доступом, которая сохраняется в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или на носителях такой информации) Уголовного кодекса Украины. За такие противоправные действия подозреваемому грозит до пяти лет лишения свободы.

Следователи направили обвинительный акт в Шевченковский районный суд города Черновцы». ***(Киберполиция выявила подростка, сбывавшего персональные данные граждан разных стран // Компьютерное Обозрение (https://ko.com.ua/kiberpoliciya_zaderzhala_podrostka_sbyvavshego_personalnye_dannye_grazhdan_raznyh_stran_133612). 03.07.2020).***

***

«…Співробітники Департаменту кіберполіції Нацполіції спільно із Головним слідчим управлінням НПУ, Службою безпеки України, під процесуальним керівництвом Офісу Генерального прокурора України, викрили чоловіка у несанкціонованому втручанні в роботу мереж електрозв'язку національних операторів телекомунікаційних послуг.

Кіберполіція встановила, що до таких дій причетний мешканець Житомирщини, 1985 року народження. Фігурант розмістив велику кількість точок із спеціалізованим телекомунікаційним обладнанням, в якому розміщувались sim-картки українських операторів мобільного зв'язку.

Обладнання було налаштоване на прийом вхідних викликів з-за кордону із подальшим перенаправленням під виглядом псевдонаціональних в обхід Міжнародного центру комутації. Таким чином міжнародні виклики тарифікувались як національні. Для таких дій фігурант використовував понад півтори тисячі стартових пакетів найбільших українських операторів мобільного зв'язку.

За попередніми даними сума збитків складає понад півмільйона гривень.

Правоохоронці провели обшуки за місцем мешкання фігуранта, в транспортних засобах та гаражних приміщеннях. За результатами вилучено комп'ютерну техніку, стартові пакети, мобільні телефони, спеціалізоване телекомунікаційне обладнання, яке приймало міжнародні виклики та підмінювало на псевдонаціональні. Попереднім оглядом техніки встановлено доступ до особистого кабінету, через який фігурант керував налаштуваннями телефонії.

За даним фактом відкрито кримінальне провадження за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України. Фігуранту загрожує до 6 років ув'язнення.

Крім цього, встановлено інші злочинні осередки які здійснюють підміну міжнародного трафіку в різних регіонах країни. Слідчі дії тривають». ***(Кіберполіція викрила мешканця Житомирщини у несанкціонованому втручанні в роботу операторів мобільного зв'язку // Кіберполіція Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-meshkanczya-zhytomyrshhyny-u-nesankczionovanomu-vtruchanni-v-robotu-operatoriv-mobilnogo-zvyazku-5625/). 06.07.2020).***

****

«…Під час проведення заходів співробітники кіберполіції Київщини спільно зі слідчими Печерського управління поліції Києва, під процесуальним керівництвом столичної прокуратури, викрили чоловіка, який у месенджері збував інформацію із обмеженим доступом.

Правопорушник розміщував на спеціалізованих хакерських форумах «прайс», що налічував понад 50 актуальних баз даних. Продаж таких баз фігурант здійснював за допомогою боту у месенджері. Гроші отримував на криптовалютні гаманці, оформлені на підставних осіб.

Крім цього, встановлено, що інформацію зловмисник також здобував шляхом підбору та зламу паролів до електронних поштових скриньок, месенджерів, облікових записів у соцмережах.

Правоохоронці провели обшуки за місцем мешкання фігуранта. За результатами вилучено комп’ютерну техніку і телекомунікаційне обладнання.

За даним фактом відкрито кримінальне провадження за ч. 2 ст. 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, створеної та захищеної відповідно до чинного законодавства) Кримінального кодексу України. Санкція статті передбачає позбавлення волі на строк від двох до п'яти років. Слідчі дії тривають». ***(Кіберполіція викрила чоловіка у продажі інформації з обмеженим доступом // Кіберполіція Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-cholovika-u-prodazhi-informacziyi-z-obmezhenym-dostupom-2285/). 08.07.2020).***

****

«Хакери за допомогою шкідливого програмного забезпечення несанкціоновано втручалися у роботу банків і привласнили кілька мільйонів гривень. Після оголошення підозри у серії кіберзлочинів – організатор переховувався від правоохоронців, тоді його оголосили у розшук.

Співробітники Департаменту кіберполіції спільно з Головним слідчим управлінням Нацполіції, під процесуальним керівництвом Офісу Генерального прокурора, затримали 30-річного чоловіка, який ґрунтовно підозрюється в організації низки кіберзлочинів.

Кіберполіція встановила, що фігурант створив шкідливе програмне забезпечення. Цей вірус злочинна група розсилала на електронні поштові скриньки для отримання доступу до «клієнт-банку». В подальшому вони відслідковували надходження значних грошових сум на банківські рахунки підприємств. Після цього гроші перерахували на відкриті рахунки спільників.

Упродовж досудового розслідування правоохоронці провели 35 обшуків на території Закарпатської, Київської, Івано-Франківської, Одеської областей та міста Києва. За результатами вилучено речові докази.

Усім фігурантам оголосили про підозру у вчиненні правопорушень, передбачених ч. 3 ст. 28 (Вчинення злочину групою осіб, групою осіб за попередньою змовою, організованою групою або злочинною організацією), ч. 2 ст. 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку), ч. 2 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут), ч. 5 ст. 185 (Крадіжка) та ч. 3 ст. 209 (Легалізація (відмивання) доходів, одержаних злочинним шляхом) Кримінального кодексу України.

Організатор переховувався від правоохоронних органів, уникаючи відповідальність, і так його було оголошено у державний розшук.

Затримання підозрюваного відбулося на підставі ухвали суду на Івано-Франківщині. Йому обрали запобіжний захід у вигляді тримання під вартою, з альтернативою внесення застави у 2,5 мільйони гривень…» ***(Кіберполіція затримала організатора хакерського угруповання, який перебував у державному***

розшуку // Кіберполіція Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-zatrymala-organizatora-xakerskogo-ugrupovannya-yakyj-perebuvav-u-derzhavnomu-rozshuku-6677/). 10.07.2020).

***

«…Співробітники кіберполіції спільно зі слідчими Луцького відділу поліції, під процесуальним керівництвом прокуратури Волинської області, припинили злочину діяльність місцевого жителя. Чоловік здійснив втручання в роботу комп'ютерів на території Австрії.

Кіберполіція встановила, що зловмисник створив шкідливе програмне забезпечення, яке шифрувало дані користувачів. Після інфікування комп'ютерної техніки користувачам надходило повідомлення про необхідність сплати «викупу». За відновлення даних зловмисник вимагав від 600 до тисячі доларів США. Потерпілі мали переказувати гроші на криптовалютний гаманець фігуранта. Жертвами хакера стали як державні установи, так і звичайні користувачі.

Правоохоронці провели обшук за місцем проживання чоловіка. За результатами обшуку вилучено комп'ютерну техніку, мобільні телефони, жорсткі диски. Вилучені речові докази направлено на проведення відповідних експертиз. Наразі встановлюється повне коло потерпілих осіб.

За даним фактом відкрито кримінальне провадження за ч. 1 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) Кримінального кодексу України. Максимальне покарання, передбачене статтею, – позбавлення волі на строк до двох років. Слідчі дії тривають». ***(Кіберполіція встановила хакера, який шифрував дані іноземних користувачів // Департамент кіберполіції Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vstanovila-xakera-yakij-shifruvav-dani-inozemnix-koristuvachiv/). 20.07.2020).***

***

«Житель Вінниці придбав та модифікував шкідливе програмне забезпечення для незаконного отримання логінів та паролів громадян для авторизації на різних Інтернет-ресурсах. У подальшому він збував такі данні на спеціалізованих форумах.

Співробітники кіберполіції спільно зі слідчими Вінниччини, під процесуальним керівництвом місцевої прокуратури, розпочали досудове розслідування за фактом несанкціонованого втручання в роботу комп'ютерних мереж.

Кіберполіція встановила, що 28-річний житель Вінниці з використанням модифікованого вірусу викрадав персональні дані з веббраузерів жертв, зокрема – логіни і паролі для авторизації.

У подальшому він перевіряв їх на валідність, а потім на тематичних форумах розміщував оголошення про продаж. Вартість однієї такої бази коливалася від 400 до 1900 гривень. Отримані гроші зловмисник перераховував на криптовалютні гаманці.

Також встановлено, що чоловік займався перепродажем даних, отриманих від інших збувачів.

Правоохоронці провели обшук за місцем проживання фігуранта.

За результатами обшуку вилучено ноутбук, жорсткий диск, флеш-накопичувач, мобільні телефони, WiFi-роутер та чорнові записи. Речові докази направлено на проведення комп'ютерно-технічної експертизи.

За даним фактом відкрито кримінальне провадження за ч. 2 ст. 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України. Зловмиснику загрожує позбавлення волі на строк від трьох до шести років.

Вирішується питання щодо оголошення підозри фігуранту. Триває слідство». ***(Кіберполіція встановила зловмисника, який продавав конфіденційні данні громадян // Департамент кіберполіції Національної поліції України (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vstanovila-zlovmisnika-yakij-prodavav-konfidenczijni-danni-gromadyan/). 14.07.2020).***

***

Коронавірус COVID-19 та питання кібербезпеки

«Стивен Берк, генеральный директор и основатель Cyber Risk Aware, рассказывает о том, как организации могут проводить свои собственные «проверки здоровья», обучать своих сотрудников в режиме реального времени и применять лучшие методы кибербезопасности после пандемии COVID-19

В недавнем отчете Европола подчеркивается, что «киберпреступники были одними из самых опытных в использовании пандемии COVID-19 для различных мошенничеств и атак, которые они совершают». В том же отчете предсказывается, что в целях использования нынешнего кризиса начинаются кампании по борьбе с фишингом и вымогательством, и ожидается, что их масштабы и масштабы будут продолжать расти.

Во многом это увеличение связано с важным переходом на удаленную работу: большая часть офисного бизнеса в мире в настоящее время управляется людьми из дома. Многие организации уже создали основы удаленной инфраструктуры, но ни одна из них не смогла подготовиться к огромным изменениям. Дело в том, что смена места работы работников, перенося их в виртуальный мир, фактически вывела их на передний край быть целью киберпреступности.

Просто с любым большим изменением придут трещины, и киберпреступник готов и отточен, как противный виртуальный спортсмен, чтобы вскочить на каждую уязвимость. Многие доклады предполагают, что киберпреступность увеличилась на 80%. Через несколько часов после появления первых признаков того, что Covid19 может иметь серьезные последствия, киберпреступник использовал свой любимый и самый эффективный метод - фишинговую атаку.

Правильно расставьте приоритеты

Атаки идут мощно и быстро. В марте сообщалось, что один из крупнейших центров тестирования COVID-19, Университетская клиника Брно в Чешской Республике, был вынужден закрыться в результате атаки с использованием вымогателей. В апреле Google сообщил, что заблокировал более 126 миллионов фишинговых атак. Организации должны привести свои приоритеты в порядок - им нужно перестать беспокоиться об унифицированных фонах Zoom или викторинах в офисе, чтобы поддерживать боевой дух: им нужно начать вооружать своих людей обучением осведомленности о кибербезопасности, чтобы они не стали жертвой следующей атаки. Жесткий факт заключается в том, что более 90% нарушений данных происходит из-за человеческой ошибки, и эта ошибка является ошибкой организации, которая не обучает своих сотрудников.

Риски кибербезопасности человека должны быть в верхней части списка приоритетов. Организациям необходимо прекратить использовать учебные бюджеты по повышению осведомленности о безопасности за учебными сессиями Zoom и направить их на обучение осведомленности о кибер-рисках. В идеале такое обучение должно проводиться в режиме реального времени: запланированные учебные занятия не настолько эффективны, как обучение на рабочем месте.

Самый простой способ сделать это - проверить работоспособность вашей организации: попробуйте бесплатную пробную версию фишинга в своей сети. Это можно сделать очень легко: бесплатные фишинговые тесты COVID-19 от Cyber Risk Aware помогают предприятиям защитить свою сеть от повышенных киберугроз в период пандемии коронавируса. Сейчас, как никогда ранее, организация должна запускать симулированные фишинговые тесты, чтобы повысить осведомленность о том, как будет выглядеть настоящая атака, и информировать персонал о том, что делать в случае получения подозрительного электронного письма.

Лучшая практика кибербезопасности

Организации также должны использовать свои лучшие практики, чтобы гарантировать, что их удаленная рабочая сила помогает защитить свой бизнес, данные и репутацию. Вот несколько ключевых указателей:

● Будьте бдительны к фишинговым мошенникам COVID-19 - запустите бесплатную фишинговую кампанию для оценки рисков, информирования и обучения своих сотрудников.

● Используйте безопасные системы, предоставляемые компанией - убедитесь, что облачные системы исправлены и не используют личные учетные записи.

● Будьте готовы и вооружите свой персонал. Предоставляйте зашифрованные современные устройства с исправленными приложениями и VPN для доступа к внутренним системам вашей компании.

● Внедрить протоколы и процессы на случай кибератаки, чтобы минимизировать воздействие. Cyber Risk Aware предлагает PhishHuk, бесплатный плагин для Outlook, который сотрудники могут использовать на своей ленте электронной почты, чтобы сообщать о фишинговых письмах в IT Security.

● иметь четкие линии связи. Избегайте социальных сетей и WhatsApp при раскрытии конфиденциальных данных. Убедитесь, что ваша компания настроена на безопасные лучшие каналы связи.

Классические ошибки

● Не выбирайте легкий путь. Shadow IT - термин, используемый для загрузки неутвержденного программного обеспечения, представляет собой возрастающую угрозу кибербезопасности. Это может включать Macro для Excel или программное обеспечение для захвата скриншотов, например.

● Не подключайтесь к общедоступному WIFI. Вместо этого используйте предоставляемые компанией VPN или мобильные данные при доступе к конфиденциальным данным.

● Не разрешайте использование личных устройств, поскольку они часто небезопасны и уязвимы для кибератак.

● Защита паролем и шифрование являются ключевыми. На устройствах, файлах и данных.

● Не забудьте сделать резервную копию данных централизованно. Будь то проблема системного сбоя или риска

В результате атаки вымогателей убедитесь, что все резервные копии выполняются ежедневно в центральном месте и что ИТ-специалисты регулярно проверяют восстановление.

Придерживаться правила ABC

Всегда будьте наставником: в то время, когда предприятия и частные лица более уязвимы, чтобы смягчить распространение этой пандемии, организации должны объединиться для общего блага. Поддержание бизнеса в рабочем состоянии и защита рабочей силы от эскалации угроз должны стать глобальным соображением и объединенным сотрудничеством.

Это время неопределенности привело к беспрецедентному поведению. Поскольку большая часть рабочей силы в настоящее время поощряется к работе из дома, риск бизнеса, испытывающего кибер-инцидент, значительно увеличивается. Поэтому крайне важно, чтобы персонал и компании были подготовлены и защищены от этих самых настоящих киберугроз как можно лучше. Лучший способ вооружить своих людей знаниями о существующих киберугрозах и защитить ваш бизнес в эти неопределенные времена - это тренинг по повышению осведомленности о кибербезопасности с помощью симуляции кибератак в реальном времени. А благодаря бесплатной симуляции фишинга в вашем распоряжении не может быть никакого оправдания тому, что вы не сделали свою собственную проверку состояния кибербезопасности». ***(Remote working and the rise of cybercriminals // Open Access Government (https://www.openaccessgovernment.org/remote-working-and-the-rise-of-cybercriminals/90051/). 08.07.2020).***

***

«Уповноважений Верховної Ради з прав людини Людмила Денісова звернулась до Кабінету міністрів із проханням виділити 14,5 млн грн з Фонду боротьби з COVID-19.

Про це йдеться у листі Уповноваженої до КМУ, який оприлюднила експертна організація StateWatch.

10 млн грн із них планується витратити на ремонт адміністративного приміщення, 3,5 млн грн – на створення веб-сайту, а також 1 млн грн - на відрядження в рамках національного превентивного механізму.

Прохання щодо виділення 10 млн грн на ремонт будівлі Секретаріату Уповноваженого з прав людини обгрунтовується скороченням передбачених на 2020 рік видатків на здійснення капітального ремонту. Зі слів Денісової, безповоротне вилучення зазначених видатків та перенесення строків проведення ремонту призведе до наступних наслідків:

– втрата результатів від проведених капітальних робіт фасаду у 2019 році на суму 22 млн грн;

– навантаження в майбутньому на державний бюджет у 2021 році у зв'язку із необхідністю компенсувати кошти передані в Фонд боротьби з COVID-19 протягом цього року;

– збільшення договірної ціни в майбутньому.

Денісова також пропонує виділити 3,5 млн грн на створення офіційного веб-сайту Уповноваженого ВРУ з прав людини. Це прохання вона аргументує тим, що діючий сайт було розроблено на платформі, що сьогодні є "морально застарілою" та не підлягає оновленню, а тому має певні технічні обмеження. Уповноважена апелює до того, що сайт має слабку систему захисту, через що постійно зазнає кібератак та блокується.

Запитувані кошти на створення сайту Уповноважена пропонує розподілити наступним чином:

– створення технічного завдання – 525 тис грн;

– розробка прототипу веб-порталу – 700 тис грн;

– розробка, тестування та введення в експлуатацію – 2,275 млн грн.

Крім того, Уповноважена просить здійснити видатки у розмірі 1 млн грн на реалізацію функції національного превентивного механізму з огляду на те, що Секретаріат Уповноваженого з прав людини є єдиним в Україні органом, що реалізує зазначену функцію, завдяки якій Україна виконує міжнародні зобов'язання. Реалізація функції НПМ передбачає систематичне відвідування місць несвободи, зокрема в період карантину, однак найближчим часом може бути призупинена через відсутність коштів у зв'язку зі скороченням видатків на відрядження.

Аргументуючи зазначені прохання, Уповноважена апелює до того, що можливість передбачити видатки у розмірі 14,5 млн грн за рахунок інших джерел, зокрема за іншими бюджетними програмами Секретаріату, відсутня, оскільки вони забезпечують фінансування інших необхідних поточних витрат Уповноваженого Верховної Ради України з прав людини». ***(Омбудсмен просить виділити 14,5 мільйона з Covid-фонду. 3,5 мільйона підуть на новий сайт // Економічна правда (https://www.epravda.com.ua/news/2020/07/6/662584/). 06.07.2020).***

***

«Компания Eset сообщает о росте количества попыток атак методом подбора пароля (brute-force attacks) с начала глобальной пандемии. Кризис COVID-19 в корне изменил характер повседневной работы, вынудив работников выполнять значительную часть своих обязанностей с помощью инструментов удаленного доступа.

До перехода на удаленный режим работы большинство людей работали в офисе и использовали инфраструктуру, которую контролировал ИТ-отдел. Однако, сегодня огромная часть «офисной» работы выполняется с помощью домашних устройств. Работники получают доступ к конфиденциальным корпоративным данным через протокол удаленного рабочего стола (RDP). Несмотря на рост важности RDP и других служб удаленного доступа, организации часто пренебрегают их настройками и защитой. Кроме этого, сотрудники используют пароли, которые легко угадать, поэтому без дополнительной двухфакторной аутентификации или защиты киберпреступники могут легко получить доступ к системам организации.

В частности, по данным телеметрии Eset, большинство заблокированных IP, которые использовались для атак в период с января по май были зафиксированы в США, Китае, России, Германии и Франции. В то время как объектами атак чаще всего становились IP-адреса в России, Германии, Японии, Бразилии и Венгрии.

В течение нескольких последних лет RDP стал популярным вектором атак, особенно среди групп, которые занимаются распространением программ-вымогателей. Эти киберпреступники часто пытаются проникнуть в плохо защищенную сеть, получить права администратора, отключить или удалить решения безопасности, а затем запустить программу-вымогатель для шифрования важных данных компании.

Также злоумышленники могут использовать плохо защищенный RDP для установки вредоносного ПО для майнинга криптовалют или создания бэкдора, который может быть использован в случае выявления и прекращения несанкционированного доступа к RDP.

Во избежание растущих рисков, связанных с увеличением использования RDP, исследователи Eset разработали новый уровень обнаружения, который является частью модуля «Eset Защита от сетевых атак» и предназначен для блокировки входящих атак методом подбора пароля с внешних IP-адресов. Он охватывает RDP, а также протокол SMB.

Однако, помимо использования современных решений по кибербезопасности, важно правильно настроить RDP:

Отключить RDP, к которому можно получить доступ через Интернет. Если это невозможно, специалисты Eset рекомендуют минимизировать количество пользователей, которые могут подключаться к серверам организации через Интернет.

Установить уникальные и сложные пароли для всех учетных записей, в которые можно войти через RDP.

Использовать дополнительный уровень аутентификации (MFA/2FA).

Установить шлюз виртуальной частной сети (VPN) для всех соединений RDP вне локальной сети.

Отключить на брандмауэре сети внешние соединения с локальными машинами на порту 3389 (TCP/UDP) или любом другом порту RDP.

Установить защиту паролем для решения по безопасности, чтобы злоумышленники не смогли получить к нему доступ и удалить.

Изолировать любые незащищенные или устаревшие компьютеры, к которым можно получить доступ из Интернета с помощью RDP». ***(Киберпреступники активизировали атаки через протокол RDP // Компьютерное Обозрение (https://ko.com.ua/kiberprestupniki_aktivizirovali_ataki_cherez_protokol_rdp_133579). 01.07.2020).***

***

«Велика Британія, Сполучені Штати і Канада звинуватили Росію в четвер у спробі вкрасти інформацію у дослідників, що працюють над створенням вакцини від коронавірусної хвороби COVID-19…

Так, три країни стверджують, що хакерське угруповання APT29, також відома як Cozy Bear і є частиною російської розвідувальної служби, атакує академічні та фармацевтичні дослідні установи, що займаються розробкою вакцин від коронавірусу.

Повідомляється, що заяву, узгоджена з владою США і Канади, зробив Британський національний центр кібербезпеки.

"Абсолютно неприпустимо, що російські спецслужби націлені на тих, хто бореться з пандемією коронавірусу. У той час як інші своєю безрозсудною поведінкою переслідують егоїстичні інтереси, Велика Британія і її союзники продовжують важку роботу з пошуку вакцини і захисту здоров'я людей в усьому світі", - заявив сьогодні міністр закордонних справ Сполученого Королівства Домінік Рааб.

Відзначається, що кібератаки розглядаються співробітниками розвідки як спроба вкрасти інтелектуальну власність, а не підірвати дослідження. Кампанія по "шкідливій діяльності" триває і включає в себе "атаки переважно проти урядових, дипломатичних, аналітичних, медичних та енергетичних цілей", йдеться в заяві національного центру кібербезпеки.

Було неясно, чи була якась інформація фактично вкрадена, але центр повідомив, що конфіденційна інформація людей, як вважається, не була скомпрометована.

Відповідно до повідомлення агентства, 16-сторінковий документ, оприлюднений у четвер Великою Британією, США та Канадою, звинувачує Cozy Bear у використанні призначених для користувача шкідливих програм, націлених на низку організацій по всьому світу. Шкідливі програми WellMess і WellMail, які раніше не асоціювалися з хакерською групою…». ***(Саша Картер. Велика Британія, США і Канада звинуватили Росію в спробі вкрасти дані про вакцину від COVID-19 // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1880951-velika-britaniya-ssha-i-kanada-zvinuvatili-rosiyu-v-sprobi-vkrasti-dani-pro-vaktsinu-vid-covid-19). 16.07.2020).***

***

«Германия не имеет данных по заявлениям со стороны Британии о якобы хакерских атаках, связанных с созданием вакцин от коронавируса, заявил представитель МИД ФРГ Кристофер Бургер.

«Мы очень внимательно следим за ситуацией, состоим в контакте и обмене с британскими ведомствами. На сегодняшний момент я не могу сообщить вам о собственных сведениях о том, что касается сообщения британской стороны о своем расследовании по данной теме», – цитирует Бургера РИА «Новости».

Представитель МВД страны Стив Альтер сообщил, что в Германии подобных кибератак в отношении важных центров разработки вакцины от COVID-19 зафиксировано не было.

Ранее национальный центр кибербезопасности Британии заявил, что хакеры, якобы связанные с Россией, пытались украсть данные о разрабатываемых в мире вакцинах от коронавируса.

Пресс-секретарь российского лидера Дмитрий Песков заявил, что Россия не имеет отношения к взломам фармкомпаний и исследовательских центров Британии, занимающихся разработкой вакцины от коронавируса.

Глава РФПИ Кирилл Дмитриев заявил, что у России нет необходимости «красть» разработки вакцин в Великобритании, так как фармкомпания AstraZeneca уже передала все наработки России и договорилась с «Р-Фарм» о производстве лекарства». ***(Алексей Дегтярев. Германия не зафиксировала кибератак на центры по созданию вакцин от коронавируса // Деловая газета «Взгляд» (https://vz.ru/news/2020/7/17/1050465.html). 17.07.2020).***

***

«Прес-секретар президента Росії Дмитро Пєсков заявив, що Росія не має ніякого відношення до спроб зламати фармкомпанії і дослідницькі центри у Великій Британії…

“Ми не володіємо інформацією, хто міг зламувати фармкомпанії і дослідницькі центри у Великій Британії. Можемо сказати одне — Росія не має до цих спроб ніякого відношення. Ми не прийнятний подібні звинувачення, рівно, як і чергові голослівні звинувачення у втручанні в вибори 2019 року”, — сказав Дмитро Пєсков…». ***(Дар'я Панченко. У Кремлі заявили, що РФ не має ніякого відношення до спроб вкрасти дані про вакцину від COVID-19 // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1880983-u-kremli-zayavili-scho-rf-ne-maye-niyakogo-vidnoshennya-do-sprob-vkrasti-dani-pro-vaktsinu-vid-covid-19). 16.07.2020).***

***

«Карантин не только изменил формат работы многих компаний, коммуникаций, формата ведения бизнеса.

Вы в новой реальности и с новыми угрозами

Карантин ускорил процесс технологизации бизнеса, а вместе с ним и увеличил риски киберугроз:

1. После COVID-19 ФБР США сообщило о росте на 300% числа зарегистрированных киберпреступлений.

2. К 2021 году на кибербезопасность в мире будет потрачено около $6 трлн.

3. По оценкам Университета Мэриленд, каждые 39 секунд в мире происходят кибератаки.

4. 43% кибератак нацелены на малый бизнес. 64% компаний сталкивались с атаками через Интернет. 62% испытали фишинговые и социальные атаки. 59% компаний сталкивались с вредоносным кодом и ботнетами, а 51% – с отказами в обслуживании.

5. Более 93% организаций здравоохранения столкнулись с утечкой данных за последние три года.

6. 95% нарушений кибербезопасности происходят из-за человеческой ошибки.

7. Мозги – лучшая защита от фишинговых атак.

8. К 2025 году количество подключенных IoT-устройств достигнет 75 миллиардов.

9. К 2021 году незаполненные вакансии кибербезопасности превысят 4 миллиона человек.

10. Инженеры по кибербезопасности являются одними из самых высокооплачиваемых должностей, начинающихся в среднем по $140 тыс. в год.

11. Более 77% организаций не имеют плана реагирования на инциденты кибербезопасности.

12. Большинству компаний требуется почти 6 месяцев для обнаружения утечки данных.

13. Для публичных компаний, кибератаки приводят в среднем к падению стоимости акций на 7%.

Вы думаете, что вы, ваши гаджеты и компьютеры защищены? Вы думаете, серверы вашей компании недоступны для киберпреступников? Вы считаете, что объекты критической инфраструктуры страны, ваших городов в безопасности?» ***(Анатолий Амелин. Приветствую в новой реальности: как карантин повлиял на киберугрозы? // Телеканал новостей «24» (https://24tv.ua/ru/privetstvuju-novoj-realnosti-karantin-povlijal-kiberugrozy-novosti-mira_n1383938). 24.07.2020).***

****

Міжнародне співробітництво у галузі кібербезпеки

«На розвиток кібербезпеки Україна отримає 38 млн доларів від США, відповідний проект вже зареєстровано в Кабміні. Про це написав у Telegram-каналі віце-прем'єр-міністр - міністр цифрової трансформації Михайло Федоров, передає УНН.

“США підтримає розвиток кібербезпеки в Україні. Бюджет міжнародної технічної допомоги становить 38 млн доларів. Більше року активної роботи — десятки складних переговорів, узгодження спільної концепції та планів — і цими днями нарешті проект остаточно зареєстровано в КМУ”, — написав Федоров.

Також він зазначив, що Мінцифри буде публічно звітувати про хід та витрати проекту.

“Такий великий проект є черговим сигналом довіри до наших результатів та планів. З усіх кіберпитань ми плануємо активно працювати з бізнесом та залучати найкращу міжнародну й українську експертизу”, — написав Федоров…». ***(Антоніна Карташева. США виділяють Україні 38 млн дол. на кібербезпеку // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1881940-ssha-vidilyayut-ukrayini-38-mln-dol-na-kiberbezpeku). 22.07.2020).***

***

«Секретар Ради національної безпеки і оборони України Олексій Данілов провів зустріч з Надзвичайним і Повноважним Послом Держави Ізраїль в Україні Джоелем Ліоном. Сторони обговорили поглиблення співпраці між безпековими відомствами двох держав у галузі кібербезпеки.

Про це повідомляє пресслужба РНБО…

Також сторони також обмінялися думками щодо розвитку безпекової ситуації у глобальному та регіональному вимірах, зокрема стосовно поширення у світі коронавірусної хвороби та ефективності заходів з протидії пандемії.

Своєю чергою, Ліон запевнив, що Ізраїль і надалі підтримуватиме Україну, і висловив впевненість в успішності практичного співробітництва між нашими державами». ***(Україна та Ізраїль поглиблять співпрацю у галузі кібербезпеки // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (https://day.kyiv.ua/uk/news/310720-ukrayina-ta-izrayil-poglyblyat-spivpracyu-u-galuzi-kiberbezpeky). 31.07.2020).***

***

Світові тенденції в галузі кібербезпеки

«Ozon запустил собственную bug bounty-программу (пользователи получают вознаграждение за найденные баги) на платформе HackerOne — площадке для компаний и исследователей безопасности по всему миру. Об этом говорится в сообщении компании.

Программа стала первой среди российских e-commerce компаний, на первом этапе Ozon планирует инвестировать в работу с хакерским сообществом более 3 млн рублей.

Вознаграждение за каждый найденный баг зависит от степени его влияния на работу сервиса, потенциального урона, который уязвимость может нанести, качества отчета и других факторов.

За найденный XSS (cross-site scripting) Ozon может заплатить порядка 17 тысяч рублей, а за более серьезные — инъекции, удаленное выполнение кода (RCE) — до 120 тысяч рублей.

«Запуск программы позволяет компаниям получить круглосуточный мониторинг безопасности, но не отменяет работу команды IT-лаборатории Ozon по обеспечению безопасности сервисов Ozon, а дополняет ее — сейчас у компании

есть необходимые ресурсы не только для развития собственных служб безопасности, но и для работы с хакерским сообществом», — говорится в сообщении.

Bug bounty-программы есть у мировых IT-компаний, в том числе Amazon, Google, Facebook, однако в России эта практика пока не получила широкого распространения, отмечают в Ozon. Собственные программы есть всего у нескольких компаний, включая «Яндекс», Mail.ru Group, Qiwi». ***(Анастасия Марьина. Ozon инвестирует более 3 млн рублей в работу с хакерами // Rusbase (https://rb.ru/news/ozon-bug-bounty/). 06.07.2020).***

***

«Британское бюро оценки составило список из 5 превентивных мер для организаций, чтобы избежать утечки данных и кибератак

С заголовками в СМИ, в которых основное внимание уделяется таким именам, как British Airways, Travelex и Uber, может возникнуть соблазн предположить, что киберпреступники нацелены только на крупные компании с глубокими карманами. Но правда в том, что шесть из десяти МСП страдают от кибератак, а четверть благотворительных организаций Великобритании подверглась атаке в 2019 году. Итак, что вы можете сделать, чтобы защитить свою организацию от такого рода преступлений?

Повышение квалификации

Многие организации не поддерживают своих сотрудников соответствующей подготовкой. Фактически, только 29% сотрудников прошли обучение по кибербезопасности в 2019 году по сравнению с невероятными 81% директоров, попечителей или высшего руководства.

Тем не менее, существует вероятность того, что многие из ваших сотрудников, если не все, могут получить доступ к конфиденциальной информации, хранящейся в вашей компании, что делает более важным, чем когда-либо, их надлежащую поддержку.

Обеспечение того, чтобы ваши сотрудники прошли соответствующий уровень подготовки, поможет им знать, что им нужно делать для обеспечения безопасности вашей информации.

Конечно, память ни у кого не идеальна, и ваша команда забудет обо всем. Регулярное обновление тренировок может помочь снизить этот риск.

Политики безопасности данных

Всем, как персоналу, так и руководству, легко рассматривать политику как пометку. Но правда в том, что политика безопасности данных намного больше, чем это.

Надежда для любой организации заключается в том, что вашей команде редко понадобится пройти обучение по безопасности данных. Это означает, что они не всегда будут помнить, что им нужно делать, когда возникает вопрос или инцидент.

Комплексная политика безопасности данных - это ресурс, к которому ваши сотрудники могут обратиться, если они не уверены, что делать дальше. Независимо от того, получили ли они запрос на доступ к данным от клиента, или они не могут

вспомнить, что им нужно делать, когда рабочее устройство выводят из офиса, политика безопасности данных либо предоставит им ответ, либо выложит процедуры, которой они должны следовать, или посоветовать им, как обострить инцидент.

Политика безопасности данных представляет собой способ поддержки вашей команды, когда они не уверены, что делать или к кому обратиться. Это также снижает риск того, что этот член команды угадывает, что ему следует делать, и потенциально может поставить под угрозу вашу конфиденциальную информацию.

Многофакторная аутентификация

Ваша команда, вероятно, уже знает, что надежный пароль является необходимостью. Но паролей не всегда достаточно, чтобы гарантировать безопасность. Вот почему вы должны по возможности использовать многофакторную аутентификацию (MFA) или двухфакторную аутентификацию (2FA).

MFA / 2FA описывает функции безопасности, когда для входа в систему или приложение требуется ввод пароля, но затем пользователю отправляется код подтверждения на мобильное устройство или по электронной почте; пользователь не может войти без ввода этого кода подтверждения.

MFA / 2FA означает, что даже если кто-то украдет пароль, ему также потребуется получить доступ к другому паролю или устройству для доступа к вашей конфиденциальной информации.

Регулярно проходить тестирование на проникновение

Тест на проникновение описывает оценку вашей кибербезопасности, когда ваша внутренняя ИТ-команда или независимые подрядчики будут имитировать кибератаку на вашу организацию, чтобы выявить любые недостатки вашей безопасности.

Эти симуляции включают попытки проникнуть в сеть вашей организации путем поиска и использования уязвимостей в вашей безопасности. Они также могут включать тесты социальной инженерии, которые пытаются обмануть вашу команду, предоставив доступ кому-то, кого они считают авторитетом.

Регулярно проверяя свою безопасность с помощью таких реальных тестов, вы можете обнаружить и усилить любые слабые места, прежде чем злоумышленник сможет их найти и использовать.

Использовать подход, основанный на оценке риска

Ключом к вашей кибербезопасности является риск: когда вы знаете, где находится риск, вы можете предпринять действия, чтобы уменьшить или избежать его.

Проведение тщательной оценки рисков может помочь вам определить, где именно ваша организация нуждается в улучшении, где вам необходимо инвестировать в дальнейшие меры безопасности или даже кому нужно дополнительное обучение.

Системы управления информационной безопасностью (СУИБ) также могут помочь вам формализовать ваши процедуры и процессы таким образом, чтобы помочь вам выявить любые пробелы и тем самым помочь вам определить любые риски для вашей безопасности данных.

Оставаться бдительным

Киберпреступники не остаются на месте; они постоянно ищут новые способы доступа к конфиденциальной информации. Таким образом, вы должны постоянно искать новые способы защиты своей организации. Вот почему ключ к большинству этих профилактических мер заключается в том, что они требуют постоянного пересмотра и обновления. Регулярно проверяя безопасность данных, вы можете быть на шаг впереди». ***(5 ways to prevent data breaches and cyber attacks // Open Access Government (https://www.openaccessgovernment.org/5-ways-to-prevent-data-breaches-and-cyber-attacks/91049/). 22.07.2020).***

***

«Світові витрати на кібербезпеку у 2020 році у порівнянні з 2019 роком зростуть на 5,6% - до 43,1 мільярда доларів з 40,8 мільярда доларів. Про це йдеться в дослідженні міжнародної аналітичної компанії Canalys, опублікованому на її веб-сайті. Зокрема, витрати на інтернет-безпеку і захист електронної пошти зростуть на 10,3%; наукові дослідження у сфері кіберзахисту – на 10%; захист кінцевих пристроїв - на 8,5%; захист баз даних – на 8,5%. Згідно з найпесимістичнішим сценарієм Canalys, витрати на киберзахист у світі зростуть на 2,5% - до 41,9 мільярда доларів. У компанії підкреслили, що ключовим ризиком для стабільного зростання витрат є негативний економічний вплив пандемії коронавірусу на фінансові можливості компаній інвестувати у свою кібербезпеку». ***(Світові витрати на кібербезпеку цього року перевищать $43 мільярди // информационный портал "ua.today" (http://ua.today/news/economy/svitovi_vitrati_na_kiberbezpeku_cogo_roku_perevishat_43_milyardi). 23.07.2020).***

***

Сполучені Штати Америки

«Новый правовой акт Lawful Access to Encrypted Data Act (LAEDA) в случае его принятия подвергнет риску не только жителей США, но всех, кто используют американские продукты и услуги со сквозным шифрованием

The Internet Society выражает свою озабоченность законопроектом о легальном доступе к зашифрованным данным LAEDA. Организация отправила соответствующее письмо в Сенат, которое было подписано более чем 75 экспертами по глобальной кибербезопасности, организациями гражданского общества, компаниями и торговыми ассоциациями. По мнению авторов письма, законопроект «слишком технически несовершенен, чтобы быть эффективным, и заставит компании сделать свою продукцию менее безопасной».

LAEDA – прямое нападение на инструмент, который для обеспечения своей безопасности каждый день используют миллионы людей, считают в The Internet Society. Закон уничтожит сквозное шифрование, заставляя компании предоставлять правоохранительным органам доступ к зашифрованным данным по запросу. Единственный для компаний способ соблюдать закон – встроить бэкдоры в свои

продукты или вообще не использовать шифрование. На минуточку, речь идёт о таких областях, как онлайн-банкинг, работа из дома, телемедицина и общение с друзьями в интернете.

LAEDA – последняя на данный момент «атака» разведывательного альянса «Пять глаз» (Five Eyes) на сквозное шифрование. В альянс входят США, Великобритания, Канада, Австралия и Новая Зеландия. Впервые разведальянс потребовал от IT-компаний отказаться от шифрования в 2018 году. Союзники считают, что технологические компании не должны развивать продукты таким образом, чтобы оставлять пространство для деятельности преступников. В прошлом году правительства этих стран заявили, что сквозное шифрование может осложнить судебное преследование лиц, причастных к сексуальному насилию над детьми или терроризму.

Но нет никакого способа обеспечить бэкдор без снижения уровня безопасности пользователей, убеждены в The Internet Society. LAEDA подвергнет риску не только американцев, но всех, кто используют американские продукты и услуги со сквозным шифрованием». ***(Американский законопроект против шифрования угрожает безопасности пользователей по всему миру // РосКомСвобода (https://roskomsvoboda.org/60982/). 08.07.2020).***

***

Країни ЄС

«На следующей неделе в Германии рассмотрят законопроект, который предоставляет всем 19 федеральным государственным спецслужбам право при поиске преступников шпионить за пользователями с помощью троянов. Интернет-провайдеры будут обязаны устанавливать в своих центрах обработки данных правительственное оборудование, распространяющее вредоносное ПО. В качестве такого ПО, вероятно, выберут FinFly ISP компании FinFisher.

Большая коалиция в немецком парламенте выработала правовую основу для легального использования вредоносного ПО, которое позволит отслеживать преступников, ещё несколько лет назад. По замыслу парламентского большинства, власти должны получить право на онлайн-слежку через программное обеспечение на смартфонах или компьютере, используя для этого вредоносную программу, которая сможет считывать всю информацию до того, как он будет отправлена и зашифрована другому абоненту.

Первая версия «бундестроянца» (Bundestrojaner) была разработана ещё в 2008 году, и тогда же Федеральный конституционный суд Германии позволил применять его в делах, связанных с терроризмом. Его использование раскритиковали правозащитники и IT-эксперты, так как программа позволяла не только просматривать переписку подозреваемых, но и открывала возможность для тайных онлайн-обысков всего компьютера.

Правозащитники, в том числе Society for Freedom Rights, уже подают иски против правительства за использование ими троянских программ. Интернет-провайдеры тоже не довольны таким развитием событий, ссылаясь на

потенциальную потерю доверия со стороны населения». ***(В Германии могут разрешить спецслужбам шпионить за пользователями с помощью троянов // РосКомСвобода (https://roskomsvoboda.org/61217/). 13.07.2020).***

***

«…"Федеральний уряд дуже серйозно сприймає загрозу кібератак. Кібератаки на економічні суб'єкти та критичну інфраструктуру ми толеруємо не більше, ніж напади на урядові установи незалежно від того, від кого вони походять і з якою метою. Вони є загрозою вільному суспільству, нашій демократії та безпеці, особливо у часи коронакризи. Німеччина залишається відданою боротьбі з кібератаками разом зі своїми партнерами, особливо в межах Європейського Союзу", - заявили в МЗС…». ***(Німеччина з партнерами співпрацюватиме проти хакерів // СтопКор (https://stopcor.org/nimechchyna-z-partneramy-spivpraczyuvatyme-proty-hakeriv/). 22.07.2020).***

***

Російська Федерація та країни ЄАЕС

«Российские власти проводят активную работу по информированию людей об угрозах киберпреступлений, число которых возросло на фоне вспышки коронавирса минувшей весной, говорится в видеообращении премьер-министра Михаила Мишустина к участникам онлайн-конференции Сбербанка по кибербезопасности Cyber Polygon.

Мишустин заявил, что весной наблюдался «рост активности киберпреступников», при этом больше 90% успешных атак «проводятся с использованием методов социальной инженерии», передает ТАСС.

Для обмана бдительности граждан мошенники используют фишинговые письма и технологии подмены номера.

«В сотрудничестве с отечественными компаниями в области информационной безопасности государственные органы проводят активную работу по информированию людей о рисках и угрозах кибербезопасности», – продолжил премьер.

По его словам, со многими проблемами удалось справиться благодаря объединению усилий, «однако множество вопросов все еще требуют особенного внимания».

Мишустин отметил, что Россия готова делиться с партнерами наработками в сфере информбезопасности, однако ключевым в вопросах безопасности является международный диалог, передает РИА «Новости».

Так, геополитические разногласия распространяются и на цифровую среду, потенциальными источниками цифровых угроз могут быть целые государства.

Мишустин заявил также, что общенациональный план по восстановлению экономики предполагает радикальное увеличение числа электронных госуслуг и новые меры поддержки цифрового бизнеса…». ***(Наталья Ануфриева. Мишустин***

заявил о росте активности киберпреступников // Деловая газета «Взгляд» (https://vz.ru/news/2020/7/8/1048919.html). 08.07.2020).

***

«Громадська палата РФ повідомила про хакерські атаки на свій сайт, одну з них провели з української IP-адреси. До цього палата заявила про масштабні фальсифікації у ході голосування про зміни до конституції Росії.

«Увечері 30 червня, після офіційного закінчення прийому голосів онлайн-виборців, сайт Громадської палати РФ був атакований хакерами, яким вдалося на деякий час порушити його нормальну роботу. Це дуже схоже на відплату тих, кому члени палати заважали сіяти хаос під час проведення голосування, особливо з огляду на «падіння» сайту «фейкам.нет» в цей же час», – сказано у заяві.

Згодом уночі 1 липня Громадська палата Росії заявила про ще одну кібератаку, яку виконали з адреси, зареєстрованої в Україні…

«Офіційний сайт Громадської палати РФ знову піддався хакерській атаці. Ведуться оперативні роботи по відновленню його функціоналу. <…> IP-адреса, з якої зроблена хакерська атака на сайт ВП РФ, зареєстрована в Україні», – повідомили у палаті.

Голосування про поправки до Конституції РФ стартувало 25 червня і тривало до 1 липня. За даними екзит-полу, станом на 25-28 червня поправки до Конституції Російської Федерації підтримали 76% росіян. Попередньо за поправки до конституції РФ проголосували 72,92% громадян, повідомили у ЦВК Росії…» ***(У РФ заявили про кібератаку з України // UA.NEWS (https://ua.news/ua/v-rf-zayavyly-o-kyberatake-yz-ukrayny/). 02.07.2020).***

***

«Россия заняла второе место после США по числу утечек данных в 2019 году. Количество утечек выросло на 46% по сравнению с прошлым годом…

Сообщается, что в 2019 году в России произошло 395 случаев утечки информации из компаний и госорганов, что на 46% больше, чем в 2018 году. В результате было скомпрометировано более 172 млн записей пользовательской информации. Это в 6 раз больше, чем в прошлом году. Россия уже седьмой год подряд занимает вторую строчку рейтинга.

Чаще всего в сеть попадали персональные данные и платежная информация. При этом более половины объема скомпрометированных данных связана с ошибкой в настройках сервера оператора фискальных данных «Дримкас». Тогда «утекли» свыше 90 млн записей, говорится в исследовании.

53,4% данных «сливались» через интернет, 17,5% — через бумажную документацию и 10% — через мессенджеры. Виновными чаще всего становились рядовые сотрудники компаний (72,1%). Топ-менеджмент оказывался ответственным за утечку в 4,6% случаев. И только в 18,4% случаев были замешаны хакеры.

По мнению экспертов InfoWatch, в 2020 году число утечек данных через электронные каналы в России вырастет за счет роста количества удаленно работающих сотрудников и снижения доли бумажного документооборота».

(Кристина Пирахмедова. Россия стала второй в мире по числу утечек данных // Rusbase (https://rb.ru/news/russia-data-leakage/). 07.07.2020).

***

«В России могут быть созданы автоматизированные системы, направленные на борьбу с киберпреступностью, соответствующую меру по итогам заседания Координационного совещания руководителей правоохранительных органов РФ потребовал принять генеральный прокурор России Игорь Краснов.

«Проанализировать эффективность взаимодействия оперативных служб с центрами реагирования на инциденты в сфере информационной безопасности. Проработать вопрос о возможности создания автоматизированных поисковых систем, в том числе на базе уже существующих путем расширения функционала по предупреждению и пресечению киберпреступности, а также их интеграции с другими базами данных», — приводит предложение Краснова официальный сайт ведомства.

Краснов также поставил задачу по устойчивому повышению раскрываемости преступлений в сфере информационных технологий. Для этого необходимо обеспечить эффективное взаимодействие всех органов правопорядка, уточнил он.

«Также Генеральный прокурор Российской Федерации обратил внимание на необходимость совершенствования действующего законодательства в части расширения признаков преступлений в сфере IT-технологий, введения в процессуальные нормы понятия “электронного доказательства», процедур внесудебной блокировки “зеркал” ранее заблокированных сайтов, а также по ряду других вопросов», - уточняется в сообщении Генпрокуратуры». ***(В России предложили создать автоматизированные системы по борьбе с киберпреступлениями // Rambler News Service (https://rns.online/internet/V-Rossii-predlozhili-sozdat-avtomatizirovannie-sistemi-po-borbe-s-kiberprestupleniyami-2020-07-17/). 17.07.2020).***

***

Інші країни

«В пятницу кувейтская газета сообщила, что Израиль несет ответственность за два взрыва на иранских объектах, один из которых связан с обогащением урана, а другой с ракетным производством, произошедших на прошлой неделе.

Ежедневная газета "Al-Jareeda" привела информацию из анонимного источника, согласно которой израильская кибератака вызвала пожар и взрыв на подземном объекте по обогащению урана в Натанзе, произошедший в предрассветные часы четверга. Согласно источнику, инцидент отодвинет иранскую программу ядерного обогащения примерно на два месяца.

Газета также сообщила, что в минувшую пятницу израильские истребители-невидимки F-35 подвергли бомбардировке участок, расположенный в районе

Парчина, где, как полагают, находится комплекс по производству ракет - район, вызывающий особую обеспокоенность у еврейского государства.

Ни одно из этих утверждений не было подтверждено израильскими официальными лицами». ***(Израильские кибератаки вызвали пожар на ядерном объекте в Иране // ISRAland Online (http://www.isra.com/news/247356). 03.07.2020).***

***

Протидія зовнішній кібернетичній агресії

«Федеральное ведомство по охране конституции, выполняющее в Германии в числе прочего функции контрразведки, фиксирует возросшую угрозу общественному строю ФРГ со стороны зарубежных государств. Именно в кризисные времена усиливаются кибератаки и кампании дезинформации с целью дестабилизировать свободное общество, говорится в докладе спецслужбы, обнародованном в четверг, 9 июля. В качестве примеров таких дестабилизирующих государств названы Россия и Китай.

В докладе также сообщается о резком увеличении количества преступлений, совершенных в Германии правыми и особенно левыми экстремистами. Ведомство насчитало в 2019 году свыше 22300 преступлений с правоэкстремистской подоплекой - почти на 10 процентов больше, чем годом ранее, и 6400 преступлений - на левоэкстремистской почве - почти на 40 процентов больше, чем в 2018 году.

В то же время число насильственных преступлений, совершенных экстремистами, сократилось: на 15 процентов в случае с правыми и на 10 процентов - в случае с левыми.

Исламистская угроза

Федеральное ведомство по охране конституции полагает, что по-прежнему сильная угроза исходит от исламских экстремистов. Авторы доклада отмечают, что за последние три года в ФРГ не было совершено ни одного теракта, но подчеркивают, что это может быть связано с разгромом джихадистской группировки "Исламское государство" (ИГ) в Сирии, а также с бдительностью немецких спецслужб.

Угроза для Германии со стороны исламистов по-прежнему высока, к примеру, салафиты продолжают усиливать свое влияние, говорится в докладе Федерального ведомства по охране конституции». ***(Сергей Ромашенк. Доклад: Россия усиливает подрывную деятельность в Германии // (https://www.dw.com/ru/%D0%B4%D0%BE%D0%BA%D0%BB%D0%B0%D0%B4-%D1%80%D0%BE%D1%81%D1%81%D0%B8%D1%8F-%D1%83%D1%81%D0%B8%D0%BB%D0%B8%D0%B2%D0%B0%D0%B5%D1%82-%D0%BF%D0%BE%D0%B4%D1%80%D1%8B%D0%B2%D0%BD%D1%83%D1%8E-%D0%B4%D0%B5%D1%8F%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%***

BE%D1%81%D1%82%D1%8C-%D0%B2-%D0%B3%D0%B5%D1%80%D0%BC%D0%B0%D0%BD%D0%B8%D0%B8/a-54103992?maca=rus-rss-MetaUA_rus_V_Mire-3045-xml-mrss). 09.07.2020).

****

«Директор ФБР Кристофер Рэй винит Китай в ограблении США, пишет CNBC. Так он охарактеризовал кибератаки и шпионаж со стороны китайских властей и компаний, в которых Вашингтон обвиняет Пекин.

По словам Рэя, действия Китая приводят к «одной из крупнейших в истории человечества передаче благосостояния» [из США в Китай]. Ущерб, наносимый американским бизнесу и экономике, не поддается подсчету, отметил глава ФБР.

Китайские компании, по его словам, стремятся на равных соперничать с зарубежными конкурентами, в том числе с американскими, однако не способны делать это на общих основаниях. Чтобы нивелировать технологическое отставание, они прибегают к промышленному шпионажу и кибератакам, а затем отвоевывают часть рынка у тех же компаний, которые стали их жертвами. Такое положение дел Рэй назвал двойным обманом.

При этом, добавил чиновник, претензии к Пекину не должны привести к отказу от сотрудничества с ним, приема китайских студентов и «сосуществования с Китаем на мировой сцене».

Обвинения в неправомерном получении доступа к американским технологиям стали одним из главных поводов для торговой войны между Вашингтоном и Пекином, начавшейся в 2018 году. Президент США Дональд Трамп апеллировал к китайскому закону, согласно которому иностранные компании могут заходить на местный рынок только через создание совместного предприятия с местными партнерами, которые получают доступ ко всем используемым в производстве технологиям.

Впоследствии власти США обвинили несколько китайских компаний, среди которых производители смартфонов и телекоммуникационного оборудования Huawei и ZTE, в незаконном сборе персональных данных и их дальнейшей передаче спецслужбам Китая. Корпорации были включены в черный список, который предусматривает запрет для американских резидентов на сотрудничество с его фигурантами. Впоследствии ограничения смягчили». ***(Китай обвинили в ограблении США // ООО «Лента.Ру» (https://lenta.ru/news/2020/07/08/theft/). 08.07.2020).***

****

«Німецький уряд запропонував країнам-членам ЄС запровадити спільні санкції через масштабну хакерську атаку на Бундестаг п’ять років тому. У федеральному уряді Німеччини вважають, що до неї був причетний хакер Головного розвідувального управління Генерального штабу Російської Федерації (ГРУ). Про це в неділю, 12 липня, повідомляє DW та інформагенція dpa з посиланням на отриману копію відповіді уряду на запит фракції Лівої партії в Бундестазі…

Федеральна прокуратура Німеччини 5 травня видала ордер на арешт громадянина Росії Дмитра Бадіна. У прокуратурі припускають, що він є членом хакерської групи APT28 і підозрюють, що Бадін "відповідав за хакерську атаку на німецький Бундестаг у квітні-травні 2015 року".

Федеральний уряд "подав пропозиції щодо санкцій в рамках ЄС і представив масштабний пакет доказів на основі результатів розслідування німецьких органів, розвідувальної інформації та загальнодоступних джерел" та надіслав їх іншим країнам-членам ЄС, йдеться у відповіді уряду на запит фракції Лівої партії.

Речник Єврокомісії у відповідь на запит dpa зазначив, що окремі країни ЄС можуть вносити такі пропозиції. "Далі рішення за Радою ЄС, яке має бути ухвалене одноголосно", — зауважив він, додавши, що відповідне повідомлення зроблять лише після ухвалення такого рішення.

Якщо ЄС таки запровадить санкції за хакерську атаку на Бундестаг, то це стане першим випадком застосування режиму санкцій у відповідь на кібератаки з моменту його ухвалення в травні 2019 році.

Нагадаємо, у травні 2015 року стало відомо про найбільшу хакерську атаку проти німецького Бундестагу. Тоді багато комп'ютерів у офісах депутатів, а також в офісі канцлерки Німеччини Анґели Меркель були заражені шпигунським програмним забезпеченням.

У 2017 році Рада ЄС вирішила розробити основу для спільної дипломатичної відповіді Євросоюзу на шкідливу кібердіяльність — так званий набір інструментів кібердипломатії (Cyber Diplomacy Toolbox).

Цей "набір інструментів" націлений на "окремих осіб чи групи, а не на країни", наголосили у федеральному уряді у відповіді на запит фракції Лівої партії». ***(Ілля Нежигай. Німеччина запропонувала ЄС запровадити санкції проти Росії за кібератаку // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1880182-nimechchina-zaproponuvala-yes-zaprovaditi-sanktsiyi-proti-rosiyi-za-kiberataku). 12.07.2020).***

***

«Президент США Дональд Трамп в 2018 році схвалив проведення кібератаки, націленої на російське "Агентство інтернет-досліджень", також відоме як "фабрика тролів". Про це оглядач видання The Washington Post Марк Тісен пише у своїй колонці в суботу, 11 липня…

За словами журналіста, який кількома днями раніше провів інтерв'ю з главою Білого дому, Трамп у відповідь на питання, чи санкціонував він атаку, відповів: "Правильно".

Президент пояснив, що діяв на підставі наданих йому розвідданих про втручання російської сторони в вибори в Сполучених Штатах. Видання повідомляло про хакерську атаку ще в лютому 2019 го, однак глава держави раніше не підтверджував її проведення.

За словами Трампа, кібератака була лише одним з елементів політики американської влади щодо РФ. "Ніхто не проявляє до Росії більше жорсткості, ніж я", — підкреслив президент. Він відніс до списку дій, націлених на протидію Росії, поставки озброєнь до України, перетворення США в "державу номер один по

видобутку нафти", а також неодноразову критику газопроводу "Північний потік — 2"…». ***(Ілля Нежигай. Трамп підтвердив кібератаку США на російську "фабрику тролів" // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1880010-tramp-pidtverdiv-kiberataku-ssha-na-rosiysku-fabriku-troliv). 11.07.2020).***

***

«Предложение Германии странам Европейского союза ввести санкции против причастных к хакерской атаке на бундестаг, которая была осуществлена в 2015 году, встретило широкую поддержку в ЕС, но переговоры о запуске процедуры и списке лиц еще продолжаются, заявил представитель МИД ФРГ Райнер Бройль.

«Мы подали этот запрос в кругу членов ЕС. Мы получили широкую поддержку», – передает ТАСС слова Бройля.

«Доверительные переговоры пока продолжаются, поэтому я не могу озвучить промежуточные результаты», – добавил он, указав на то, что требует обсуждения, в частности, определение лиц, которые, как предполагается, будут включены в санкционный список.

Напомним, в воскресенье правительство Германии предложило странам-членам Евросоюза совместно ввести санкции против России за масштабную кибератаку на германский бундестаг пять лет назад.

Посол России был вызван в МИД Германии в связи с делом о хакерской атаке на бундестаг. Позже Берлин заявил, что возможные санкции в отношении Москвы по делу о хакерской атаке на бундестаг предполагают ограничение въезда ответственных лиц на территорию Европейского союза…». ***(Дмитрий Зубарев. ЕС поддержал предложение Германии ввести санкции против России из-за кибератаки на бундестаг // Деловая газета «Взгляд» (https://vz.ru/news/2020/7/13/1049720.html). 13.07.2020).***

***

«После того, как Трамп дал ЦРУ полную свободу в проведении кибердиверсий против других стран, а также публично признался, что лично приказал провести интернет-атаку в России, США превратились для нас в киберугрозу номер 1… Частично обезопасить себя от подобной угрозы России удается благодаря вовремя принятому закону «Об устойчивом интернете».

«В конце 80-х годов мы сами отбросили свое аппаратное программное обеспечение и по сути позволили американцам провести захват нашей цифровой территории», – сказал газете ВЗГЛЯД гендиректор компании «Ашманов и партнеры» Игорь Ашманов. Причем, добавил эксперт, Россия по-прежнему во многом зависит от той самой страны, которая в своей военной стратегии назвала РФ своим основным противником. А теперь, после указа президента США, ее спецслужбам и вовсе разрешено в любой момент проводить кибератаки против РФ.

«Трамп официально разрешил ЦРУ не согласовывать с Белым домом кибератаки. США считают абсолютно нормальным вести спецоперации в интернете в мирное время, и не просто наблюдение или слежку, а диверсии. Мы

видели, как с помощью кибератак обрушивают центрифуги в Иране», – подчеркнул Ашманов.

Ашманов считает, что кибервойска есть теперь у большинства стран мира, но Москву должна беспокоить прежде всего угроза со стороны Вашингтона. «Европа настолько слаба в программистском плане, что использует почти все американское. У них нет ни своих соцсетей, ни поисковиков. Это очевидный показатель. Что касается Китая, то он не является нашим врагом», – указал Ашманов…

Как заявил газете ВЗГЛЯД зампред комиссии Общественной палаты по СМИ, президент Фонда защиты национальных ценностей Александр Малькевич, компьютерные диверсии, которые ЦРУ теперь может проводить без отмашки Белого дома, могут нанести в том числе физический и материальный ущерб. «Попытки спецслужб США взломать энергосистему России, о которых уже ранее сообщалось, выглядят одной из самых больших угроз – они могут принести прямой вред здоровью людей», – подчеркнул Малькевич.

В экспертной среде неоднократно отмечали, что наибольшую угрозу представляют как раз хакерские атаки американских спецслужб на энергосистемы других стран. Так, в прошлом году в Венесуэле без света осталось 80% территории страны. Министр информации республики Хорхе Родригес заявил, что причиной сбоя стала кибератака с территории США, которой подверглась автоматическая система контроля венесуэльской ГЭС «Гури».

Бывший сотрудник АНБ Эдвард Сноуден, получивший убежище в России, подробно рассказывал взломах компьютерных сетей Гонконга и материкового Китая, которые проводили США, а также о диверсиях на оборонных объектах Северной Кореи. По его словам, американским спецслужбам разрешено нападать даже и на объекты критической инфраструктуры, хотя международное сообщество предварительно договорилось считать их неприкасаемыми для виртуальных атак.

Что касается уровня защищенности России от такого роа угроз, то он растет, отмечает Ашманов. «В стране производится довольно много продуктов по информационной безопасности, по этой линии работают спецслужбы. С рынка в сфере информационной безопасности вытесняются такие западные IT-гиганты как Symantec, Check Point и другие, – перечислил он. – Импортозамещение в сфере IT происходит быстрее, чем в других областях. Теперь российские госорганы, госкорпорации и обычные крупные компании покупают отечественный софт в области информационной безопасности».

Однако сохраняется сильная зависимость России от США на уровне пользовательского софта, прежде всего – операционных и офисных программ. «А в области программного обеспечения по управлению производственными процессами (АСУ ТП) у нас стопроцентная зависимость. Во времена приватизации на предприятиях ставили исключительно западный софт, чтобы привлекать иностранных инвесторов. В результате: все эти производства при желании могут быть выключены из-за рубежа», – предупредил собеседник.

Интернет в целом, как известно, также опирается на западные технологии, «поэтому мы неспроста приняли закон «Об устойчивом интернете», отметил Ашманов. «Либеральная пропаганда очень долго пыталась переименовать его в закон «об изоляции российского интернета». Но как мы видим, никакой изоляции

не происходит. Если наши довольно безумные киберпротивники вдруг выключат рубильник, то мы сможем благодаря этому закону все равно сгенерировать себе интернет, который уже стал для страны критической инфраструктурой. Мы постепенно становимся защищенными, хотя не все еще сделано. Закон правильный, но его надо полностью исполнять. Для этого нужны дополнительные вложения государства в сферу информационной безопасности», – уверен Ашманов.

Малькевич тоже считает, что «уберечься от серьезных аварий вследствии кибератак, России помогают меры принятые в рамках нового закона, вступившего в силу прошлой осенью. Эксперт напомнил, что закон «Об устойчивом интернете» регулирует вопросы создания необходимой инфраструктуры, которая позволит обеспечить работоспособность российских ресурсов на случай, если отечественный операторы связи вдруг лишатся доступа к зарубежным корневым серверам.

«Кроме того, в стране регулярно проводятся учения, на которых проверяется устойчивость и безопасность интернета, «интернета вещей» и различных сегментов сетей связи общего пользования – фиксированной и мобильной. Такие «маневры» носят исследовательский характер. Не случайно их решено проводить только в наименее загруженные периоды, когда низкий трафик. Так что мы готовы встречать врага во всеоружии», – подытожил Малькевич». ***(Андрей Резчиков. Эксперты назвали самые уязвимые для интернет-атак США российские цели // Деловая газета «Взгляд» (https://vz.ru/news/2020/7/17/1050494.html). 17.07.2020).***

***

«Рада Євросоюзу ухвалила рішення застосувати новий режим кіберсанкцій проти Росії, Китаю та Північної Кореї. Термін чинності санкцій — рік. Їх спрямовано проти організацій та окремих осіб, діяльність яких загрожує державам-членам та інституціям ЄС. Сутність обмежувальних заходів полягає у візовій забороні на в'їзд кіберзлочинців на територію Євросоюзу й арешті їхніх рахунків у банках країн-членів ЄС.

Об'єктами кіберсанкцій ЄС в Росії стало головне розвідувальне управління (ГРУ), яке Брюссель вважає відповідальним за поширення програми-хробака NotPetya, під ударом якого опинилися треті країни, зокрема Україна, де вірус вразив банківську систему і систему енергопостачання.

«ГРУ відповідає за кібератаки зі значним впливом, які виникли за межами ЄС і становлять зовнішню загрозу для його держав-членів, а також за ті, що мають суттєвий вплив на треті держави, зокрема загальновідома NotPetya, спрямовані на українську електромережу взимку 2015 та 2016 років», — ідеться в рішенні Ради ЄС.

У документі наголошено, що вірус NotPetya «зробив недоступними дані багатьох компаній ЄС, інших країн світу, що призвело до значних економічних втрат. Кібератака на українську електромережу призвела до того, що взимку її частково було відімкнено», — зазначено в документі.

У список кіберсанкцій внесено чотирьох співробітників ГРУ: Олексія Мініна, Олексія Моренця, Євгена Серебрякова і Олега Сотникова за причетність до спроб кібератаки проти Організації із заборони хімічної зброї в Нідерландах.

На початку липня Берлін звернувся до Єврокомісії із проханням покарати Росію за масштабну кібератаку на Бундестаг, здійснену п’ять років тому. Уряд ФРН вважає, що до неї причетна російська розвідка. Федеральна прокуратура ФРН у травні цього року видала ордер на арешт громадянина РФ Дмитра Бадіна, який «як член хакерської групи APT28, імовірно, керував кібератакою на німецький Бундестаг в квітні-травні 2015 року». В МЗС ФРН заявили, що мають достовірні докази того, що на момент атаки Бадін був співробітником ГРУ.

Цілком можливо, що список кіберсанкцій буде розширено найближчим часом.

Експерти вважають, що санкції ЄС навряд чи зупинять російських хакерів у подальших спробах дестабілізувати Захід. Проте вони — чіткий сигнал, що такі дії не залишаться безкарними». ***(Вікторія ВЛАСЕНКО. ЄС покарав Кремль за хакерські атаки // Урядовий кур’єр (https://ukurier.gov.ua/uk/news/yes-pokarav-kreml-za-hakerski-ataki/). 31.07.2020).***

***

«Міністр закордонних справ Дмитро Кулеба заявив, що рішення Європейського Союзу про застосування санкцій за кібератаки допоможе стримувати агресивні дії Росії у кіберпросторі

Про це він написав у Twitter.

“Вітаю рішення ЄС застосувати обмежувальні заходи проти тих, хто вчиняє кібератаки. Це дозволить ЄС накладати санкції на осіб і організації, які здійснюють кібератаки чи надають підтримку для таких злочинних дій. Це також допоможе стримувати агресивні дії Росії у кіберпросторі”, - зазначив Кулеба.

Він зауважив, що цей крок підвищить стійкість кіберпростору до атак, які загрожують підвалинам демократичних суспільств.

За словами міністра, новий санкційний режим ЄС передбачає також санкції за кібератаки проти третіх країн.

“Відтак, це відкриває можливості для співпраці між Україною та ЄС в питаннях відстежування, виявлення та реагування на тих, хто здійснює кібератаки на критичну інфраструктуру нашої держави”, - наголосив Кулеба». ***("Допоможе стримувати агресивні дії Росії у кіберпросторі": Кулеба відреагував на санкції ЄС проти хакерів // Espreso.tv (https://espreso.tv/news/2020/07/30/quotdopomozhe_strymuvaty_agresyvni_diyi_rosiyi_u_kiberprostoriquot_kuleba_vidreaguvav_sankciyi_yes_proty_khakeriv). 30.07.2020).***

***

Захист персональних даних

«Неизвестный киберпреступник получил несанкционированный доступ к 29 тыс. баз данных MongoDB, доступных через интернет без какого-либо пароля, и оставил в них записку с требованием выкупа. 29 тыс. – это 47% от всех подключенных к Сети установок MongoDB.

С помощью скрипта автоматизации злоумышленник находит в интернете незащищенные базы данных, стирает их контент и оставляет записку с требованием 0,015 биткойна (порядка $140). На уплату выкупа жертвам дается два дня, после чего киберпреступник грозится опубликовать похищенные данные и сообщить об утечке местному органу, ответственному за соблюдение «Общего регламента по защите данных» (GDPR).

Вредоносная кампания продолжается с апреля 2020 года. Как сообщил изданию ZDNet специалист GDI Foundation Виктор Геверс (Victor Gevers), изначально злоумышленник не удалял данные из БД. Он оставлял записку с требованием выкупа, а через несколько дней повторно подключался к БД и оставлял записку снова. Однако впоследствии киберпреступник понял свою ошибку, исправил скрипт, и теперь он удаляет содержимое баз данных.

Хотя некоторые установки MongoDB являются тестовыми, по словам Геверса, в ходе кампании пострадали и производственные системы, а некоторые предприятия также лишись резервных копий своих данных.

На днях Геверс также сообщил о том, что киберпреступная группировка Cl0ud SecuritY взламывает устаревшие сетевые хранилища (NAS) LenovoEMC (в прошлом Iomega), стирает все файлы и требует $200-275 за их возвращение». ***(Хакер стирает данные из MongoDB и требует выкуп // SecurityLab.ru (https://www.securitylab.ru/news/509650.php) 02.07.2020).***

***

«Операторы вымогательского ПО REvil выставили на web-аукцион в даркнете конфиденциальные данные, похищенные у юридической фирмы Grubman Shire Meiselas & Sacks. Стартовая цена составляет $600 тыс. за каждый из трех лотов данных, принадлежащих поп-звездам Мэрайе Кэри и Ники Минаж, а также баскетболисту Леброну Джеймсу. Каждый лот можно выкупить вне очереди за сумму в размере $1,5 млн в криптовалюте Monero, сообщил ресурс Computerweekly.

Группа также предлагает выкупить все данные, похищенные в результате взлома Grubman Shire Meiselas & Sacks, за сумму в $42 млн (один из крупнейших выкупов в истории).

На втором аукционе, планируемом 3 июля, операторы REvil выставят на продажу данные ряда развлекательных компаний, в том числе лейбла Bad Boy Entertainment, киностудии Universal и музыкального канала MTV. Третий аукцион назначен на 5 июля, однако остается неизвестным, что будет выставлено на продажу.

Каждый аукцион продлится три месяца, и если будет продан определенный лот, преступники обещают удалить все данные лота со своих серверов и сделает их доступными только для покупателя…». ***(Группировка REvil выставила на web-аукцион данные знаменитостей // SecurityLab.ru (https://www.securitylab.ru/news/509664.php). 02.07.2020).***

***

«В прошлом году мы рассказывали о бывшем инженере компании Yahoo Рейесе Даниэле Руисе (Reyes Daniel Ruiz), который проработал в компании более 10 лет (с 2009 по 2019 год) и пользовался своим служебным положением: получал доступ к почтовым ящикам молодых женщин и похищал оттуда откровенные фото и видео.

В общей сложности Руис взломал более 6000 учетных записей, причем некоторые из них принадлежали его коллегам и подругам. Он использовал свой доступ к бэкэнду Yahoo для получения доступа к хешированным паролям, а затем взламывал их и проникал в чужие учетные записи Yahoo Mail. Из почтовых ящиков своих жертв хакер похищал эротические изображения и видео, которые хранил дома на жестком диске.

Кроме того, Руис использовал доступ к скомпрометированным почтовым ящикам для взлома других учетных записей жертв, в том числе iCloud, Facebook, Gmail, DropBox и так далее (для которых жертвы использовали почту Yahoo при регистрации). Для этого он запрашивал сброс пароля на сторонних сайтах и получал письмо на подконтрольный ему адрес в почте Yahoo. После Руис продолжал поиск откровенного контента и на этих аккаунтах. Считается, что он взломал примерно 100 учетных записей в iCloud, Gmail, Hotmail, Dropbox и Photobucket.

По данным следствия, Руис пытался уничтожить свой домашний «архив» и компьютер, где хранил все загруженные изображения и видео, когда в Yahoo наконец заметили подозрительную активность и начали расследование в его отношении. Позже он признался в этом сотрудникам ФБР. Из-за уничтожения жесткого диска обвинение сумело идентифицировать только 3137 из примерно 6000 пострадавших.

В общей сложности Руис похитил у пользовательниц около 2 ТБ данных и хранил от 1000 до 4000 частных изображений и видео.

В этом месяце суд наконец вынес Руису приговор: сталкер получил пять лет условно и был помещен под домашний арест, то есть ему разрешено покидать дом только для поездок на работу, религиозной деятельности, посещения врача или выполнения обязанностей, предписанных с судом. Также Руис выплатит штраф в размере 5000 долларов США и возместит убытки компании Yahoo в размере 118 456 долларов США.

Столь мягкий приговор объясняется тем, что Руис сотрудничал со следствием и никогда не публиковал украденные данные в интернете». ***(Мария Нефёдова. Сотрудник Yahoo, шпионивший за пользователями, избежал тюрьмы // Хакер (https://xakep.ru/2020/07/07/ruiz-sentenced/). 07.07.2020).***

****

«Специалисты из компании Digital Shadows обнаружили 15 млрд учетных данных на различных подпольных торговых площадках в даркнете. Скомпрометированные учетные данные были похищены в результате более чем 100 тыс. взломов и предоставляют доступ к различным аккаунтам, в том числе к учетным записям администраторов доменов, банковским и финансовым учетным записям, а также аккаунтам сервисов социальных сетей и стриминговых площадок.

Цены на подпольных торговых площадках за подобную информацию варьируются в среднем от $71 за банковские аккаунты, $21 за доступ к учетным записям антивирусных программ и до $3,1 тыс. за учетные записей администраторов домена. Логины и пароли для учетных записей пользователей видеоигр и сайтов для обмена файлами были доступны менее чем за $2 за запись.

По словам экспертов, учетные данные для финансовых аккаунтов с подтвержденным наличием денежных средств или учетных записей с привилегированным доступом к сетям и системам крупных предприятий, продавались по очень высоким ценам. На подпольных форумах были обнаружены десятки рекламных объявлений об учетных записях администраторов, которые были проданы с аукциона участникам торгов по ценам от $500 до $120 тыс.

В общей сложности, 25% объявлений о продаже украденных и утекших учетных данных были связаны с банковскими и другими финансовыми счетами. Другие популярные категории объявлений включали учетные записи стриминговых сервисов, прокси/VPN и кабельного телевидения.

По словам специалистов, угроза от взломов усугубляется тенденцией среди большого числа интернет-пользователей использовать одни и те же и зачастую легко угадываемые пароли для нескольких учетных записей. Такие инструменты, как Sentry MBA и OpenBullet, упростили киберпреступникам проверку миллионов логинов и паролей. Таким образом, злоумышленники могут использовать учетные данные, полученные в результате одного взлома, чтобы попытаться получить доступ к другим аккаунтам.

Как показали результаты исследования специалистов Digital Shadows, число скомпрометированных учетных данных, доступных для киберпреступников в даркнете, выросло на 300% с 2018 года. По оценкам экспертов, из 15 млрд похищенных учетных данных около 5 млрд являются уникальными.

Нелегальные торговые площадки, такие как Genesis Market, UnderWorld Market и Tenebris, предоставляют преступникам возможность арендовать доступ к различным типам учетных записей, включая электронную коммерцию, стриминг и социальные сети, иногда всего лишь за $10 долларов за определенный период использования». ***(На подпольных торговых площадках обнаружено около 15 млрд похищенных учетных данных // SecurityLab.ru (https://www.securitylab.ru/news/509847.php). 09.07.2020).***

***

«Данные из приложений TikTok и WeChat идут прямо на серверы в Китае, к китайским военным и Китайской коммунистической партии, заявил торговый советник Белого дома Питер Наварро. По его словам, «TikTok и WeChat — самые большие площадки с цензурой на материковой части Китая». Наварро пригрозил сервисам «решительными действиями» в отношении них.

TikTok ответил, что защита конфиденциальности данных пользователей является важнейшим приоритетом для компании и она никогда не делилась и не будет делиться информацией с китайским правительством. WeChat ситуацию никак не прокомментировал.

Ранее госсекретарь США Майкл Помпео заявил об опасениях властей США о том, что TikTok может использоваться Пекином в качестве средства наблюдения и пропаганды. В октябре прошлого года два американских конгрессмена попросили директора Национальной разведки проверить, имеет ли коммунистическое китайское правительство какое-либо влияние на то, что американцы видят в приложении. По их словам, «с более чем 110 млн загрузок только в США TikTok является потенциальной контрразведывательной угрозой», которую нельзя игнорировать. Президент США Дональд Трамп однажды и вовсе назвал возможный запрет TikTok «одним из многих» вариантов, которые он рассматривал, чтобы наказать Китай за коронавирус.

Пока политики только рассуждают и грозятся, американские корпорации всерьёз откликаются на их призыв бойкотировать TikTok из соображений безопасности. Так, в банковском холдинге Wells Fargo сказали сотрудникам, чтобы они убрали приложение со своих телефонов. В Amazon попросили сделать то же самое, но, впрочем, быстро отступили от этого требования.

WeChat — приложение, которое большей частью использует китайская диаспора, тогда как TikTok — молодёжь по всему миру. Поэтому ущерб от запрета в США у WeChat скорее всего будет меньше, чем у TikTok, у которого в этой стране не менее 52 млн пользователей». ***(В США продолжают грозить TikTok и WeChat ограничениями // РосКомСвобода (https://roskomsvoboda.org/61399/). 16.07.2020).***

***

«Исследовательская команда vpnMentor обнаружила в открытом доступе незащищенный сервер популярных бесплатных VPN-приложений, хранящий пользовательские данные. Все эти приложения базируются в Гонконге. Отсутствие элементарной защиты в таком продукте безопасности, как VPN-приложение, не только вызывает большое удивление, но также демонстрирует полное пренебрежение их разработчиков стандартными практиками VPN, ставящее пользователей под угрозу.

Обнаруженный исследователями сервер используется приложениями UFO VPN, FAST VPN, Free VPN, Super VPN, Flash VPN, Secure VPN и Rabbit VPN. Судя по количеству их пользователей, на сервере хранится персонально идентифицируемая информация более 20 млн человек, в том числе электронные адреса, незашифрованные пароли, IP-адреса, домашние адреса, данные о моделях смартфонов, идентификаторы устройств и другие технические подробности. Всего на сервере была обнаружена 1 083 997 361 запись общим объемом 1,207 ТБ.

Несмотря на заявления владельцев приложений о том, что их программы не собирают пользовательские логи, vpnMentor нашла на сервере множество записей об активности пользователей в интернете.

Поскольку все данные хранятся на одном сервере Elasticsearch и размещены в одних и тех же активах, а получателем платежей для приложений значится одна и та же гонконгская компания Dreamfii HK Limited, исследователи предположили, что они были созданы одним и тем же разработчиком, но используются под разными брендами.

Попытки установить диалог с владельцами сервисов практически не увенчались успехом, а гонконгский CERT заявил, что «если IP-адреса расположены в США, то предоставленная информация не имеет отношения к Гонконгу», исследователям нужно обратиться в американский CERT или предоставить больше данных, свидетельствующих о связи утечки с Гонконгом». ***(Базирующиеся в Гонконге бесплатные VPN допустили утечку пользовательских данных // РосКомСвобода (https://roskomsvoboda.org/61387/). 16.07.2020).***

***

«Cyber Risks Калифорнийский страховщик First American Title Insurance, который непреднамеренно оставил десятки миллионов пользовательских записей доступными в Сети, стал первой компанией, обвиненной Нью-Йоркским департаментом финансовых услуг (Department of Financial Services, DFS) в нарушении правил кибербезопасности.

По словам финансового регулятора, First American Title Insurance небрежно относится к защите своих данных, в результате чего нарушила законы штата о защите непубличной информации. В апреле 2018 года в системах страховщика содержалось около 753 млн документов, 65 млн из которых были помечены как конфиденциальные. В мае 2019 года количество записей возросло до 850 млн. Вся информация находилась в общем доступе в Сети в течение четырех лет из-за уязвимости в системах безопасности.

По крайней мере с октября 2014 года по май 2019 года из-за уязвимости на общедоступном веб-сайте First American практически любой пользователь мог получить доступ к персональным данным, включая номера банковских счетов и выписки, записи об ипотеке и налогах, номера социального страхования, квитанции об оплате транзакций и изображения водительских прав.

Документы содержались в базе данных FAST компании First American Title Insurance. Как сообщается в обвинении, утечка данных произошла в 2014 году из-за уязвимости в программном обеспечении EaglePro для обмена документами с FAST по электронной почте с клиентами. Уязвимость могла быть проэксплуатирована для просмотра любого изображения в системе — документы, отправленные через EaglePro, отображались с URL-адреса с параметром ImageDocumentID, который можно изменить на любое другое значение и получить доступ к документам других пользователей без проверки авторизации.

Компания знала об этой уязвимости в программном обеспечении на протяжении шести месяцев, однако не сделала ничего, чтобы решить данную проблему». ***(Американская страховая компания допустила утечку 850 млн данных пользователей // TRISTAR.com.ua (http://tristar.com.ua/1/news/amerikanskaia_strahovaia_kompaniia_dopustila_utechku_850_mln_dannyh_polzovatelei_13853.html). 28.07.2020).***

***

«Facebook Messenger, которым пользуются сотни миллионов людей, не является безопасным каналом связи. Несмотря на все усилия компании обеспечить конфиденциальность, пользователи не могут быть уверены в ней.

Об этом пишет Зак Доффман в статье для Forbes.

Объявляя о своих последних обновлениях, Facebook заверил, что “конфиденциальность лежит в основе Messenger – где вы можете быть самим собой с людьми, которые для вас наиболее важны”. Компания заявила, что добавит еще один уровень безопасности чтобы предотвратить доступ других людей к ним.

“К сожалению, это обновление похоже на добавление дополнительных замков к входной двери банка, когда хранилище оставлено широко открытым … В настоящее время есть альтернативы, которые предлагают большую часть той же функциональности без риска. Пришло время переключаться“, – пишет автор статьи.

Одной из основных проблем Доффман называет сквозное шифрование. В частных разговорах можно включить сквозное шифрование для отдельных чатов, а не для групп и по умолчанию. “Секретный разговор в Messenger полностью зашифрован и предназначен только для вас и вашего собеседника”, – говорит Фейсбук, подразумевая, что сообщения, которые не являются “секретными” имеют риск стать доступными для всех.

Компания стала ведущим защитником сквозного шифрования в мире, даже генеральный директор Марк Цукерберг лично оценил ее преимущества. Однако компания также признала, что технические сложности добавления этого уровня безопасности в Messenger займут годы. При этом, например, в WhatsApp, абсолютно все сообщения уже сейчас защищены сквозным шифрованием.

“Пользователи, которые хотят общаться через Messenger, должны понимать реальную угрозу их информации в таких приложениях. Хотя многие могут подумать, что содержимое их сообщений не является личным, реальная проблема заключается в том, что любая информация о вас открыта для злоупотребления в чужих руках“, – предупреждает эксперт ESET по кибербезопасности Джейк Мур.

Мур выступает за Signal – платформу, предпочтительную для кибер-экспертов, с ее первоочередным подходом к обеспечению безопасности и отсутствием резервных копий обмена сообщениями.

Мур также рекомендует Telegram – немного более сложный вариант. Telegram не выполняет сквозное шифрование по умолчанию. Тем не менее, Telegram применяет подход, основанный на принципах безопасности, и распределяет ключи шифрования, которые он хранит, в разных юрисдикциях, чтобы предотвратить любые внутренние попытки – злонамеренные или по запросу служб безопасности – получить доступ к контенту.

“Платформы обмена незашифрованными сообщениями широко открыты для атак и остаются уязвимыми. Мы должны начать информировать людей о рисках и начать переходить на приложения, ориентированные на конфиденциальность“, – резюмировал Мур.

Автор статьи подчеркивает, что Facebook Messenger останется небезопасной платформой для общения до тех пор, пока не внедрит полную защиту сквозным шифрованием.

Как сообщал “источник”, в мессенджере Telegram появилось долгожданное нововведение – возможность совершения видеозвонков». ***(Forbes: Почему вы***

должны прекратить использование Facebook Messenger // Луганский Радар (https://lugradar.net/2020/07/225441). 26.07.2020).

***

«Атаки, лоснованные на методе Ransomware of Things (RoT), позволяют злоумышленникам контролировать окружающие устройства — от умных устройств в наших домах до автомобилей, подключенных к интернету.

Согласно отчету кибербезопасности Check Point 2020, атаки с использованием вымогателей были очень распространены из-за высокой успешности. При этом типе кибератак киберпреступники требовали от компаний выкуп за украденную информацию. В среднем 8 % компаний становятся жертвами такого рода угроз еженедельно.

Сейчас мы живем в мире растущей гиперподключенности, когда устройства подключаются к одним и тем же сетям, и наблюдаем эволюцию этого типа угроз. Вместо того, чтобы перехватывать информацию или данные компании или отдельного лица, злоумышленники берут на себя полное управление устройствами, подключенными к интернету. Пользователи не смогут использовать их, пока выкуп не будет выплачен. Эта тактика называется Ransomware of Things (RoT). Традиционные атаки с помощью вымогателей представляют риск для организаций, но RoT-атаки несут серьезные последствия для всего общества в целом.

Возможность подключиться к всемирной сети не только несет бесчисленные преимущества, но и создает риски кибербезопасности. Интернет вещей все больше входит в нашу повседневную жизнь, но пробелы в безопасности остаются и предоставляют киберпреступникам возможности для атак. Сегодня 1 из 4 атак направлена на IoT-устройства, поскольку благодаря устаревшим операционным системам и отсутствию средств защиты эти устройства легко взломать.

RoT-атаки схожи с традиционными тем, что они требуют выкуп — но на этом их сходство заканчивается. В случае RoT-атак, а не только данные, а целое устройство, удерживается «в заложниках» с использованием вируса, известного как jackware. Jackware — вредоносное ПО, которое контролирует устройства, подключенные к интернету, даже если они не обрабатывают данные. Например, в этом случае киберпреступник может контролировать все виды бытовой техники в доме. В более сложных случаях в подключенных домах киберпреступники могут управлять поставками, такими как электричество или вода, и даже домашней автоматизацией.

Когда мы выходим за пределы домашней среды, чтобы рассмотреть что-то более масштабное, мы видим, что последствия могут быть гораздо серьезнее. Например, если речь идет о безопасности дорожного движения — подключенных к интернету автомобилей становится все больше, такая машина уже обычное явление. Ожидается, что к концу 2020 года они будут составлять 22% всех автомобилей в мире. Владельцы таких машин могут, например, через приложение

на смартфоне открывать и закрывать двери, запускать двигатель. Все это позволяет киберпреступникам совершать нападения на машину как непосредственно, так и с помощью смартфона. Если злоумышленник получит доступ к управлению транспортным средством, это может поставить под угрозу жизнь его пассажиров, пешеходов и других транспортных средств. Пока этого еще не происходило, но учитывая технологический прогресс таких автомобилей, такая атака RoT возможна в ближайшем будущем.

Новые поколения киберугроз очень изощренные — они используют старую тактику совершенно новым способом, чтобы обойти традиционные решения безопасности. RoT-атаки хорошо это демонстрируют, поскольку киберпреступники используют возможности подключения к IoT-устройствам и отсутствие защиты на их для запуска атак и, возможно, захвата контроля над целыми сегментами общества.

Все это может показаться очень футуристическим, но киберпреступники, как и технологии, развиваются стремительно. Таким образом, очень важно использовать подход к кибербезопасности, который нацелен на предотвращение рисков и угроз еще до их возникновения. Здесь нет второго шанса, поэтому лучшая защита — предотвращение с помощью передовых технологий». ***(RoT-атаки: тактика нового поколения // IKSMEDIA.RU (http://www.iksmedia.ru/news/5680863-RoT-ataki-taktika-novogo-pokoleniya.html). 10.07.2020).***

***

«Новый стандарт кибербезопасности для интернета вещей (IoT) был представлен сегодня Техническим комитетом по кибербезопасности Европейского института телекоммуникационных стандартов (ETSI). Стандарт задает основы безопасности для устройств, подключенных к интернету, и будущих схем сертификации IoT. Стандарт получил название ETSI EN 303 645, и он призван предотвратить масштабные атаки на устройства, подключенные к интернету.

Разработанный в сотрудничестве с промышленностью, учеными и правительством, этот стандарт должен ограничить возможности киберпреступников к контролю устройств и запуску DDoS-атак, майнингу криптовалюты и сбору пользовательских данных. Эти проблемы становятся все серьезнее в связи со стремительным ростом количества интеллектуальных устройств в домашних хозяйствах, многие из которых имеют уязвимости.

К примеру, расследование, проведенное в этом году, выявило, что 3,5 миллиона беспроводных камер по всему миру потенциально имеют критические недостатки безопасности, позволяющие взломать их.

В стандарте ETSI EN 303 645 изложены 13 положений о безопасности для широкого спектра IoT устройств и связанных с ними услуг. К ним относятся детские игрушки и радионяни, детекторы дыма и дверные замки, интеллектуальные камеры, телевизоры и колонки, переносные устройства слежения за здоровьем, системы умного дома и сигнализации, подключенные к интернету бытовые приборы и умные домашние помощник». ***(Европейский институт телекоммуникационных стандартов установил новый стандарт***

кибербезопасности для IoT устройств // SecureNews (https://securenews.ru/european-telecommunications-standards-institute-has-set-a-new-cybersecurity-standard-for-iot-devices/). 01.07.2020).

***

Кіберзлочинність та кібертерроризм

«IP-адрес, с которого произошла новая кибератака на сайт Общественной палаты России, зарегистрирован на Украине, сообщили в ОП.

Хакеры заменили «несколько новостей о ходе общественного наблюдения за общероссийским голосованием» текстом «фейкового сообщения».

Это уже вторая атака на сайт за сутки, передает РИА «Новости…». ***(Антон Антонов. Хакеры атаковали сайт Общественной палаты России с украинского IP // Деловая газета «Взгляд» (https://vz.ru/news/2020/7/2/1047948.html). 02.07.2020).***

***

«Представники Facebook викрили мережі фейкових акаунтів у декількох країнах, враховуючи Україну. Про це повідомив глава політики кібербезпеки Facebook Натаніель Глейхер, інформує "Новое время".

Так, в Україні видалили 72 фейкових акаунти і 35 фейкових сторінок у Facebook, а також 13 фейкових Instagram-акаунтів. Загалом на ці акаунти були підписані майже 770 тис. користувачів.

Керівники фейкових сторінок маскували їх під незалежні акаунти і онлайн-медіа, а натомість публікували там неправдиву інформацію для маніпуляції даними та коментування своїх постів для їх просування на платформі.

Автори акаунтів використовували різні тактики, судячи з періодичної зміни назв фейкових сторінок, повідомляє Глейхер.

Він заявляє: "Адміністратори сторінок і власники акаунтів публікували політичні меми, сатиру та інший контент, зокрема про Крим, НАТО, економічну політику в Україні, внутрішню політику, вибори, критику і підтримку різних кандидатів, враховуючи Володимира Зеленського, Юлію Тимошенко і Петра Порошенка".

Фейкові сторінки були активні і під час президентських виборів в Україні у 2019-му.

За просування акаунтів у цій мережі відповідали PR-фірми, і всього на їх рекламу витратили майже $1,93 млн. Розслідувачі з Facebook пов'язують активність фейкових акаунтів з українським маркетинговим агентством Postmen.

Натаніель Глейхер пояснив, що методика розслідування фейків на платформах Facebook враховує автоматичний пошук підозрілої активності за допомогою інструментів компанії, а також співпраця з правоохоронними органами, журналістами і розслідувачів.

Повну версію звіту про викриття мережі фейкових акаунтів в Україні можна прочитати за цим посиланням…» ***(Facebook розкрив в Україні мережу фейкових***

акаунтів, які використовували для впливу на президентські вибори // 5 канал (https://www.5.ua/nauka/facebook-rozkryv-v-ukraini-merezhu-feikovykh-akauntiv-iaki-vykorystovuvaly-dlia-vplyvu-na-prezydentski-vybory-219036.html). 09.07.2020).

***

«Лаборатория Касперского» обнаружила по всему миру более тысячи неактивных доменов, которые используются злоумышленниками для перенаправления пользователей на нежелательные и вредоносные сайты. В 89% случаев это ресурсы с рекламой, однако в 11% при входе на такой домен пользователь затем попадает на страницы, где ему под благовидным предлогом предлагают установить вредоносный софт, в том числе троянец для macOS Shlayer, скачать зараженные документы Microsoft Office или, например, PDF-документы со ссылками на мошеннические ресурсы.

Обычно пользователи, которые пытаются зайти на неработающие страницы, видят заглушку, но в данном случае они автоматически перенаправляются на нежелательный или вредоносный ресурс, причем не всегда на один и тот же. Так, в совокупности с найденной тысячей страниц перенаправление шло на более 2,5 тыс. нежелательных сайтов.

Злоумышленники, возможно, получают оплату за каждый переход пользователя – как на легитимные рекламные страницы, так и на те, с помощью которых распространяются вредоносные программы. Одна из таких страниц получила 600 редиректов за 10 дней. В случае же с троянцем Shlayer оплата, по всей видимости, производилась за каждую установку на устройстве.

Используется сложная схема, поскольку сами по себе домены, которые используют злоумышленники, являются легитимными, и часть посетителей может зайти на них, набрав адрес по памяти, а также щелкнув по ссылке в окне «О программе» используемого приложения либо найдя их с помощью поисковых систем. Узнать, в каких случаях перенаправление будет идти на страницы, которые загружают вредоносное ПО, невозможно, и предотвратить опасные переходы самостоятельно, без помощи защитного решения, пользователь не может». ***(Мошенники используют неактивные домены для распространения вредоносов // Компьютерное Обозрение (https://ko.com.ua/moshenniki_ispolzuyut_neaktivnye_domeny_dlya_rasprostraneniya_vredonosov_133679). 09.07.2020).***

***

«Компания ESET сообщает о росте атак с использованием метода подбора пароля до 100 000 в день во время перехода компаний на режим хоум-офиса.

До изменений, вызванных пандемией, большинство организаций функционировали под контролем ИТ-отдела. Теперь многие из них предоставляют сотрудникам удаленный доступ к корпоративной сети и конфиденциальным данным с домашних устройств при помощи RDP. В результате в безопасности компаний открывается брешь. Персонал нередко использует ненадежные пароли, которые легко подобрать, а значит сеть становится еще более уязвимой для

киберпреступников. Проблема усугубляется при отсутствии дополнительной защиты в виде средства двухфакторной аутентификации.

Согласно телеметрии ESET, большинство заблокированных IP-адресов в январе-мае 2020 года были обнаружены в США, Китае, России, Германии и Франции. Россия заняла первое место по количеству уникальных атак, обнаруженных ESET. Далее в рейтинге — Германия, Япония, Бразилия и Венгрия.

Однако несанкционированный доступ к системам организации — лишь первый шаг, за которым следуют более серьезные действия киберпреступников. Так, RDP стал популярным вектором атак, особенно среди групп, которые занимаются распространением вирусов-вымогателей. Злоумышленники часто пытаются проникнуть в плохо защищенную сеть, получить права администратора, отключить или удалить решения безопасности, а затем запустить вредонос для шифрования значимых корпоративных данных.

Кроме того, преступники могут установить криптомайнер и даже создать бэкдор, который будет работать даже в случае выявления и прекращения несанкционированного доступа к RDP.

ESET призывает службы безопасности компаний тщательно проверить настройки RDP. Защитить корпоративную сеть от несанкционированного доступа поможет надежное средство двухфакторной аутентификации. Предотвратить попадание вредоносов в корпоративную сеть можно с помощью комплексных антивирусных бизнес-решений». ***(Ежедневно около ста тысяч компьютеров подвергаются атакам методом подбора пароля // IKSMEDIA.RU (http://www.iksmedia.ru/news/5679451-Ezhednevno-okolo-sta-tysyach-kompyu.html). 02.07.2020).***

***

«…по данным Verizon, более 40% кибератак направлено на малый бизнес. Небольшие игроки не могут позволить себе прерывать свою деятельность — и сейчас это важнее, чем когда-либо. Инвестирование в инфраструктуру для обеспечения кибербезопасности может приводить к существенной экономии в будущем, но важно знать, к чему готовиться. Понимание, какими бывают киберугрозы — это первый шаг к защите от них.

О шести самых распространённых кибератаках изданию Entrepreneur рассказал Рашан Диксон, сооснователь консалтинговой компании Techincon и старший консультант Microsoft.

1. Программы-вымогатели (ransomware)

Программное обеспечение, которое публикует личные данные или наносит вред другим способом, пока пострадавший не заплатит «выкуп», быстро стало одной из самых больших угроз для малого бизнеса. По данным IBEX, компании с фокусом на ИТ-обучение и партнёра Verizon, на «вымогателей» приходится более четверти проблем, вызванных вредоносными программами.

Многие владельцы бизнеса предпочитают просто заплатить, чтобы всё вернулось в нормальное русло. Но кибератака может повториться.

Хотя антивирус необходим для предотвращения самых сложных атак, простое обновление операционной системы может сыграть важную роль в предотвращении ransomware-атак меньших масштабов.

2. Фишинг

Когда служба безопасности Microsoft предупреждает, что бизнесу угрожает «масштабная» фишинговая операция, вам, вероятно, следует обратить на это внимание. Фишинг — это любая попытка получить конфиденциальную информацию, выдавая себя за другого пользователя или администратора, и он широко распространён в современной цифровой экономике.

Единственный способ уберечь себя от фишинга — это защитить все внутренние коммуникации в вашей компании. Шифрование электронной почты, внимательность при работе с учётными записями, управление каналами дистрибуции — всё это абсолютно необходимо.

3. Кибератаки изнутри

Некоторые из самых известных хакерских скандалов в мире бизнеса, от Sony до Ashley Madison, произошли не по вине опытных хакеров — они зародились внутри компании. Как бы вы ни доверяли своей команде, достаточно одного разочарованного сотрудника, чтобы произошла утечка катастрофического объёма информации.

В отличие от других кибератак в списке, эту можно предотвратить не цифровыми способами, а человеческой заботой.

Открыто говорите своим сотрудникам о чувствительности данных, к которым они имеют доступ, и всегда будьте готовы выслушать, с какими трудностями сталкивается команда. Вы никогда не сможете полностью контролировать сотрудников, но всегда можете дать им возможность высказаться.

4. DoS и DDoS (Denial of Service и Distributed Denial of Service)

При атаках типа «отказ в обслуживании» злоумышленники с одного или нескольких устройств направляют на сайт вашего бизнеса чрезвычайно большие объемы трафика и серверные запросы, что приводит к полной остановке его функций. Компания в сфере информационной безопасности Corero сообщает, что большинство DoS-атак специально предназначены для нарушения деятельности малого бизнеса.

Увеличение ёмкости сервера и вычислительной мощности может смягчить последствия DoS-атак, но единственный способ предотвратить их — это инвестировать в цифровые продукты, которые останавливают атаки в самом начале.

5. Внедрение SQL-кода

Kingfisher Technologies сообщает, что 26% малых предприятий пострадали от SQL-инъекций в прошлом году, но это, вероятно, наименее обсуждаемая угроза в списке. По сути это означает вставку кода из языка SQL на сайт для манипулирования процессом извлечения данных.

Старые языки, такие как PHP, а также сайты и приложения, которые не обновляются регулярно, особенно подвержены таким атакам.

Предотвращение SQL-инъекций — это работа для профессионалов, но обновление инфраструктуры не будет лишним.

6. Атаки по электронной почте

Некоторые из киберугроз в этом списке могут исходить от электронных писем — это 91% киберпреступлений — так что особенно важно защищать вашу почту. Атаки по электронной почте не относятся к конкретному типу — это, скорее, метод.

Шифрование электронной почты — обязательно, но не стоит ограничиваться лишь этим. Убедитесь, что все сотрудники знают, что не нужно открывать вложения из электронных писем от людей вне вашей организации, и тщательно проверяйте адреса отправителей.

Сегодня угроза кибератак почти повсеместна, но это не значит, что вы ничего не можете с этим поделать. Инвестиции в цифровую защиту сейчас — это инвестиции в будущее». ***(Татьяна Петрущенкова. 6 киберугроз, которые не может игнорировать ваша компания // Rusbase (https://rb.ru/story/common-cyberattacks/). 05.07.2020).***

***

«В ближайшие десять лет основными киберугрозами будут финансовая преступность, шпионаж и кибертерроризм. Об этом сообщает РИА «Новости» со ссылкой на заявление гендиректора компании Group-IB Ильи Сачкова.

Эксперт отметил, что рынок киберпреступности меняется очень быстро, поэтому прогнозировать можно только на ближайшие один-два года.

Но если смотреть на десять лет вперед, то, по мнению Сачкова, финансовая преступность будет наиболее развитой и часто встречающейся.

«Как на мне могут заработать? Как у меня могут украсть? Ответы на эти два вопроса, если чуть-чуть раскрыть в виде такой мозговой карты, — полностью строят стратегию цифровой безопасности человека», — комментирует Сачков.

Специалист добавил, что вместе с тем будут развиваться политический, межгосударственный и корпоративный шпионаж, а также кибертерроризм». ***(Екатерина Кочкина. Глава Group-IB назвал основные киберугрозы ближайшего десятилетия // Rusbase (https://rb.ru/news/group-ib-cyberthreats/). 04.07.2020).***

***

«Ранним утром 2 июля 2020 года официальная учетная запись Департамента ситуационно-кризисного отдела МИД России была скомпрометирована. В итоге на протяжении более 12 часов аккаунт рекламировал продажу БД с данными россиян.

Неизвестные злоумышленники, взломавшие учетную запись МИД, опубликовали два сообщения, в которых заявили, что продают базу «Туристы база ЕПГУ актуальность июнь 2020 выплаты заграница». Речь, видимо, шла о туристах, которые находятся за границей и получают выплаты от России через Единый портал госуслуг. Хакеры отмечали, что «подлинность базы подтверждается данным твитом, также как и доступы к определенным аккаунтам».

Этот дамп, содержащий 115 000 строк, неизвестные оценили в 66 биткоинов, то есть примерно 42 млн рублей, и оставили в своем необычном «объявлении» jabber-аккаунт для связи.

В настоящее время сообщения взломщиков уже были удалены (архивную версию можно увидеть здесь), а МИД восстановил контроль над учетной записью. Официальный представитель министерства Мария Захарова сообщила изданию «Подъем», что аккаунт действительно взломали, и восстановить доступ быстро не получилось. Вскоре официальный комментарий об инциденте появился и в Twitter.

«В очередной раз мы видим, как сливаются в сеть государственные базы с чувствительными данными граждан. Мы неоднократно обращали внимание, что сбор, хранение и использование широким кругом лиц данных, включая биометрию, находится вне общественного контроля и накопление подобной конфиденциальной информации, особенно в максимально централизированном виде — грозит множественными рисками, включая утечки. К сожалению, госструктуры практически ничего не делают для исправления этой острой проблемы, более того — усугубляют е, вводя все новые и новые основания для сбора и безконтрольного накопления все большего количества персональных данных», — комментирует руководитель «РосКомСвободы» Артем Козлюк.

Руководитель компании DeviceLock Ашот Оганесян пишет в своем Telegram-канале, что хакеры, вероятно, рекламируют БД, слухи о которой ходят с июня текущего года. В объявлениях утверждалось, что база актуальна на июнь 2020 и в ней содержится примерно 115 000 строк. Эту базу хакеры оценивали в ту же баснословную сумму — 66 биткоинов…». ***(Мария Нефёдова. Twitter-аккаунт МИД РФ взломали, и он рекламировал продажу БД с данными россиян // Xakep (https://xakep.ru/2020/07/02/mid-hack/). 02.07.2020).***

***

«Компания ESET сообщила о росте брутфорс-атак. Во время пандемии и перехода компаний на режим хоум-офиса количество атак достигло 100 000 в день.

Исследователи объясняют, что до изменений, вызванных пандемией коронавируса, большинство организаций функционировали под контролем ИТ-отдела. Теперь же многие из них предоставляют сотрудникам удаленный доступ к корпоративной сети и конфиденциальным данным с домашних устройств при помощи RDP.

В результате в безопасности компаний появилась брешь. Персонал нередко использует ненадежные пароли, которые легко подобрать, а значит, сеть становится более уязвимой для киберпреступников. Проблема усугубляется отсутствием дополнительной защиты в виде средств двухфакторной аутентификации.

По данным ESET, в период между декабрем 2019 года и февралем 2020 года можно было наблюдать от 40 000 до 70 000 ежедневных атак. Тенденция к росту обозначилась в феврале, когда число брутфорс-атак достигло 80 000.

С тех пор значения неуклонно росли и превысили 100 000 в апреле и мае, то есть когда большинство стран с большим количеством заболевших COVID-19 были вынуждены ввести карантинные меры, а бизнес массово перешел на удаленную работу.

Согласно собранной ESET телеметрии, в январе-мае 2020 года большинство заблокированных IP-адресов, с которых осуществлялись атаки, были обнаружены в США, Китае, России, Германии и Франции. Россия заняла первое место по количеству уникальных атак, обнаруженных ESET. Далее в рейтинге — Германия, Япония, Бразилия и Венгрия.

Однако несанкционированный доступ к системам организации — лишь первый шаг, за которым обычно следуют более серьезные действия со стороны хакеров. Так, RDP стал популярным вектором атак, особенно среди хак-групп, которые занимаются распространением вымогателей.

Злоумышленники часто пытаются проникнуть в плохо защищенную сеть, получить права администратора, отключить или удалить решения безопасности, а затем запустить вредонос для шифрования значимых корпоративных данных. Кроме того, преступники могут установить майнер и даже создать бэкдор, который будет работать даже в случае выявления и прекращения несанкционированного доступа к RDP». ***(Мария Нефёдова. Брутфорс-атаки на RDP достигли отметки 100 000 попыток в день // Хакер (https://xakep.ru/2020/07/03/covid-rdp/). 03.07.2020).***

***

«Компания Microsoft через суд перехватила контроль над шестью доменами, которые были задействованы в различных фишинговых операциях, направленных против пользователей Office 365. Мошенники были активны с декабря 2019 года и в последнее время активно эксплуатировали темы пандемии и COVID-19…

Фишеры рассылали электронные письма компаниям, которые размещали почтовые серверы и корпоративную инфраструктуру в облаке Microsoft Office 365. Письма были составлены таким образом, будто они были написаны коллегой или доверенных деловым партнером жертвы.

Отмечается, что эта кампания была весьма необычной, так как злоумышленники не перенаправляли пользователей на фишинговые сайты, имитирующие страницу логина в Office 365. Вместо этого хакеры использовали документ Office. Когда пользователи пытались открыть этот файл, срабатывало перенаправление для установки вредоносного стороннего приложения Office 365, созданного злоумышленниками.

Если пользователь попадался на удочку мошенников и устанавливал приложение, хакеры получали полный доступ к его учетной записи Office 365, настройкам, файлам, содержимому электронных писем, спискам контактов, заметкам и так далее.

Microsoft пишет, что благодаря этому приложению, хакеры получали полный доступ к учетным записям пользователей, причем без хищения паролей, ведь вместо этого у злоумышленников был токен OAuth2.

К сожалению, по ряду причин это мошенничество было весьма успешным. Дело в том, что вредоносное приложение выглядело как официальное и настоящее, будто его действительно разработали в Microsoft. К тому же среда Office 365 ориентирована на модульность, и пользователи привыкли устанавливать

приложения на регулярной основе. Более того, ссылка на установку вредоносного приложения сначала приводила пользователей на официальную страницу логина Microsoft. Лишь после успешной аутентификации злоумышленники задействовали хитрый трюк и перенаправляли жертв на загрузку вредоносного приложения, создавая впечатление, будто жертвы используют легитимное ПО, проверенное Microsoft.

Исследователи считают, что за этой кампанией стояли как минимум два человека. Сначала фишеры эксплуатировали темы, связанные с бизнесом, но вскоре после начала пандемии перешли к письмам-приманкам, якобы содержащим документы, посвященные коронавирусу.

Хуже того, по словам корпоративного вице-президента Microsoft Тома Берта (Tom Burt), сторонние вредоносные приложения могли использоваться для анализа внутренней инфраструктуры жертв, а затем злоумышленники использовали собранную таким образом информацию для BEC-атак (Bussiness Email Compromise).

Обычно BEC-скам подразумевает под собой компрометацию легитимного почтового аккаунта одного из сотрудников компании. После этого злоумышленники используют эту учетную запись для рассылки поддельных писем сотрудниками той же компании или ее партнерам, и применяют социальную инженерию, убеждая их перевести средства на подставные счета, прикрываясь фальшивыми инвойсами и вымышленными сделками. Напомню, что похожим образом злоумышленники обманули Google и Facebook более чем на 100 млн долларов, а также известны случаи, когда для имитации голоса CEO использовались deepfake'и.» ***(Мария Нефёдова. Microsoft перехватила контроль над 6 доменами «коронавирусных» мошенников // Xakep (https://xakep.ru/2020/07/08/office-365-phishing-2/). 08.07.2020).***

***

«Исследователи безопасности из организации Privacy Affairs рассказали о распространенности и стоимости похищенных персональных данных и прочих нелегальных услуг на подпольных торговых площадках.

По словам экспертов, одними из наиболее распространенных товаров в даркнете являются данные кредитных карт. Они обычно указываются в формате CC|MM|YY|CVV|HOLDER_NAME|ZIP|CITY|ADDRESS|EMAIL|PHONE. Первые 4 раздела представляют собой данные о самой карте, а остальные — информацию о владельце счета.

Продавцы, как правило, предлагают гарантию в 80%, что карты будут работать или будут иметь заявленные денежные средства. Стоимость подобных данных может варьироваться от $15 до $65, в зависимости от карты и заявленного баланса.

Данные учетных записей PayPal оказались самыми распространенными в даркнете и стоят около $200 за одну запись с минимальным балансом в $100. Преступники также предлагают услуги по переводу денежных средств со взломанных аккаунтов.

Еще одним очень распространенным предметом для продажи являются руководства о том, как «обналичить» деньги — получить денежные средства таким образом, чтобы не вызвать подозрения у властей. Подобные руководства продаются всего за несколько центов.

Поддельные документы поставляются с рядом гарантий и доступны с любыми подробностями, выбранными покупателем. Имея всего несколько реальных сведений о ком-то, преступник может создать целый набор официальных документов, которые будут использоваться для всех видов мошеннических действий. Стоимость поддельных документов может варьироваться от $70 за американское водительское удостоверение до $1500 за паспорт гражданина США, Канады или Европы.

Поддельные банкноты также оказались чрезвычайно распространены. В основном на подпольных торговых площадках продают доллары, евро, фунты, канадские и австралийские доллары, а иногда продавец предоставляет гарантию на УФ-тест. «Качественные» подделки, как правило, стоят около 30% стоимости банкноты.

Предложения взломать аккаунты или продать доступ к ним встречаются относительно редко. Возможно, это связано с отсутствием спроса на продукт в сочетании с усилением мер безопасности. Киберпреступники, пытающиеся похитить учетные данные пользователей социальных сетей, в основном вынуждены прибегать к использованию методов социальной инженерии, которые требуют очень больших усилий при относительно низком уровне успеха.

Внедрение вредоносного программного обеспечения на устройство жертвы может обойтись покупателю от $70 до $6000 за 1 тыс. установок. Что касается осуществления DDoS-атак, то их стоимость подобной услуги варьируется от $10 до более $800 в зависимости от длительности атаки ***(1 час, 24 часа, 1 неделя или 1 месяц)». (Какие услуги и товары продают хакеры в даркнете в 2020 году? // SecurityLab.ru (https://www.securitylab.ru/news/509831.php). 09.07.2020).***

***

«Исследователи из Check Point предупреждают об активно растущей тенденции: хакеры маскируют фишинговые атаки на Google Cloud Platform (GCP). К примеру, была зафиксирована атака, начинавшаяся с того, что злоумышленники загружали на Google Drive PDF-документ, который содержал ссылку на фишинговую страницу. Там пользователю предлагалось войти в систему с помощью Office 365 или корпоративной электронной почты. Когда пользователь выбирал один из вариантов, появлялось всплывающее окно со страницей входа в Outlook. После ввода учетных данных пользователь получал отчет в формате PDF, опубликованный известной международной консалтинговой фирмой. На протяжении всего времени пользователь даже не испытывал подозрений: фишинговая страница размещалась в облачном хранилище Google.

Однако просмотр исходного кода фишинговой страницы показал, что большинство ресурсов загружаются с веб-сайта, принадлежащего злоумышленникам, prvtsmtp [.] com. Злоумышленники используют сервис Google Cloud Functions, который позволяет запускать код в облаке. Ресурсы на

фишинговой странице были загружены из экземпляра Google Cloud Functions без раскрытия собственных вредоносных доменов злоумышленников. Многие другие домены, связанные с этой фишинг-атакой, были привязаны к одному и тому же IP-адресу или к разным в одном и том же сетевом блоке.

Эксперты Check Point рекомендуют:

Проверяйте названия доменов, орфографических ошибок в электронных письмах или на веб-сайтах, незнакомых отправителей электронной почты;

Будьте осторожны с файлами, полученными по электронной почте от неизвестных людей, особенно если они просят сделать что-то такое, что вы обычно не делаете;

Убедитесь, что вы заказываете товары из оригинального магазина источника. Для этого нужно не переходить по ссылкам из электронных писем, а вместо этого найти нужного вам продавца в Google и открыть ссылку на странице результатов поиска;

Остерегайтесь «специальных» предложений. Предложение купить лекарство от коронавируса за $150 обычно не заслуживает доверия;

Убедитесь, что вы используете индивидуальный пароль для каждой учетной записи». ***(Хакеры используют облачные сервисы Google для маскировки фишинговых атак // Компьютерное Обозрение (https://ko.com.ua/hakery_ispolzuyut_oblachnye_servisy_google_dlya_maskirovki_fishingovyh_atak_133837). 22.07.2020).***

***

«Компания ESET сообщает о преступной кампании, нацеленной на пользователей WhatsApp. Злоумышленники рассылают фишинговые сообщения, используя бренд Nespresso.

Жертву приглашают перейти по ссылке и ответить на несколько вопросов, чтобы получить в подарок кофеварку.

После прохождения опроса сайт якобы обрабатывает результаты и сообщает, что пользователь может получить подарок. Однако появляется еще одно условие: требуется рассказать о промоакции как минимум 30 контактам WhatsApp. С помощью такого простого запроса злоумышленникам удается собрать максимальное количество данных о различных пользователях и расширить границы преступной кампании.

После того как пользователь поделился промоакцией со своими контактами, ему необходимо передать данные якобы для отправки подарка. Как только все этапы завершены, предпринимается попытка установить на устройство жертвы рекламное ПО, которое будет отправлять PUSH-уведомления и объявления. Также появится предложение поучаствовать в еще одном опросе и выиграть Macbook Pro.

В данном случае после завершения опроса пользователям предлагается отправить сообщения на 13 номеров, каждый из которых представляет международный сервис обмена СМС, которые взимают средства за подписку до тех пор, пока не будут отключены вручную.

Таким образом, как отмечается, фишинговые атаки способны нанести пользователям серьезный финансовый ущерб. Защититься от них поможет

соблюдение элементарных правил цифровой гигиены: необходимо всегда проверять достоверность подобных промоакций на официальном сайте бренда, не открывать ссылки и не скачивать вложения от незнакомых отправителей». ***(Пользователи WhatsApp вновь подверглись атаке фишинговыми сообщениями // Компьютерное Обозрение (https://ko.com.ua/polzovateli_whatsapp_vnov_podverglis_atake_fishingovymi_soobsheniyami_133932). 30.07.2020).***

***

«На прошлой неделе, 23 июля, стало известно, что взломаны серверы, обслуживающие сервисы Garmin, крупнейшего производителя фитнес-трекеров, смарт-часов и навигационного оборудования.

Пользователи устройств Garmin не смогли подключиться к своим экаунтам, партнеры компании также оказались отключены от корпоративной системы. Кроме того, перестал обновляться сервис для пилотов-любителей flyGarmin. Ко всему этому добавилось и то, что пользователи не могут дозвониться в службу поддержки.

До сих пор компания так и не дала развернутого комментария по возникшей ситуации, при том, что блокировка продолжается. При этом Garmin уверяет, что утечек и потерь пользовательских данных не произошло.

Согласно некоторым наблюдателям, серверы Garmin подверглись атаке вымогателей, запустивших вирус-шифровальщик WastedLocker. За этой кибератакой якобы стоит группа Evil Corp, имеющая российские корни. По непроверенной информации злоумышленники требуют десятки миллионов долларов за разблокировку файлов». ***(Сервисы Garmin подверглись взлому и до сих пор блокированы // Компьютерное Обозрение (https://ko.com.ua/servisy_garmin_podverglis_vzlomu_i_do_sih_por_blokirovany_133888). 27.07.2020).***

***

Діяльність хакерів та хакерські угруповування

«Задолго до того, как китайская компания Huawei добилась большого успеха в области технологий 5G, в начале 2000-х годов успешной разработкой беспроводных сетей, получивших название 4G и 5G, занималась крупная канадская компания Nortel. Однако успех Nortel не только приносил большой доход ее руководству, но также сделал компанию мишенью для конкурентов, пишет Bloomberg.

По данным издания, в конце 1990-х годов Канадской службе разведки и безопасности (Canadian Security Intelligence Service, CSIS) стало известно о «необычном трафике», указывающем на то, что хакеры из Китая похищают данные прямиком из штаб-квартиры Nortel в Оттаве.

«Мы отправились к Nortel в Оттаву и сказали их руководству: “Они выкачивают вашу интеллектуальную собственность”. Но они ничего не

предприняли», - цитирует Bloomberg Мишеля Жуно-Кацуя (Michel Juneau-Katsuya), в то время возглавлявшего азиатско-тихоокеанское подразделение CSIS.

В 2004 году хакеры взломали учетные записи высшего руководства Nortel. Воспользовавшись учетной записью старшего исполнительного директора компании Фрэнка Данна (Frank Dunn), злоумышленники отправили в Китай порядка 800 документов, в том числе презентации в PowerPoint, анализ убытков от продаж, проекты американских сетей связи и даже исходный код. Документы были переданы некой компании Shanghai Faxian, с которой у Nortel не было никаких сделок.

С помощью скрипта Il.browse киберпреступники «выкачивали» из компьютерных сетей канадской компании целые разделы: Product Development, Research and Development, Design Documents & Minutes и пр. Старший советник по системной безопасности Nortel Брайан Шилдс (Brian Shields) сравнил активность хакеров в то время с пылесосом. Спустя годы, Шилдс стал рассматривать сам взлом и неспособность Nortel принять адекватные меры как начало конца канадского техногиганта. По его словам, компания никогда не пыталась установить, как были взломаны учетные записи, и просто сменила пароли. Неудивительно, что они снова оказались взломаны. К 2009 году Nortel обанкротилась.

Кто стоял за взломом и какие именно данные были похищены, доподлинно не установлено. Тем не менее, как считают Шилдс и другие эксперты, занимавшиеся расследованием инцидента, к кибератаке причастно правительство КНР, стремившееся ослабить западных конкурентов и продвинуть свои технологические компании, в частности Huawei.

Согласно заявлению Huawei, компании не было ничего известно о взломе канадского техногиганта, она не имеет к нему никакого отношения и не получала никаких принадлежавших Nortel документов.

«Все очень просто и понятно. Nortel сгубил экономический шпионаж. Достаточно лишь посмотреть, кто стал Номером 1 в мире и как быстро», - заявил Шилдс». ***(Bloomberg: Своим успехом в развитии 5G Huawei может быть обязана кибершпионажу // SecurityLab.ru (https://www.securitylab.ru/news/509710.php). 03.07.2020).***

***

«Специалисты голландской ИБ-компании SanSec обнаружили, что северокорейская хак-группа Lazarus (она же Hidden cobra) практикует веб-скимминг и взламывает интернет-магазины.

Напомню, что изначально название MageCart было присвоено одной хак-группе, которая первой начала внедрять веб-скиммеры (вредоносный код) на страницы интернет-магазинов для хищения данных банковских карт. Но такой подход оказался настолько успешным, что у группировки вскоре появились многочисленные подражатели, а название MageCart стало нарицательным, и теперь им обозначают целый класс подобных атак. И если в 2018 году исследователи RiskIQ идентифицировали 12 таких группировок, то к концу 2019 года, по данным IBM, их насчитывалось уже около 40.

В ходе подобных атак хакеры обычно получают доступ к серверу интернет-магазина, каким-либо связанным ресурсам или сторонним виджетам, и получают возможность загружать и запускать вредоносный код.

Обычно веб-скиммер загружается только на странице оформления заказа и автоматически похищает данные платежной карты, когда пользователь вводит их при оформлении заказа. Эти данные отправляются на удаленный сервер злоумышленников, и хакеры собирают их, используют сами или и продают в даркнете.

Массовые атаки на интернет-магазины продолжаются примерно с середины 2018 года. Среди наиболее значительных жертв взломщиков за последнее время: компании Wongs Jewellers, Focus Camera, Paper Source, Jit Truck Parts, CBD Armour, Microbattery, Realchems и Claire's.

Свежий отчет SanSec связывает конкретные домены и IP-адреса, использованные для недавних MageCart-атак на американские магазины, с ранее известной хакерской инфраструктурой «правительственных» хакеров. Так, основатель SanSec Виллем де Грот (Willem de Groot) пишет, что собранные доказательства указывают на то, что за рядом атак на американские магазины стояла известная северокорейская хак-группа на Lazarus.

«Как же Hidden cobra получила доступ (к скомпрометированным магазинам), пока неизвестно, но злоумышленники часто используют фишинговые атаки (вредоносные электронные письма) для получения паролей сотрудников из сферы розничной торговли», — пишет эксперт». ***(Мария Нефёдова. Северокорейских хакеров связали с атаками MageCart // Xakep (https://xakep.ru/2020/07/07/lazarus-magecart/). 07.07.2020).***

***

«Twitter подтвердил, что хакеры использовали инструменты, которые, как предполагалось, были доступны только его собственному персоналу, чтобы отразить хакерскую атаку в среду.

В результате взлома появились сообщения о Бараке Обаме, Элоне Маске, Канье Уэсте и Билле Гейтсе, а также о других знаменитостях, которые твитнули мошенничество с биткойнами.

Twitter также сообщил, что преступники загрузили данные с восьми учетных записей.

Он отказался раскрыть их личности, но сказал, что ни один из них не был "проверен".

Это означает, что у них не было синей галочки, чтобы подтвердить свое право собственности, и, следовательно, они не были среди самых громких взломанных аккаунтов.

Однако тот факт, что злоумышленники смогли использовать инструмент загрузки данных Twitter, означает, что теперь они потенциально могут получить доступ к уязвимым пользователям:

- личные личные сообщения, включая фотографии и видео
- контакты, которые приложение Twitter импортировало бы из своих адресных книг смартфона

- история физического местоположения, регистрируемая в периоды использования сервиса
- сведения об аккаунтах, которые они отключили и заблокировали

Интерес и демографическая информация, которую Twitter вывел о них, используя их платформу

В качестве дальнейшего развития New York Times предположила, что социальная сеть стала доступной после того, как хакеры получили доступ к учетным данным, которые были предоставлены на внутреннем канале обмена сообщениями Slack в Twitter - сервисе, который некоторые компании используют в качестве альтернативы электронной почте.

Газета также предполагает, что по крайней мере двое из причастных были из Англии.

В общей сложности в Твиттере говорится, что было взято 130 учетных записей, из которых хакерам удалось сбросить 45 паролей, предоставив им контроль.

Он добавил, что, по его мнению, виновные, возможно, пытались продать некоторые из украденных имен пользователей.

«Злоумышленники успешно манипулировали небольшим количеством сотрудников и использовали свои учетные данные для доступа к внутренним системам Twitter», - говорится в сообщении.

«Мы продолжаем расследование этого инцидента, работаем с правоохранительными органами и определяем долгосрочные действия, которые мы должны предпринять для повышения безопасности наших систем».

Он добавил: «Мы смущены, мы разочарованы, и больше всего, мы сожалеем».

Как развернулась атака?

Твиттер сказал, что злоумышленники преследовали определенных сотрудников Твиттера через «схему социальной инженерии».

«В этом контексте социальная инженерия - это преднамеренное манипулирование людьми для выполнения определенных действий и разглашения конфиденциальной информации», - говорится в заявлении.

По его словам, небольшое количество персонала было успешно манипулировано.

Оказавшись во внутренних системах Twitter, хакеры не могли видеть предыдущие пароли пользователей, но могли получить доступ к личной информации, включая адреса электронной почты и номера телефонов, поскольку они видны сотрудникам с помощью внутренних инструментов поддержки.

Они также могли просматривать дополнительную информацию, говорится в сообщении компании. Было предположение, что это может включать прямые сообщения.

Личные сообщения Kanye West, Kim Kardashian West или Elon Musk могут стоить денег на темных веб-форумах. Продажа личных сообщений кандидата в президенты Джо Байдена или бывшего мэра Нью-Йорка Майкла Блумберга также может иметь политические последствия.

Непонятно, почему хакеры не загрузили все данные этих аккаунтов знаменитостей, а сделали это для других.

Твиттер «активно работает над непосредственным общением» с затронутыми пользователями, говорится в его заявлении. Он также продолжает восстанавливать доступ для других пользователей, которые по-прежнему заблокированы в своих учетных записях, в результате первоначальной реакции фирмы на взлом.

Что случилось во время взлома?

15 июля ряд аккаунтов, связанных с биткойнами, начали твитнуть то, что казалось простой мошенничеством с биткойнами, обещая «отдать» сообществу, удвоив любой биткойн, отправленный на их адрес.

Затем явное мошенничество распространилось на такие известные аккаунты, как Ким Кардашьян Уэст и Джо Байден, а также корпорации Apple и Uber.

Твиттер взломал, чтобы сдержать беспрецедентную атаку, временно не позволяющую всем проверенным пользователям - тем, у кого на аккаунтах есть отметки синего цвета - твитнуть.

Тем не менее, президент США Дональд Трамп, один из самых известных пользователей Twitter, не пострадал.

В течение некоторого времени ходили слухи, что президент Трамп имеет дополнительные средства защиты после того, как его аккаунт был деактивирован сотрудником в последний день его работы в 2017 году .

The New York Times подтвердила, что именно так аккаунт мистера Трампа избежал атаки , сославшись на анонимного чиновника Белого дома и отдельного сотрудника Twitter.

Несмотря на то, что мошенничество было очевидным для некоторых, злоумышленники получили сотни переводов на сумму более 100 000 долларов США (80 000 фунтов стерлингов).

Что мы знаем о злоумышленниках?

Биткойн чрезвычайно трудно отследить, и три отдельных кошелька криптовалюты, которые использовались киберпреступниками, уже опустошены.

Цифровые деньги, вероятно, будут разбиты на меньшие суммы и проходить через так называемые «микшерные» или «тумблерные» сервисы, чтобы еще сложнее отследить злоумышленников.

Подсказки о виновных всплыли в хвастовстве в социальных сетях, в том числе в самом Твиттере.

Ранее на этой неделе исследователи из аналитической компании по киберпреступности Hudson Rock заметили на хакерском форуме рекламу, в которой утверждается, что она может украсть любую учетную запись Twitter, изменив адрес электронной почты, с которым она связана.

Продавец также разместил скриншот панели, обычно предназначенной для высокопоставленных сотрудников Twitter. Похоже, что позволяет полностью контролировать добавление электронной почты к учетной записи или "отключение" существующих.

Это означает, что злоумышленники имели доступ к серверной части Twitter по крайней мере за 36-48 часов до того, как в среду вечером начали появляться мошеннические биткойны.

Исследователи также связали по крайней мере один аккаунт в Твиттере с взломом, который сейчас заблокирован». ***(Twitter says hackers downloaded private account data // BBC (https://www.bbc.com/news/technology-53455092?intlink_from_url=https://www.bbc.com/news/topics/c347w30eq7xt/computer-hacking&link_location=live-reporting-story). 18.07.2020).***

***

«Сьогодні, 29 липня, стало відомо, що компанія яка займається питаннями кібербезпеки Recorded Future опублікувала доповідь, в якій стверджує, що група хакерів, імовірно пов'язаних з урядом Китаю зламала комп'ютерну мережу Ватикану.

Хакери користувалися тими ж методами злому, якими зазвичай користуються хакерські угруповання, які працюють на владу КНР. Здійснювались хакерські атаки на комп'ютери католицької церкви угрупованням RedDelta, яке спонсорується урядом Китаю, впевнені експерти компанії, пише "Коммерсантъ".

Хакерські атаки почалися ще у травні. Метою хакерів був як Ватикан так і Дослідницька місія Святого Престолу в Китаї — група дипломатів, які представляють церкву в Гонконзі й ведуть переговори з китайською владою про статус церкви в Китаї. Попередня угода між Ватиканом і Китаєм була укладена в 2018 році, термін її дії закінчується в цьому році. Нові переговори імовірно мають відбутися у вересні і саме з ними, на думку Recorded Future, пов'язані хакерські атаки.

Метою атак, можливо, було дізнатися, на які умови розраховує церква напередодні нового раунду переговорів.

Китайська сторона відкинула всі звинувачення. За повідомленням Reuters, представник МЗС КНР Ван Вэньбинь заявив, що Китай виступає проти хакерської діяльності і є "вірним захисником" основ кібербезпеки. Він додав, що при розслідуванні хакерських атак необхідно керуватися неспростовними доказами, а не гіпотезами…» ***(Китайці зламали комп'ютерні мережі Ватикану // Дзеркало тижня. Україна (https://zn.ua/ukr/WORLD/kitajtsi-zlamali-kompjuterni-merezhi-vatikanu.html). 29.07.2020).***

***

«У ніч на п’ятницю хакери атакували сайти міністерства освіти і науки та міністерства охорони здоров'я Північної Македонії, доступ до ресурсів був заблокований…

На сайтах з’явився чорний фон з текстом та зображенням Anonymous в масці. Відповідальність за хакерську атаку взяла на себе група AnonOpsMKD.

Раніше це об'єднання хакерів направило звернення македонським партіям, що пройшли до парламенту на виборах 15 липня, в якому заявила, що в разі призначення керівником уряду країни албанця вони "перевернуть Македонію".

"Якщо ДУІ (албанський "Демократичний союз за інтеграцію") змусить вас обрати прем'єр-міністром албанця, ми перевернемо всю Македонію з ніг на голову, і протягом 24 годин влаштуємо в країні кінець світу. Не жартуйте з македонським народом...Чекайте нас", - підкреслюється в заяві AnonOpsMKD.

"Ми - не росіяни, не китайці, не угорці, ми - примари, яких вам ніколи не знайти. Наша IP-адреса знаходиться на Марсі, і шукати її марно", - зазначили хакери.

Парламентські вибори у Північній Македонії відбулися 15 липня. Під час голосування хакерської атаки зазнали сайти Державної виборчої комісії та деяких ЗМІ. AnonOpsMKD стверджує, що до кібератаки на ДВК причетні хакери з Косова.

Згідно з неофіційними результатами голосування, коаліція під керівництвом Соціал-демократичного союзу Македонії (СДСМ) "Можемо" здобула 46 депутатських мандатів, коаліція ВМРО-ДПМНЄ ("Внутрішня македонська революційна організація - Демократична партія македонської національної єдності") - 44, ДУІ -15, Альянс для албанців та Альтернатива - 12, "Левица" - 2 та "Демократична партія албанців" (ДПА) - 1.

За таких результатів СДСМ може сформувати урядову коаліцію з ДУІ.» ***(Хакери атакували урядові сайти Північної Македонії // Європейська правда (https://www.eurointegration.com.ua/news/2020/07/24/7112489/). 24.07.2020).***

***

Вірусне та інше шкідливе програмне забезпечення

«Android підтримує в п'ять разів більше смартфонів і планшетів, ніж iOS. В результаті кількість додатків в Google Play Store значно вище, ніж в Apple App Store, і це робить процес перевірки додатків менш суворим для Android. Як і очікувалося, це дозволяє багатьом шкідливим програмам набагато легше проходити процес перевірки і залишатися в магазині Play Store до тих пір, поки їх не видалять за наявність вірусів. Google, однак, оперативно видаляє шкідливі програми, особливо коли мова йде про серйозні звинувачення, таких як фішинг. Згідно з недавнім звітом, інтернет-гігант в даний час закрив 25 додатків для обману користувачів та реєстрації облікових даних Facebook…

Французьке агентство кібербезпеки Evina нещодавно повідомило в Google про 25 шкідливих програмах для злому облікових даних користувачів Facebook. Це було досягнуто шляхом створення підробленої сторінки входу поверх фактичної сторінки входу в Facebook. Шкідливі елементи були замасковані під функціонал в додатках.

Французький агент також повідомив ZDNet, що деякі з цих шкідливих програм були в магазині Google Play більше року. Google видалив їх після перевірки результатів на початку червня…» ***(Николай Олефиренко. Google Play кишить вірусами, 25 додатків потрібно терміново видалити зі смартфона // Знай.ua (https://techno.znaj.ua/322564-google-play-kishit-virusami-25-dodatkiv-potribno-terminovo-vidaliti-zi-smartfona).08.07.2020).***

***

«Компания Avast обнаружила, что использование шпионских программ (в том числе и тех, которые установлены незаметно от пользователя) в мире

увеличилось на 51% в период карантина в марте-июне, по сравнению с январем-февралем.

Stalkerware (шпионское, сталкерское) – неэтичное ПО, которое позволяет людям отслеживать местоположение другого человека, получать доступ к его личным фотографиям и видео, перехватывать электронные письма, текстовые сообщения и сообщения в мессенджерах, например в таких как WhatsApp и Facebook, а также прослушивать телефонные звонки и делать скрытые записи разговоров через Интернет. Как правило, такие программы тайно устанавливают на смартфоны жертв ревнивые супруги, бывшие партнеры, заинтересованные родители, иногда даже друзья.

Примечательно, что среди всего спектра сталкерского ПО Avast также обнаружил ряд приложений, с темой COVID-19, которые были предназначены для шпионажа за пользователями. Они собирали больше информации, чем требовалось для их функционирования.

Нередко смартфоны остаются незащищенными по вине самих пользователей. По данным Pew Research, более четверти мобильных пользователей не используют защиту блокировки экрана на своих смартфонах, и чуть более половины не используют ни отпечатки пальцев, ни PIN-коды для обеспечения конфиденциальности своих устройств. Это дает возможность посторонним незаметно установить шпионское приложение. Ведь это занимает менее минуты». ***(Активность шпионских приложений в период карантина выросла в полтора раза // Компьютерное Обозрение (https://ko.com.ua/aktivnost_shpionskih_prilozhenij_v_period_karantina_vyrosla_v_poltora_raza_133688). 10.07.2020).***

***

«Шанс для домашних устройств столкнуться с любым типом вредоносных программ для ПК равен 25,6% в 2019 году по сравнению с 20,1% в 2018 году.

Такие данные опубликованы в отчете Avast Global PC Risk Report 2020, подготовленном компанией Avast.

Домашние устройства по всему миру с вероятностью 6,7% могут стать мишенью для продвинутых угроз. Это на 20% больше, чем годом ранее — тогда коэффициент риска составлял 5,6%. Avast определяет продвинутые угрозы как новые, ранее не замеченные разработчиками антивирусного ПО угрозы, разработанные для обхода распространенных технологий защиты, включенных в программное обеспечение безопасности, таких как сигнатуры, эвристика, эмуляция, фильтрация URL-адресов и сканирование электронной почты.

В России вероятность того, что домашнее устройство столкнется с угрозой любого типа, за год увеличилась на 7,7% с 20,36% до 21,93%. Россияне с вероятностью 9,90 % столкнулись с продвинутой угрозой — этот показатель увеличился на 47,5% по сравнению с предыдущим годом, где коэффициент риска составлял 6,71%.

«Наши отчеты за 2020 год показывают, что риск столкнуться с угрозой увеличился для всех устройств по всему миру. Количество подключенных

устройств продолжает заметно увеличиваться. Также этот отчет показывает, что компьютеры остаются уязвимыми — а они составляют важную часть цепочки атак, — рассказывает Луис Корронс, ИБ-евангелист Avast. — Киберпреступники создают угрозы, которые эксплуатируют действия пользователей. Они пользуются потенциальным отсутствием осведомленности о базовых правилах кибербезопасности — а значит, большинству людей жизненно важно установить решение безопасности на каждое устройство».

Топ-10 стран, в которых домашние устройства подвергаются наибольшему риску столкновения с угрозами, немного изменились с 2018 по 2019 гг. Венесуэла, Алжир, Сент-Люсия, Йемен и Ангола заменили Эфиопию, Египет, Вьетнам, Лаос и Мьянму». ***(Для домашних устройств увеличился риск столкнуться с киберугрозами // IKSMEDIA.RU (http://www.iksmedia.ru/news/5679380-Risk-dlya-domashnix-ustrojstv-stolk.html). 02.07.2020).***

***

«Исследователи информационной безопасности обнаружили новый вирус-шифровальщик для macOS, который распространяется через торрент-трекеры в пиратском ПО. Среди зараженного ПО удалось обнаружить популярную диджейскую программу Mixed In Key, программный пакет Google Software Update и программу для контроля приложений в macOS Little Snitch.

Вирус шифрует данные на компьютере пользователя, после чего выводит всплывающее окно с соответствующим сообщением и требованием перечислить выкуп в размере $50 в криптовалюте в течение 3 дней. При этом нет никаких контактов для обратной связи с преступниками для получения возможности дешифровать данные. Это позволяет предположить, что вирус не просто шифрует данные, а и вовсе стирает их.

Также сообщается, что вирус устанавливает на компьютер кейлогер, а также крадет любые файлы, связанные с криптовалютными кошельками.

Вирусу, первоначально называвшемуся EvilQuest, дали название OSX.ThiefQuest, чтобы избежать путаницы с компьютерной игрой EvilQuest. На данный момент специалисты изучают вирус и ищут пути борьбы с ним». ***(Новый вирус-шифровальщик для macOS распространяется через пиратское ПО // SecureNews (https://securenews.ru/new-ransomware-virus-for-macos-distributed-via-pirated-software/). 02.07.2020).***

***

«На этой неделе киберпреступники стали распространять новое вымогательское ПО Avaddon с помощью давно забытой техники. Для загрузки на атакуемую систему вредонос использует макросы Excel 4.0.

Как сообщают специалисты Microsoft Security Intelligence, шифровальщик Avaddon появился в начале июня и распространялся в масштабной спам-кампании, не нацеленной на какую-либо определенную категорию жертв. Сейчас операторы вымогательского ПО ищут партнеров для его распространения.

Avaddon использует надежное шифрование, и восстановить зашифрованные им файлы самостоятельно жертвы не могут. Как минимум один вариант вымогателя требует выкуп в размере $900.

По словам специалистовMicrosoft Security Intelligence, последняя спам-кампания нацелена исключительно на пользователей в Италии. Вымогательское ПО попадает на их системы через спам-письма с документом с вредоносными макросами Excel 4.0.

Одно из таких писем, обнаруженное исследователем безопасности JamesWT_MHT, было адресовано представителям малого бизнеса якобы Инспекцией по защите труда Италии. В его теме было указано, будто адресата ожидают штрафы и судебные иски за нарушения ограничительных норм для работников во время карантина. Письмо содержало ZIP-архив с названием «Официальное уведомление».

В свою очередь, документ содержал макросы Excel 4.0 (XML), до сих пор совместимые с современным ПО, где вместо них уже используется код VBA. После запуска макросы загружали Avaddon непосредственно на систему без использования загрузчика-посредника.

Использование макросов Excel 4.0 для распространения вымогательского ПО кажется немного странным, учитывая, что они были представлены в продуктах Microsoft Office 28 лет назад. Однако данная техника, похоже, все еще успешна». ***(Вымогательское ПО Avaddon распространяется через макросы Excel 4.0 // SecurityLab.ru (https://www.securitylab.ru/news/509720.php). 05.07.2020).***

***

«Операторы вымогательского ПО Sodinokibi (REvil) требуют выкуп в размере $14 млн от бразильской электроэнергетической компании Light S.A.

Хотя компания подтвердила факт кибератаки, она не представила никаких подробностей. Тем не менее, специалистам из AppGate удалось заполучить образец вымогательского ПО и выяснить, что злоумышленники использовали Sodinokibi.

Проанализировав вредонос, исследователи обнаружили данные о его операторах, идентификатор вредоносной кампании и URL-адрес, по которому жертвы должны связываться с киберпреступниками для дальнейших инструкций. На странице в даркнете, куда вел указанный URL-адрес, сказано, что до 19 июня жертва должна была заплатить вымогателям 106 870,19 XMR (Monero) – эквивалент порядка $14 млн. Также отчетливо упоминается название вредоноса – Sodinokibi.

По словам исследователей, атака выглядит очень «профессионально», а на странице даже присутствует чат для непосредственного общения с операторами вредоноса.

Sodinokibi распространяется по бизнес-модели «вымогательское ПО как услуга» (RaaS). Его оператором является киберпреступная группировка Pinchy Spider, также ответственная за распространение вымогательского ПО GandCrab. Как показал анализ вредоноса, он оснащен функцией повышения привилегий путем эксплуатации уязвимости CVE-2018-8453 в Windows». ***(Бразильская***

электроэнергетическая компания стала жертвой Sodinokibi // SecurityLab.ru (https://www.securitylab.ru/news/509688.php). 03.07.2020).

***

«Вымогатель Snake (он же EKANS) был впервые обнаружен ИБ-специалистами в январе 2020 года, и за прошедшие месяцы превратился в весьма распространенную угрозу для промышленных систем управления (ICS), так как малварь ориентирована на процессы, специфичные для этих сред. К примеру, в прошлом месяце сообщалось, что от атаки этого шифровальщика пострадала компания Honda.

Одной из особенностей Snake является ликвидация процессов из заранее подготовленного списка, включая процессы, связанные с ICS. Также известно, что малварь обычно похищает данные компаний, перед тем как приступить к шифрованию файлов, а затем операторы вымогателя требуют выкуп за эту информацию.

Теперь эксперты компании Deep Instinct рассказали еще об одной интересной особенности шифровальщика. Оказалось, что малварь старательно изолирует зараженные машины, чтобы никто не помешало процессу шифрования файлов. Для этого разработчики Snake «научили» свою малварь включать и отключать брандмауэр и использовать специальные команды для блокировки нежелательных подключений к системе.

«Перед началом шифрования Snake использует брандмауэр Windows, чтобы блокировать любые входящие и исходящие сетевые подключения к компьютеру жертвы, которые не числятся в настройках брандмауэра. Для этой цели используется встроенный в Windows инструмент netsh», — пишут специалисты.

Также малварь ищет процессы, которые могут помешать процессу шифрования, и ликвидирует их. Это касается процессов промышленных приложений, защитных инструментов и решений для резервного копирования. Snake также удаляет теневые копии, чтобы максимально затруднить восстановление данных.

Эксперты компании Fortinet, которые недавно тоже представили собственный отчет о Snake, отмечают, что завершив шифрование, малварь обычно отключает брандмауэр. Кроме того, исследователи Fortinet обратили внимание, что вымогатель предпочитает атаковать контроллеры домена, которые прицельно ищет в сети после изначального заражения. Для этих целей Snake использует WMI-запросы и определяет роли различных машин в сети.

Fortinet предупреждает, что если компрометация контроллера домена удалась, Snake получает возможность влиять на запросы аутентификации в сетевом домене, что может серьезно сказаться на пользователях». ***(Мария Нефёдова. Вымогатель Snake изолирует системы перед шифрованием // Xakep (https://xakep.ru/2020/07/06/snake-ransomware/). 06.07.2020).***

***

«Специалисты ESET обнаружили шпионскую программу Evilnum, нацеленную на финтех-компании и их клиентов, и рассказали об активности одноименной хакерской группы, существующей в 2018 года.

По данным исследователей, наибольшее количество атак Evilnum сосредоточено на территории стран ЕС и Соединенного Королевства, несколько атак также зафиксированы в Канаде и Австралии.

Малварь Evilnum ориентирована на хищение всевозможных конфиденциальных данных. Как и многие другие хакеры, специализирующиеся на финансовых целях, данная группа стремится проникнуть в корпоративные сети, получить доступ к учетным данным и похитить ценную финансовую информацию, которая затем может использоваться для мошеннических покупок или продается оптом другим преступникам. Так, Evilnum интересуют:

- информация о банковских картах клиентов и документы, удостоверяющие личность;
- электронные таблицы и документы со списками клиентов, сведениями об инвестициях и торговых операциях;
- внутренние презентаций компаний;
- лицензии на программное обеспечение и учетные данные для торгового ПО/торговых платформ;
- учетные данные электронной почты.
- Также операторы Evilnum могут собирать информацию, связанную с ИТ-инфраструктурой компании-жертвы, например, конфигурации VPN.

Интересно, что, по данным ESET, за разработкой малвари для группы Evilnum стоят хакеры из группы Golden Chickens, работающие по схеме малварь-как-услуга (malware-as-a-service). Эти же люди являются поставщиками вредоносных программ для таких известных хак-групп, как FIN6 и Cobalt.

Их инструменты включают в себя компоненты ActiveX (файлы OCX), содержащие TerraLoader, и дропер для других вредоносных программ, доступных клиентам Golden Chickens (например, бэкдор More_eggs и сложная RAT-малварь).

«Мы полагаем, что FIN6, Cobalt и Evilnum — это не одно и то же, несмотря на все совпадения в их наборах инструментов. Просто так случилось, что у этих группировок один и тот же поставщик MaaS», — пишут специалисты и отмечают, что пока группировку Evilnum вряд ли можно связать с другими известным APT.

Как правило атака Evilnum включает следующие этапы: пользователь получает фишинговое письмо со ссылкой на Google Drive, по которой можно скачать ZIP-файл. В этом архиве хранятся несколько LNK-файлов (ярлыков), которые извлекают и запускают вредоносный компонент JavaScript при отображении документа-приманки.

Файлы-приманки, в свою очередь, маскируются под весьма интересные вещи, а сами письма якобы написаны представителями технической поддержки и менеджерами по работе с клиентами. Как правило, файлы представляют собой различную KYC-информацию (Know Your Customer): фотографии банковских карт, документов, удостоверяющих личность, или счетов с подтверждением адреса, так как многие финансовые учреждения требуют от своих клиентов предоставить подобные данные.

По сути, если жертва открывает вредоносный документ, запускаются вредоносные программы Evilnum, инструменты написанные на Python и компоненты, созданные Golden Chickens. К примеру, упомянутый компонент JavaScript способен развернуть дополнительную малварь в системе жертвы. К тому же каждый из компонентов имеет собственный управляющий сервер и может действовать независимо.

Основная полезная нагрузка Evilnum направлена на сбор различной, уже упомянутой выше конфиденциальной информации, включая кражу и отправку на управляющий сервер паролей, сохраненных в Google Chrome, куки из Google Chrome, а также сохранение скриншотов». ***(Мария Нефёдова. Малварь для хак-группы Evilnum пишут те же люди, чьими услугами пользуются FIN6 и Cobalt // Xakep (https://xakep.ru/2020/07/10/evilnum/). 10.07.2020).***

***

«Лаборатория Касперского» с января 2019 года по апрель 2020 года обнаружила более 22 тыс. попыток заражения устройств вредоносными файлами, в названии которых упоминался Netflix.

«Злоумышленники добавляют названия популярных шоу в рекламные и вредоносные программы, а также используют их для проведения фишинговых атак», – передает РИА «Новости» сообщение антивирусной компании.

Уточняется, что чаще всего в качестве «приманки» злоумышленниками использовались сериалы «Очень странные дела», «Ведьмак», «Половое воспитание», «Оранжевый – хит сезона». В числе найденных вредоносных файлов были трояны с разного рода функционалом, позволяющие, например, удалять или блокировать данные, а также программы-шпионы, с помощью которых можно красть фотографии пользователей и пароли от онлайн-банкинга.

Кроме того, эксперты обнаружили вредоносное и нежелательное ПО, мимикрирующее под сервисы и онлайн-кинотеатры, популярные в России, такие как «КиноПоиск HD», Okko, IVI.

«Пользователи все активнее осваивают стриминговые сервисы. В период пандемии интерес к онлайн-кинотеатрам был особенно высоким, ведь многие из этих ресурсов открывали бесплатный доступ к большому количеству фильмов и сериалов. Популярность таких платформ злоумышленники стараются обернуть в свою пользу. Поэтому мы хотим напомнить, что лучше смотреть сериалы и фильмы на официальных площадках», – приводятся в сообщении слова эксперта по кибербезопасности Антона Иванова.

«Лаборатория Касперского» порекомендовала заходить на стриминговые ресурсы только через официальные сайты или приложения и не скачивать файлы с неофициальных ресурсов, а также установить надежное защитное решение.

Ранее «Лаборатория Касперского» проанализировала более 2 тыс. новых сайтов – из них 1,8 тыс. признаны потенциально опасными. Эксперты по цифровой безопасности предупредили пользователей Сети о резкой активизации хакеров.

В свою очередь премьер-министр Михаил Мишустин заявлял о «росте активности киберпреступников». По его словам, больше 90% успешных атак «проводятся с использованием методов социальной инженерии». ***(Александра***

Юдина. Появился новый вид мошенничества в интернете с помощью сериалов Netflix // Деловая газета «Взгляд» (https://vz.ru/news/2020/7/21/1051050.html). 21.07.2020).

***

«По оценкам «Лаборатории Касперского», как минимум с весны 2018 г. APT-группа Lazarus проводит атаки с использованием продвинутого фреймворка MATA. Его особенность заключается в том, что он может взломать устройство вне зависимости от того, на какой операционной системе оно работает, – Windows, Linux или macOS.

Мультиплатформенные вредоносные инструменты – редкость, так как их разработка требует значительных вложений. Соответственно, они создаются не для разового применения, а для долгосрочного использования. Так, этот фреймворк был замечен в атаках с целью краж баз данных компаний и заражения корпоративных сетей троянцами-шифровальщиками. Он состоит из загрузчика, программы для управления процессами после заражения устройства и плагинов.

По данным «Лаборатории Касперского», среди жертв MATA есть организации, расположенные в Польше, Германии, Турции, Южной Корее, Японии и Индии, в том числе производитель ПО, торговая компания и интернет-провайдер». ***(Группа Lazarus использует для атак мультиплатформенный фреймворк // Компьютерное Обозрение (https://ko.com.ua/gruppa_lazarus_ispolzuet_dlya_atak_multiplatformennyj_frejmvork_133854). 23.07.2020).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«В США официально предъявили обвинения казахскому хакеру, которого называют "невидимый бог сети"

Через две недели после того, как специалисты по кибербезопасности установили личность предполагаемого хакера из Казахстана, федеральные власти Сиэтла официально предъявили обвинения хакеру. Об этом сообщает Associated Press, информирует enovosty.com/news.

Мужчина, известный в хакерских кругах как «fxmsp», и его сообщники организовали хакерскую группу, которая совершила сотни хакерских атак на различные объекты, включая правительственные учреждения, школы, банки и сети роскошных отелей.

37-летний «fxmsp» находится в Казахстане. Американские прокуроры держали обвинительное заключение в тайне, чтобы не дать хакеру понять, что его разыскивают. Прокуратура США в Сиэтле написала, что теперь они считают, что «fxmsp» знает об уголовном расследовании, и, учитывая его публичную идентификацию, теперь нет причин держать обвинение в тайне». ***(В США***

официально предъявили обвинения хакеру, известному как "невидимый бог сети", - Associated Press // Экономические новости (https://enovosty.com/news_abroad/full/807-v-ssha-oficialno-predyavili-obvineniya-xakeru-kotorogo-nazyvayut-nevidimyj-bog-seti-associated-press). 08.07.2020).

***

«В Великобритании была проведена крупнейшая в истории британских правоохранительных органов операция по закрытию зашифрованного сервиса для общения EncroChat, используемого киберпреступниками. В ходе операции под названием Operation Venetic было произведено 746 арестов, а также изъято £54 млн наличными, 77 единиц огнестрельного оружия и более двух тонн наркотических веществ. Помимо Великобритании в операции участвовали правоохранительные органы Франции и Нидерландов, а также Европол.

EncroChat был одним из крупнейших в мире сервисов для зашифрованной связи (обмена сообщениями и телефонных звонков). Сервис насчитывал порядка 60 тыс. пользователей по всему миру, из них 10 тыс. в Великобритании. По данным Национального агентства по борьбе с преступностью Великобритании (NCA), EncroChat использовался исключительно для планирования и организации преступной деятельности, в частности для распространения нелегальных товаров, отмывания денег и подготовки убийств.

С 2016 года NCA вместе с правоохранительными органами других стран работало над отключением EncroChat и других сервисов, обеспечивающих зашифрованную связь. Два месяца назад партнерам NCA во Франции и Нидерландах удалось проникнуть в EncroChat и передать полученные данные в Европол, участвовавший в французско-нидерландском расследовании с 2018 года.

Без ведома пользователей сервиса NCA совместно с полицией осуществляло мониторинг каждого их действия. Уверенные в полной безопасности, преступники общались как ни в чем не бывало, однако в течение нескольких месяцев правоохранители перехватывали их коммуникации с помощью установленного на сетях EncroChat специального инструмента.

По словам представителей NCA, агентство создало технологию и обеспечило специальные возможности использования информации, необходимые для обработки данных EncroChat, а также для выявления и определения местонахождения правонарушителей путем анализа миллионов сообщений и сотен тысяч изображений.

Операторы EncroChat засекли правоохранительную операцию лишь 13 июня. Они разослали пользователям сообщения с просьбой выбросить свои телефоны. Эти телефоны стоимостью порядка £1,5 тыс. за штуку продавались с шестимесячным контрактом и предустановленными приложениями для мгновенного обмена сообщениями и VOIP-звонков. Кроме того, устройства были оснащены функцией самоуничтожения, позволяющей стирать все хранящиеся на нем данные…». ***(Правоохранители отключили зашифрованный сервис для общения EncroChat // SecurityLab.ru (https://www.securitylab.ru/news/509670.php). 03.07.2020).***

***

«Сотрудники правоохранительных органов Германии изъяли web-сервер сайта BlueLeaks, на котором хранились внутренние документы полицейских управлений США. Сервер принадлежал группе активистов DDoSecrets (Distributed Denial of Secrets), опубликовавшей более 1 млн файлов в середине прошлого месяца. Об изъятии сервера во вторник, 7 июля, сообщила одна из ключевых фигур BlueLeaks журналистка Эмма Бест (Emma Best).

«Мы получили официальное подтверждение того, что власти Германии (Прокуратура города Цвиккау, номер дела AZ 210 AR 396/20) изъяли основной публичный сервер загрузок DDoSecrets. Сервер использовался исключительно для предоставления данных общественности. У него нет контактов с источниками, и он участвовал только для просвещения общественности через журналистские публикации», - сообщила Бест в Twitter.

В настоящее время сайт BlueLeaks, работавший с 19 июня, отключен. На нем были опубликованы 296 ГБ внутренних данных двухсот полицейских участков США, предположительно предоставленных участниками движения Anonymous. Сюда входят сканированные копии документов, видео, электронные письма, аудиофайлы, учебные материалы, частные уведомления правоохранителей и другие документы. Данные предположительно были похищены у хьюстонского хостинг-провайдера, чьими услугами пользуются американские правоохранительные органы.

Через четыре дня после публикации похищенных документов учетная запись DDoSecrets в Twitter была заблокирована за нарушение правил пользования платформой, запрещающих публикацию ссылок на похищенные материалы. Кроме того, администрация Twitter начала блокировать твиты с ссылками на BlueLeaks.

Согласно заявлению американских властей, в прошлом месяце они изучали утечку данных BlueLeaks, но не подтвердили факт проведения официального расследования. Действовали ли сотрудники правоохранительных органов Германии по просьбе своих американских коллег (что весьма вероятно), в настоящее время неясно». ***(Власти Германии изъяли web-сервер сайта BlueLeaks // SecurityLab.ru (https://www.securitylab.ru/news/509799.php). 08.07.2020).***

***

«Американская прокуратура обвинила двух китайских граждан, которые, как говорят, работают в государственном разведывательном управлении Китая, за их предполагаемую причастность к масштабной глобальной хакерской операции, которая более десяти лет преследовала сотни компаний и правительств.

В обвинительном заключении из 11 пунктов, опубликованном во вторник, утверждается, что Ли Сяою, 34 года, и Донг Цзяжи, 33 года, похитили терабайты данных высокотехнологичных компаний со всего мира, в том числе из Соединенных Штатов, сообщили прокуроры.

Совсем недавно прокуроры обвинили хакеров в том, что они нацелены на сети более дюжины американских компаний в Мэриленде, Массачусетсе и Калифорнии, разрабатывающих вакцины и препараты для лечения COVID-19.

Обвинение было вынесено через несколько недель после того, как ФБР и Министерство внутренней безопасности предупредили, что Китай активно пытается украсть данные американских исследований, связанных с пандемией коронавируса.

Хакеры были впервые обнаружены после нападения на сеть Министерства энергетики США в Хэнфорде, штат Вашингтон. Хакеры также нацелены на компании в Австралии, Южной Корее и нескольких европейских странах. Хакеры использовали известные, но не исправленные уязвимости в широко используемом программном обеспечении веб-сервера, чтобы проникнуть в сети своих жертв. Утвердившись в сети, хакеры установили программное обеспечение для кражи паролей, чтобы получить более глубокий доступ к своим системам. Прокуроры заявили, что хакеры будут «часто» возвращаться в сети - в некоторых случаях спустя годы.

Согласно обвинительному заключению , хакеры похитили коммерческие секреты и интеллектуальную собственность стоимостью в сотни миллионов долларов. Обвинители также утверждают, что хакеры похитили данные, связанные с военными спутниковыми программами, военными беспроводными сетями и мощными микроволновыми и лазерными системами у оборонных подрядчиков.

Говорят, что хакеры преследовали своих жертв от имени разведывательных служб Китая, но также взламывали для получения личной финансовой выгоды. В одном случае прокуроры заявили, что хакеры «пытались вымогать криптовалюту» у компании-жертвы, угрожая опубликовать украденный исходный код жертвы в Интернете.

Джон С. Демерс, помощник генерального прокурора США по национальной безопасности, заявил, что обвинения являются «конкретными примерами» того, как Китай использовал хакеров для «грабежа, тиражирования и замены» некитайских компаний на мировом рынке.

Демерс также обвинил Китай в предоставлении убежища для хакеров.

«Китай занял свое место вместе с Россией, Ираном и Северной Кореей в этом постыдном клубе наций, которые предоставляют убежище для киберпреступников в обмен на то, что эти преступники находятся« на призыве »работать на благо государства, здесь чтобы накормить ненасытный голод Коммунистической партии Китая за трудную интеллектуальную собственность американских и других некитайских компаний, включая исследования COVID-19 », - сказал Демерс.

Mandiant, подразделение по реагированию на инциденты охранной фирмы FireEye, говорит, что отслеживает хакеров с 2013 года, и тактика, методы и процедуры, используемые хакерами, «согласуются» с его выводами.

«Китайское правительство давно полагалось на подрядчиков при проведении кибер-вторжений», - сказал Бен Рид, старший менеджер по анализу в Mandiant, по электронной почте. « Использование этих фрилансеров позволяет правительству получать доступ к более широкому кругу талантов, а также обеспечивает некоторую отрицательность при проведении этих операций».

«Схема, описанная в обвинительном заключении, когда подрядчики проводили одни операции от имени своих правительственных спонсоров, в то время как другие были за свою собственную прибыль, согласуется с тем, что мы

видели у других групп China-nexus, таких как APT41», - сказал он, обращаясь к Китайская передовая группа постоянных угроз, связанная с обвинительным заключением.

В случае судебного преследования каждый хакер может оказаться в тюрьме на срок более 40 лет. Но поскольку считается, что хакеры все еще находятся в Китае, любые экстрадиции в США маловероятны». ***(Zack Whittaker. US charges two Chinese spies for a global hacking campaign that targeted COVID-19 research // Verizon Media (https://techcrunch.com/2020/07/21/us-prosecutors-charge-chinese-spies-global-hacking/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAALXASnR_X483jL5nKQav0oMOGQQV04GnMNN5QmtFz6tK4PycQic9sJ9xPA_-ZqoUXfb4sGSZqkNpabDILIsQmM99LX8HyLHpG3pHlwrtkpFlsyYqrPlFkxH6ff1rUv3HiOkAx_q_Q1yOGb4xHWLEddjiEyp4Ch_27XGEcYx_nAzl). 21.07.2020).***

****

«В распоряжении издания Motherboard оказалась презентация с вебинара SpyCloud потенциальным клиентам, где компания заявила, что предоставляет следователям из правоохранительных органов возможность быстрее и эффективнее находить злоумышленников. SpyCloud подлинность слайдов подтверждает.

Должны ли правоохранительные органы использовать информацию, первоначально украденную хакерами? Покупая продукты у SpyCloud, правоохранительные органы также могут получить доступ к данным о людях, которые не замешаны в каких-либо преступлениях, и таких — подавляющее большинство. Некоторых экспертов тревожит, что правоохранительные органы получают возможность просто купить огромное количество информации, без какого-либо юридического процесса.

«В норме, если полиция хочет выяснить, скажем, какой IP-адрес связан с определённым аккаунтом, она должна пройти юридические процедуры в отношении поставщика услуг. Это обычное дело. Мы предъявляем эти требования к правоохранительным органам по веской причине», — сказала Риана Пфефферкорн, заместитель директора по надзору и кибербезопасности Стэнфордского центра интернета и общества.

На сайте SpyCloud любой желающий может зарегистрироваться по адресу электронной почты и затем посмотреть, какие утёкшие данные там имеются. В некотором смысле это коммерческая версия сервиса проверки скомпрометированных аккаунтов «Have I Been Pwned?». SpyCloud отличается тем, что позволяет объединять свои данные с исследовательским программным обеспечением, таким как Maltego, для облегчения установки связи между различными битами информации.

SpyCloud предлагает такой доступ и правоохранительным органам, позволяя им просматривать информацию о других людях. На одном из слайдов говорится, что данные могут быть использованы для «разоблачения конкретных преступников», включая определение их местоположения. По мысли соучредителя

и главного директора по продуктам компании Дейва Эндлера, данные, которые SpyCloud предоставляет правоохранительным органам, находятся в руках преступников и потому уже являются публичными.

SpyCloud также взламывает пароли. Наборы данных часто содержат только хэш или криптографический отпечаток пароля пользователя. После взлома следователь может увидеть, каким был пароль. Возможно, это полезно в установке связи между учётными записями, которые имеют общий пароль.

По словам Эндлера, среди клиентов из правоохранительных органов компании есть несколько федеральных служб. В 2018 Министерство юстиции поблагодарило SpyCloud за помощь.

Кевин Меткалф, глава Национальной целевой группы по защите детей, специализирующихся на борьбе с торговлей людьми, рассказал Motherboard, что утёкшие данные «обычно не используются и не понимаются, и на них пока тратится не так много времени». Но он добавил, что группа использует такую информацию, чтобы идентифицировать активных «хищников», которые скрываются от правоохранительных органов, пока охотятся на наиболее уязвимых членов общества.

SpyCloud также может быть полезна тем, кто занимается финансовыми преступлениями, считает Эндлер.

Многие компании, продающие информационные продукты коммерческому сектору, стали обслуживать и правоохранительные органы. Федеральные службы, включая иммиграционные и таможенные, приобретают данные о местоположении, собранные из приложений для смартфонов, которые обычно покупаются рекламными агентствами.

«Использование этих наборов утёкших данных сомнительно в плане этики, но совершенно привлекательно — как в случае злых, так и добрых намерений», — заключила Пфефферкорн.

Существует ряд юридических ограничений, которые не позволят правоохранительным органам просто покупать украденные данные у преступников и использовать их в расследованиях, пишет CPO Magazine. В судах многих юрисдикций использование незаконно полученных данных или доказательств прямо запрещено законом. Иногда компании действительно покупают такие данные, но их использование редко становится «официальным» и чаще служит различным «внутренним» целям, говорит Илья Колоченко, глава компании по информационной безопасности ImmuniWeb. Он сомневается, что правоохранительные органы бросятся покупать такую информацию: её легче запросить у технологических компаний через суд». ***(Motherboard: полиция покупает данные со взломанных сайтов // РосКомСвобода (https://roskomsvoboda.org/61790/). 24.07.2020).***

***

«Державний департамент США пропонує $1 млн винагороди за інформацію, яка допоможе заарештувати двох громадян України, яких розшукують за кіберзлочинність.

"Сьогодні Державний департамент США оголошує винагороду в розмірі до $1 млн (за кожного розшукуваного) за інформацію, що допоможе заарештувати та/або засудити громадян України Артема В'ячеславовича Радченка та Олександра Віталійовича Єременка за їхню участь у транснаціональній організованій злочинності, зокрема у кіберзлочинах", - йдеться в заяві для преси держсекретаря США Майка Помпео, оприлюдненій у середу на сторінці посольства США в Україні в соцмережі Facebook.

У заяві зазначено, що в січні 2020 року в результаті розслідування, проведеного Секретною службою США, було висунуто обвинувачення проти Радченка та Єременка за 16 статтями, зокрема в змові для вчинення шахрайства з цінними паперами, електронному шахрайстві і кібершахрайстві. Обвинувачення стверджує, що Радченко та Єременко зламали електронну систему збирання, аналізу та пошуку даних (EDGAR) Комісії з цінних паперів і бірж США і викрали тисячі конфіденційних файлів, які потім незаконно продали, щоб отримати прибуток. Комісія з цінних паперів і бірж США також подала позов, висунувши обвинувачення проти Єременка та інших фізичних і юридичних осіб.

"Це оголошення про винагороду зроблено в рамках програми TOCRP, за якою, разом з програмою Державного департаменту США з винагород за надання інформації про міжнародну наркоторгівлю, до відповідальності було притягнуто понад 75 транснаціональних злочинців з моменту започаткування цих програм у 1986 році. Державний департамент США виплатив понад $130 млн винагород за інформацію, що привела до зазначених арештів", - йдеться в повідомленні.

Бюро Державного департаменту США з міжнародних питань у сфері боротьби з незаконним обігом наркотиків і правоохоронних питань керує цими програмами винагород у тісній координації з Секретною службою США (USSS), Управлінням боротьби з наркотиками (DEA), Федеральним бюро розслідувань (FBI), Міграційною та митною правоохоронною службою США й іншими урядовими агентствами США.

"Ці дії демонструють прихильність Державного департаменту США підтримувати зусилля правоохоронних органів і загальнодержавний підхід до боротьби з транснаціональною організованою злочинністю", - йдеться в повідомленні». ***(Держдеп США оголосив винагороду у $1 млн за кожного з двох українських хакерів // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (https://day.kyiv.ua/uk/news/220720-derzhdep-ssha-ogolosyv-vynagorodu-u-1-mln-za-kozhnogo-z-dvoh-ukrayinskyh-hakeriv). 22.07.2020).***

****

Технічні аспекти кібербезпеки

«Велика ціна за знахідку критичних вразливостей зростає, оскільки Sony оголосила про свою власну програму винагород для PlayStation 4 (PS4) і PlayStation Network. Sony дасть хакеру 50 000 доларів, якщо йому вдасться виявити критичну вразливість, яка раніше не була виявлена.

“Ми запрошуємо співтовариство дослідників в області безпеки, геймерів і всіх, хто хоче перевірити безпеку PlayStation 4 і PlayStation Network”, - йдеться в заяві Sony після декількох тижнів подання Sony PS5.

“На сьогоднішній день ми запускаємо нашу програму винагород за помилки в приватному порядку з деякими дослідниками”, - повідомили в Sony.

Оголошення було зроблено після того, як Sony стала партнером з платформою безпеки HackerOne, платформою для координації вразливостей і усунення помилок, яка пов'язує підприємства з тестерами на проникнення і дослідниками кібербезпеки.

У програмі є два види винагород. 50 000 доларів сша будуть присуджені за виявлення критичної уразливості, а 3 000 доларів - за виявлення уразливості в мережі PlayStation Network…» ***(Николай Олефиренко. Sony озолотить будь-якого геймера за виявлення вразливостей PlayStation 4 // Знай.ua (https://techno.znaj.ua/322810-sony-ozolotit-bud-yakogo-geymera-za-viyavlennya-vrazlivostey-playstation-4). 09.07.2020).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«В последний день июня фирма Palo Alto Networks сообщила об опасной уязвимости, которая позволяет хакерам обойти аутентификацию в её межсетевых экранах и устройствах корпоративных VPN, работающих под управлением операционной системы PAN-OS.

Уязвимость получила наименование CVE-2020-2021 и довольно редкий наивысший рейтинг опасности — 10 из 10 по шкале CVSSv3. Киберкомандование США (US Cyber Command) считает, что иностранные хакерские группы с поддержкой на государственном уровне практически наверняка попытаются её использовать уже в ближайшие дни.

«Пожалуйста, немедленно исправьте все устройства, затронутые CVE-2020-2021, особенно если используется SAML (Security Assertion Markup Language)», — говорится во вчерашнем твит-сообщении US Cyber Command.

Инженеры из поддержки PAN говорят, что эта ошибка может быть использована только в том случае, если опция «Подтвердить сертификат поставщика удостоверений» отключена и одновременно включен язык разметки утверждений безопасности, SAML.

По умолчанию эти две настройки не находятся в уязвимых положениях — это означает, что не все устройства PAN-OS по умолчанию открыты для атаки, которая может привести к отключению брандмауэров или политик контроля доступа к виртуальной приватной сети.

Тем не менее, именно такие настройки рекомендованы владельцам устройств на основе PAN-OS, использующим сторонние решения для аутентификации, например, от провайдеров Centrify, Trusona или Okta,

В число продуктов Palo Alto Networks, которые поддерживают обе эти настройки, входят следующие устройства: GlobalProtect Gateway; GlobalProtect Portal; GlobalProtect Clientless VPN; Authentication and Captive Portal; брандмауэры следующего поколения (PA-Series, VM-Series) и веб-интерфейсы Panorama; системы Prisma Access.

По данным фирмы Bad Packets, просканировавшей 58521 доступный сервер Palo Alto (PAN-OS), 4291 из них использует SAML-аутентификацию какого-либо типа. Сканирование не показывает, выполнено ли в этих хостах второе условие (отключен Validate Identity Provider Certificate), но позволяет в первом приближении оценить масштабы угрозы». ***(Опасная уязвимость найдена в оборудовании для защиты корпоративных сетей // Компьютерное Обозрение (https://ko.com.ua/opasnaya_uyazvimost_najdena_v_oborudovanii_dlya_zashhity_korporativnyh_setej_133580). 01.07.2020).***

***

«На прошлой неделе мы рассказывали о крайне опасной RCE-проблеме, исправленной в конфигурационном интерфейсе популярного контроллера доставки приложений BIG-IP. Данная уязвимость была обнаружена экспертами Positive Technologies, получила идентификатор CVE-2020-5902 и набрала 10 баллов по шкале CVSSv3 (из 10 возможных), что соответствует наивысшему уровню опасности.

Многоцелевые сетевые устройства BIG-IP могут быть настроены для работы в качестве систем управления трафиком, балансировщиков нагрузки, брандмауэров, шлюзов доступа и так далее. Эти устройства являются одними из наиболее востребованных сетевых продуктов на сегодняшний день и используются в работе многих крупнейших и важнейших сетей. Так, девайсы BIG-IP работают в государственных сетях, в сетях интернет-провайдеров, в облачных ЦОД, а также во множестве корпоративных сетей.

Эксплуатируя найденный экспертами баг, злоумышленник получает возможность выполнять команды от лица неавторизованного пользователя и полностью скомпрометировать систему, например, перехватить трафик веб-ресурсов, которым управляет контроллер. Атака может быть реализована удаленно.

Аналитики Positive Technologies писали, что по состоянию на конец июня 2020 года в мире насчитывалось свыше 8000 уязвимых устройств, доступных из интернета, из них 40% — в США, 16% — в Китае, 3% — на Тайване, по 2,5% — в Канаде и Индонезии. В России было обнаружено менее 1% уязвимых устройств.

Уязвимость привлекла внимание множества ИБ-специалистов, и в силу ее серьезности даже Киберкомандование США выпустило соответствующее предупреждение, призвав всех как можно скорее установить патчи.

Теперь специалист NCC Group Рич Уоррен (Rich Warren) предупредил, что уязвимость уже находится под атаками. Специалисту принадлежат несколько honeypot-приманок, замаскированных под BIG-IP, и, по его словам, атаки на них начались через несколько часов после публикации предупреждения Киберкомандования США. Атаки исходили как минимум с пяти различных IP-

адресов: хакеры пытались похитить пароли администраторов с уязвимых устройств.

Дело в том, что ИБ-исследователи уже начали публиковать эксплоиты для уязвимости CVE-2020-5902, стремясь продемонстрировать, насколько легко используется этот баг, и как быстро с его помощью можно похитить данные или выполнить произвольные команды.

На GitHub уже появился репозиторий, где собраны PoC для выполнения различных задач, в том числе отображение файла /etc/passwd для доступа к сохраненным учетным данным, а также просмотр файла конфигурации уязвимых устройств.

Исследователи отмечают, что по масштабности данная проблема во многом похожа на RCE-уязвимости в Pulse Secure VPN и сетевых шлюзах Citrix. Такие баги очень популярны у злоумышленников и обычно используются ими, чтобы закрепляться в корпоративных сетях (после этого хакеры внедряют в сети организаций бэкдоры, крадут конфиденциальные файлы или разворачивают вымогательское ПО). К примеру, на такие уязвимости часто полагаются хак-группы REvil, Maze и Netwalker, что позволяет им компрометировать крупнейшие компании мира». ***(Мария Нефёдова. Начались атаки на уязвимость в F5 BIG-IP, в сети уже доступен PoC-эксплоит // Xakep (https://xakep.ru/2020/07/06/big-ip-attacks/). 06.07.2020).***

***

«В окружной суд Южного округа Нью-Йорка был подан коллективный иск против компаний Apple и T-Mobile за уязвимость в iMessage и FaceTime. Проблема заключалась в том, что долгое время сервисы Apple привязывались к номерам мобильных телефонов, в результате чего при повторном использовании номера данные абонента оказывались доступными для посторонних.

Согласно исковому заявлению , уязвимость была обнаружена в iMessage еще в 2011 году. Именно тогда стала появляться информация о том, что краденые iPhone получали сообщения в iMessage, адресованные настоящим владельцам. Проблема оставалась, несмотря на все предпринимаемые владельцами меры – смену номера учетной записи и Apple ID и удаленную очистку iPhone от содержимого с помощью инструментов безопасности iCloud.

По мнению истцов, проблема заключалась в том, как Apple обрабатывала идентификаторы устройств – протокол, обеспечивающий доставку сообщений в iMessage нужным пользователям.

«Говоря конкретно, когда пользователь iPhone переставал пользоваться SIM-картой, и оператор связи наподобие T-Mobile повторно использовал связанный с этой SIM-картой номер телефона, предыдущий владелец связанной с этим номером SIM-карты по-прежнему получал в iMessage и FaceTime на своем iPhone сообщения, предназначавшиеся новому владельцу этого номера», – говорится в исковом заявлении.

Насколько широко распространенной была проблема, неизвестно. Выпущенная в 2018 году версия iOS 12 устранила уязвимость, поскольку стала запрашивать двухфакторную аутентификацию для определенных сервисов iCloud.

Истцы требуют от Apple и T-Mobile компенсацию судебных издержек и ущерба, причиненного в результате вводящих в заблуждение действий, ложной рекламы, намеренного введения в заблуждение и несправедливого обогащения». ***(Пользователи подали в суд на Apple и T-Mobile за уязвимость в iMessage и FaceTime // SecurityLab.ru (https://www.securitylab.ru/news/509782.php). 07.07.2020).***

***

«Словенская ИБ-компания ACROS Security раскрыла уязвимость в ПО для конференцсвязи Zoom, позволяющую злоумышленнику удаленно выполнить код на компьютере, где установлен уязвимый клиент Zoom для Windows. Проблема затрагивает только пользователей устаревших версий ОС от Microsoft, в частности Windows 7, Windows Server 2008 R2 и более ранних. Пользователям Windows 8 и Windows 10 беспокоиться не о чем.

Как пояснил глава ACROS Security Митя Колсек (Mitja Kolsek), злоумышленник может удаленно выполнить код на системе с установленным клиентом Zoom для Windows, вынудив жертву произвести определенные действия (например, открыть файл документа). В процессе эксплуатации уязвимости никаких уведомлений и предупреждений об угрозе не отображается.

Уязвимость была обнаружена неизвестным исследователем безопасности, пожелавшим сохранить анонимность. Он сообщил о проблеме ACROS Security, которая в свою очередь уведомила о ней Zoom. ACROS Security также обновила свой клиент 0patch, добавив в него микропатч, закрывающий уязвимость в четырех разных частях кода в устаревших версиях Windows.

«Наши микропатчи уже выпущены и разосланы всем подключенным online приложениям 0patch Agent. Пользователей Zoom с установленным 0patch уязвимость больше не затрагивает», - сообщил Колсек…

Zoom уже работает над исправлением, но дата его выхода пока неизвестна. Никаких технических подробностей об уязвимости ACROS Security не представила. Также неясно, эксплуатировалась ли она в реальных атаках». ***(Критическая уязвимость в Zoom ставит под угрозу ПК с устаревшими версиями Windows // SecurityLab.ru (https://www.securitylab.ru/news/509857.php). 10.07.2020).***

***

«Компанія Digitpol, яка спеціалізується на проблемах кібербезпеки, опублікувала звіт китайського хакерського угруповання Team Pangu, яке виявило критичну уразливість в iPhone і iPad. Вона дозволяє зламати практично будь-який гаджет, вироблений компанією Apple, повідомляє «Популярная механика».

Суть уразливості полягає в тому, що ключовий механізм забезпечення безпеки гаджетів Apple - співпроцесор SEP (Secure Enclave Processor) — в ході свого «спілкування» з основним чіпсетом використовує спільну пам'ять. При роботі з нею, використовуючи раніше виявлений експлойт checkm8, можна обійти такі

бар'єри, як ліміт на кількість спроб введення пароля. В результаті, питання доступу до особистих даних на пристрої зводиться до простого перебору значень.

Наголошується, що уразливість присутня у всіх пристроях компанії, які були випущені на чіпсетах від A7 до A11, нові пристрої не схильні до неї і більш захищені. Але механізм взаємодії SEP з основними процесорними ядрами в чіпах A12 і A13 відрізняється від попередників не занадто радикально. Тому, ймовірно, що зловмисники зможуть знайти спосіб, щоб отримати доступ до пам'яті і більш нових пристроїв…». ***(Фаина Ваулина. Хакери знайшли спосіб зламати практично будь-який iPhone // Дзеркало тижня. Україна (https://zn.ua/ukr/TECHNOLOGIES/khakeri-znajshli-sposib-zlamati-praktichno-bud-iphone.html). 28.07.2020).***

***

«…Исследователи в области кибербезопасности компании Eclypsium обнаружили критическую уязвимость в загрузчике GRUB2, которая может подвергать опасности операционную систему устройства. Они назвали эту уязвимость BootHole. Она затрагивает любые устройства, использующее загрузчик GRUB2, в том числе в сочетании с технологией Secure Boot. Загрузчик GRUB2 является достаточно популярным решением. Он развёрнут на миллиардах компьютеров, серверов и практически на любом устройстве, использующем Unix-подобную операционную систему.

Уязвимость BootHole использует недостатки архитектуры двух ключевых компонентов GRUB2: bison (генератор парсера) и flex (лексический анализатор). Специалисты Eclypsium обнаружили, что эти два компонента могут иметь «несоответствующие проекту допущения», которые могут привести к переполнению буфера. Это переполнение буфера может быть использовано для выполнения произвольного кода.

Устройства с современными микропрограммами UEFI и активированным протоколом Secure Boot, как правило, не допускают к вмешательству в процесс загрузки даже привилегированных пользователей-администраторов. Однако в случае BootHole загрузчик анализирует файл конфигурации, расположенный в разделе EFI загрузочного устройства, который может быть изменен любым пользователем (или вредоносным процессом) с правами администратора.

Следует отметить, что исправленные версии загрузчика GRUB2 уже выпущены и начали распространяться. Так что осталось лишь дождаться, пока поставщики *nix-систем или производители серверов выпустят исправления для своих конечных пользователей. В частности, SUSE уже начала распространение исправления для всех версий SUSE Linux». ***(Вадим Карпусь. BootHole – новая уязвимость, которой подвержены миллиарды устройств с загрузчиком GRUB2 // ООО «ХОТЛАЙН» (https://itc.ua/news/boothole-novaya-uyazvimost-kotoroj-podverzheny-milliardy-ustrojstv-s-zagruzchikom-grub2/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+itc-ua+%28ITC.ua%29). 30.07.2020).***

***

«Компания ESET предупредила о рисках, связанных с выявлением ряда уязвимостей в технологии Thunderbolt, которые известные под названием Thunderspy. Используя их, злоумышленники могут изменить и даже выключить систему защиты интерфейса Thunderbolt на компьютере пользователя.

Как результат, киберпреступники с физическим доступом к определенному устройству способны похитить данные с него, даже в случае использования полнодискового шифрования и блокировки с помощью пароля или пребывания устройства в режиме энергосбережения. Уязвимости Thunderspy были обнаружены в мае 2020 года.

«Хотя об исследовании и стало известно общественности из-за интереса к новому вектору атаки, однако пока мало информации о том, как защититься или даже определить, не стали вы потенциальной жертвой», — отмечает Арье Горецкий, ведущий исследователь ESET.

Стоит отметить, что Thunderbolt — это интерфейс для обеспечения скоростных соединений между компьютерами и периферийными устройствами, такими как внешние накопители RAID, камеры, дисплеи с высоким разрешением и тому подобное.

Технология скоростных соединений Thunderbolt открывает новые возможности для киберпреступников. ESET.

Атаки с использованием Thunderbolt случаются редко, поскольку в основном они являются целенаправленными. «То, что типичный пользователь не является целью этой угрозы, не означает, что каждый находится в безопасности. Для многих соблюдение некоторых рекомендаций, описанных ниже, действительно имеет важное значение», — комментирует исследователь ESET.

Существует два типа атак, нацеленных на безопасность Thunderbolt. Первый вид предполагает копирование информации об устройствах Thunderbolt, которым компьютер уже доверяет. Второй тип связан с отключением безопасности Thunderbolt навсегда с невозможностью повторного включения.

«Атака с использованием копирования похожа на методы воров, которые похитили ключ и сделали копию. После этого они могут использовать скопированный ключ несколько раз для открытия замка. Вторая атака является формой отключения микросхемы. В этом случае окончательно выключается уровень безопасности Thunderbolt и обеспечивается защита от изменений для невозможности их отмены», — объясняет Арье Горецкий.

Обе атаки осуществить непросто, поскольку нужен личный доступ к устройству, а также инструменты для разборки компьютера, присоединение программатора, считывание встроенного программного обеспечения с микросхемы SPI flash ROM, изменение кода и запись обратно на микросхему.

Необходимость физического доступа к компьютеру сужает круг потенциальных жертв к особо важным целям. Жертвами могут стать руководители бизнеса, инженеры, административный персонал или другие сотрудники, если злоумышленник имеет коммерческий мотив, например, действует в целях промышленного шпионажа. В странах с репрессивными режимами целями таких

угроз, как Thunderspy, могут быть политики, общественные организации и журналисты.

Рекомендации ESET, которые помогут защитить Thunderbolt от кражи данных с использованием Thunderspy.

«Для защиты от подобных атак предотвратите любой несанкционированный доступ к компьютеру. Также позаботьтесь о защите всех соответствующих интерфейсов и портов, например, USB-C. Кроме этого, важно не ограничиваться физическими мерами безопасности, а обеспечить защиту встроенного и другого программного обеспечения», — рассказывает исследователь ESET.

Кроме этого, специалисты ESET подготовили ряд рекомендаций, которые помогут защититься от кражи данных с использованием Thunderspy.

Обновляйте операционную систему и встроенное программное обеспечение компьютера до актуальных версий. В случае с последним недостаточно ограничиваться только BIOS или UEFI. Также в обновлении нуждается встроенное ПО видеочипов, сетевых интерфейсов, сенсорной панели, контроллеров жидкокристаллических дисплеев. Кроме этого, смартфоны, планшеты, роутеры и модемы имеют собственное встроенное ПО, которое необходимо регулярно обновлять.

Ограничьте использование спящего режима или других гибридных режимов отключения, а лучше полностью выключайте компьютер, когда он не используется. Такие действия могут предотвратить атаки с использованием памяти устройства с помощью Thunderspy.

Используйте полнодисковое шифрование для внутренних накопителей и сменных носителей. Хотя по данным исследований технологию можно обойти, если компьютер заблокирован или находится в спящем режиме, однако полностью выключенное устройство оставалось в безопасности.

В случае покупки нового компьютера подумайте о приобретении устройства без DMA-интерфейсов, таких как порты Thunderbolt, ExpressCard и FireWire. Хотя они часто могут быть выключены при настройке встроенного ПО, злоумышленник с длительным доступом к устройству может попробовать их повторно включить.

Используйте надежное решение для защиты с возможностью сканирования интерфейса UEFI — одно из мест, где хранится информация о безопасности Thunderbolt». ***(Уязвимости в технологии Thunderbolt как новый вектор атак // Компьютерное Обозрение (https://ko.com.ua/uyazvimosti_v_tehnologii_thunderbolt_kak_novyj_vektor_atak_133962). 31.07.2020).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Компания Check Point Software Technologies объявила о запуске Infinity SOC – платформы, объединяющей возможности предотвращения,

обнаружения, расследования и устранения угроз для обеспечения высокой безопасности и эффективности работы.

Infinity SOC ежедневно применяется командами исследователей Check Point для выявления и изучения самых опасных и сложных кибератак в мире. Она использует анализ инцидентов на основе ИИ для фильтрации миллионов ненужных журналов и предупреждений, помогая группам безопасности предприятия выявлять и блокировать кибератаки с высочайшей скоростью и точностью.

Согласно данным опроса команд SOC, проведенного Dimensional Research, 68% респондентов заявили, что до половины событий, которые они анализируют, являются ложноположительными. В результате критические атаки часто остаются незамеченными, пока не станет слишком поздно. 98% профессионалов в области ИТ-безопасности сообщили о проблемах, связанных с SOC, причем основными операционными проблемами являются ручная работа, связанная с анализом и устранением инцидентов (по мнению 52%), точное определение наиболее критических событий (52%) и перегрузка журналов и оповещений (51%).

Платформа Infinity SOC от Check Point решает эти проблемы и помогает предприятиям защитить свои сети, предоставляя:

Высокую точность для быстрого прекращения реальных атак: платформа автоматически находит даже самые неявные атаки из миллионов ежедневных журналов и предупреждений, благодаря первому в отрасли анализу инцидентов ИИ. Infinity SOC автоматически включает оповещения, чтобы быстрее реагировать на критические атаки, и предлагает расследование одним щелчком мыши с помощью облегченного клиента на зараженном хосте. Infinity SOC не позволяет хакерам запускать фишинговые кампании против пользователей, блокируя запуск атак, создавая похожие корпоративные веб-сайты и почтовые домены.

Быстрое расследование инцидентов: Infinity SOC работает на основе ThreatCloud, крупнейшей в мире сети для совместной работы по борьбе с киберпреступностью, позволяющей командам быстро находить подробные последние данные по любому показателю компрометации, включая глобальное распространение, временные рамки, шаблоны атак, ДНК вредоносных программ и прочее. Это также включает в себя поиск по ссылкам в социальных сетях и OSINT для углубления расследований – в отличие от других решений, которые используют автономные базы данных угроз. Подозрительные файлы быстро проверяются с помощью технологии SandBlast threat emulation.

Моментальное развертывание: Infinity SOC – единая облачная платформа с централизованным управлением, которая повышает эффективность работы команд и снижает совокупную стоимость владения. Она развертывается за считанные минуты и позволяет избежать дорогостоящих проблем с хранением журналов и конфиденциальностью благодаря уникальному облачному анализу событий, который не экспортирует и не сохраняет журналы событий». ***(Платформа Check Point Infinity SOC использует анализ инцидентов на основе ИИ // Компьютерное Обозрение (https://ko.com.ua/platforma_check_point_infinity_soc_ispolzuet_analiz_incidentov_na_osnove_ii_133655). 08.07.2020).***

***

«Компания F5 Networks, предоставляющая корпоративным клиентам услуги по управлению сетевым трафиком, анонсировала новый сервис безопасности, защищающий веб-сайты от вредоносных ботов и других типов автоматизированных атак.

Полностью управляемая служба под названием Silverline Shape Defense, построена на базе технологии, которую F5 получила в декабре прошлого года, когда она купила компанию Shape Security, заплатив за последнюю около миллиарда долларов. Интеллектуальная платформа Shape Security широко использовалась авиакомпаниями, банками, правительственными агентствами и другими организациями для выявления мошенничеств. На момент приобретения с её помощью ежедневно регистрировалось более миллиарда поддельных транзакций.

По информации F5, Silverline Shape Defense использует алгоритмы искусственного интеллекта для выявления запросов, например, на авторизацию в приложениях и веб-сайтах, сделанных вредоносным ботом. Сервис призван блокировать мошеннический трафик, но при этом не создавать никаких неудобств для законных пользователей. Полная прозрачность действий Silverline Shape Defense с веб-трафиком позволяет клиентам контролировать, как осуществляется защита веб-сайтов от злоумышленников.

Этот инструмент защищает бизнес и от других угроз, в том числе от подстановки логинов/паролей, украденных на других ресурсах (credential stuffing), уменьшая риски ущерба для доходов и репутации бренда. Кроме того, он избавляет компании от необходимости тратить средства на содержание больших команд специалистов по информационной безопасности.

«Управляемые службы Silverline от F5 улучшают не только безопасность и производительность приложений, но и компенсируют нехватку квалифицированных специалистов по кибербезопасности, которые необходимы для противодействия новейшим киберугрозам в режиме реального времени», — сказала Гейл Коури (Gail Coury), вице-президент и генеральный менеджер F5 Silverline.

В пакет продуктов Silverline также входят межсетевой экран для веб-приложений, платформа аналитики угроз и средство защиты от распределённых атак методом отказа в обслуживании (DDoS)». ***(F5 Networks выпускает новое решение для защиты от мошеннического трафика // Компьютерное Обозрение (https://ko.com.ua/debyutirovalo_novoe_reshenie_f5_networks_dlya_zashhity_ot_moshennicheskogo_trafika_133665). 08.07.2020).***

****

«Инновационные решения Verint развернуты в более чем 180 странах, ими пользуются свыше 10 тыс. организаций по всему миру. Решения компании применяются в таких сферах как охрана правопорядка, борьба с преступностью и терроризмом, защита объектов критически важной инфраструктуры и т.д.

Разработки Verint тесно связаны с такими инновационными технологиями как большие данные, искусственный интеллект, машинное обучение и др. В распоряжении компании шесть собственных научно-исследовательских центров, на базе которых создаются и тестируются передовые решения.

Портфель разработок Verint, объединенный общим брендом Actionable Intelligence, включает в себя специализированные системы, каждая из которых идеально сбалансирована и настроена для решения определенного круга задач.

Система распознавания лиц Verint FaceDetect использует один из самых точных в отрасли алгоритмов распознавания лиц. Благодаря возможностям ИИ это решение для анализа видео обеспечивает операции по обеспечению безопасности необходимыми ситуационными данными. Система отслеживает интересующих лиц, анализируя потоковые данные в режиме реального времени (или постфактум) одновременно от нескольких систем и тысяч камер видеонаблюдения. Выявление отдельных лиц в толпе под разным углом и при сложном освещении за считанные секунды.

Решение VMS компании Verint включает мощные, полностью интегрированные инструменты для управления видеоданными, в том числе автоматическое отслеживание состояния системы и реагирование на события, управление расследованиями, программно-реализованную виртуальную матрицу, интерактивные карты объектов, мощный и интуитивно понятный интерфейс для просмотра видео, тонкий клиент для удаленных/ мобильных пользователей и многое другое. Благодаря решениям Verint операторы могут прогнозировать потенциальные угрозы или инциденты и обеспечивать необходимую готовность служб реагирования. Гибкая открытая архитектура решения легко интегрируется с существующими технологиями. Решение масштабируется от операций на одном объекте до крупномасштабных операций с разным географическим расположением объектов.

Verint VMS One преобразует традиционные Центры по обеспечению безопасности (SOC) в Интеллектуальные центры по обеспечению безопасности (ISOC). Данная система предназначена для одного объекта малого или среднего размера. Это решение для обеспечения безопасности и управления реагированием на основе полученных данных обеспечивает все преимущества более мощных решений, но при этом имеет меньшую стоимость. Используя передовые технологии ИИ и аналитики, VMS One позволяет получать информацию, необходимую для прогнозирования потенциальных угроз и их предотвращения, а также устранения последствий уже имеющихся инцидентов.

Платформа Verint Situational Awareness Platform для ситуационной осведомленности осуществляет сбор, структурирование и контекстуализацию огромных объемов данных из нескольких систем и источников информации для обеспечения полной ситуационной осведомленности. Благодаря сложным алгоритмам решения Verint позволяют оперативно обрабатывать большие объемы информации и выявлять в ней именно те элементы, которые важны для принятия решений в данный момент.

Передовая технология управления действиями сил реагирования NowForce анализирует критически важные события и мгновенно обеспечивает всестороннюю

ситуационную осведомленность. Диспетчерские службы, сотрудники быстрого реагирования и другие ресурсы могут использовать и обмениваться между собой оперативными данными о происходящих событиях в режиме реального времени, обрабатывая текущую и прошлую информацию с использованием геоинформационных карт GIS, географических зон, местоположения сотрудников, а также информации, получаемой от сообщающих лиц и других внешних источников.

Портфолио высоконадежных Verint IP-камер позволяет работать с видео в высоком разрешении, с самыми разными форматами сжатия данных для потоковой передачи, а также эффективными средствами контроля полосы пропускания. IP-камеры легко устанавливаются и интегрируются с уже используемыми устройствами, благодаря чему организация может оптимизировать имеющиеся технологии, повысив их эффективность для обеспечения безопасности. Мы предлагаем самые разные варианты исполнения, включая PTZ-камеры, встраиваемые камеры, мини-камеры, камеры в защитном колпаке, цилиндрические камеры, как для внутренней, так и для наружной установки для работы во всепогодных условиях и в вандалозащитном варианте исполнения, которые подойдут для вашего бюджета и задач.

Это далеко не полный список разработок Verint, доступных теперь партнерам ELKO и украинским заказчикам». ***(ELKO Ukraine начинает поставки решений безопасности Verint Systems // Компьютерное Обозрение (https://ko.com.ua/elko_ukraine_nachinaet_postavki_reshenij_bezopasnosti_verint_systems_133626). 06.07.2020).***

***

«Компания Google открыла исходники сканера Tsunami — масштабируемого решения для обнаружения опасных уязвимостей с минимальным количеством ложных срабатываний. Сканер ориентирован на крупные корпоративные сети, состоящие из тысяч или даже миллионов подключенных к интернету систем. Код уже доступен на GitHub.

Tsunami не будет зарегистрирован как продукт Google, но будет поддерживаться опенсорс-сообществом. Ранее компания поступила похожим образом с другим своим внутренним инструментом, Kubernetes, который тоже стал доступен для широких масс.

Как уже было сказано выше, от других подобных инструментов Tsunami отличает масштаб, ведь Google создавала свой сканер для по-настоящему гигантских компаний (таких, как она сама). В том числе для компаний, которые управляют сетями, куда входят сотни тысяч серверов, рабочих станций, сетевое оборудование и IoT-девайсы.

Tsunami хорошо адаптирован к большим и разнородным сетям такого рода и решает проблему запуска различных сканеров для каждого типа устройств. Для этого сканер разделен на две основные части, а также оснащен расширяемым механизмом поддержки плагинов.

Первый и основной компонент Tsunami — сам сканер или разведмодуль. Он сканирует сеть компании в поисках открытых портов, а затем проверяет все порты

и определяет точные протоколы и службы, работающие на них (чтобы предотвратить неправильную маркировку портов и не проверять устройства на наличие неправильных уязвимостей). Этот фингерпринтинговый модуль основан на nmap, но также использует и кастомный код.

Второй компонент Tsunami работает на основе результатов первого. Он взаимодействует с каждым устройством и его открытыми портами: выбирает список уязвимостей для тестирования и запускает безопасные эксплоиты, чтобы проверить, действительно ли устройство уязвимо для атак.

Возможности данного модуля для проверки на уязвимости можно расширить с помощью плагинов. Текущая версия сканера поставляется с плагинами для проверки открытых стратегически важных UI (Jenkins, Jupyter, Hadoop Yarn и так далее), а также слабых учетных данных. Для реализации последнего Tsunami использует инструменты с открытым исходным кодом, такие как ncrack, которые помогают обнаружить слабые пароли, используемые различными протоколами и инструментами, включая SSH, FTP, RDP и MySQL.

Разработчики Google обещают расширить список плагинов для Tsunami уже в ближайшие месяцы. Они будут публиковаться в отдельном репозитории GitHub». ***(Мария Нефёдова. Google открыла исходный код сканера уязвимостей Tsunami // Xakep (https://xakep.ru/2020/07/09/tsunami/). 09.07.2020).***

***

«Компания Avast выпустила обновленные версии своих решений безопасности.

Как отмечается, обновление коснулось прежде всего защиты от недавнего роста вымогателей по всему миру, связанного с пандемией COVID-19. Avast добавил функцию Ransomware Shield к своему бесплатному антивирусу Avast. Ранее эта функция была доступна только в платной версии антивируса Avast Premium Security. Также для Avast Premium Security компания представила совершенно новый Remote Access Shield.

В последние годы компания Avast отслеживала рост атак, использовавших протокол удаленного рабочего стола (RDP). Этот протокол применяется для проведения широко распространенных атак с программами-вымогателями. В марте 2020 года, в пик пандемии, Avast наблюдал увеличение этих атак во всем мире на 20%. Из-за того, что миллионы людей по всему миру ежедневно использовали RDP для удаленного доступа к своей бизнес-сети, этот инструмент стал очень активно использоваться злоумышленниками.

Чтобы усовершенствовать существующую технологию обнаружения угроз, Avast представила дополнительный уровень, который обеспечивает защиту файлов от вымогателей и других вредоносных программ, пытающихся изменить файлы. Ransomware Shield не дает вымогателям и другим ненадежным программам изменять, удалять или шифровать личные фотографии и файлы в защищенных папках. Эта функция защищает изображения, документы и другие папки от любых несанкционированных изменений.

В Avast Free Antivirus теперь включена упрощенная защита USB-накопителей — пользователям будет предложено просканировать USB-накопители при их подключении к компьютеру.

Улучшена защита от ботнетов — Web Shield предотвращает подключение программ к вредоносным серверам через устройство пользователя.

Чтобы устранить уязвимости удаленного рабочего стола, Avast добавил функцию Remote Access Shield для пользователей Avast Premium Security.

Remote Access Shield позволяет выбрать, кто сможет получать удаленный доступ к защищенному компьютеру: теперь пользователи могут определять, какие конкретные IP-адреса или диапазоны IP-адресов могут получить доступ к их компьютеру, а Avast заблокирует все другие IP-адреса. По умолчанию RAS уже блокирует IP-адреса, которые кажутся недопустимыми.

Решение автоматически блокирует любые атаки методом перебора, которые пытаются взломать учетные данные защищенного компьютера.

Remote Access Shield также автоматически блокирует соединения, через которые совершаются попытки использовать эксплойты удаленного рабочего стола, такие как BlueKeep, чтобы получить контроль над защищенным компьютером.

Кроме того, Remote Access Shield автоматически блокирует подключения к удаленному рабочему столу с опасных IP-адресов.

Экран удаленного доступа доступен начиная с версии 20.5 Avast Premium Security.

«На протяжении самоизоляции по всему миру, Avast отслеживал новые и растущие угрозы, которые появлялись из-за массовой удаленной работы, рассказывает Михал Пехоучек, технический директор Avast. — Мы наблюдали за ростом числа атак через RDP — это стало еще одной проблемой для людей, пытающихся работать и учиться через Интернет. Каждый имеет право на безопасность в сети, поэтому мы расширили нашу бесплатную антивирусную систему, которой пользуются миллионы людей во всем мире, и предоставили дополнительные уровни защиты». ***(Avast укрепляет защиту от атак вымогателей // Компьютерное Обозрение (https://ko.com.ua/avast_ukreplyaet_zashhitu_ot_atak_vymogatelej_133951).*** 31.07.2020).

***

«Компания Trend Micro Incorporated, мировой лидер в разработке решений для кибербезопасности, объявляет о том, что программное обеспечение Trend Micro Cloud One™ – Conformity теперь доступно и для пользователей платформы Azure. Это поможет глобальным организациям лучше справляться с ошибками конфигурации, проблемами соответствия требованиям и киберрисками, возникающими в облачных средах.

Компания Trend Micro Incorporated, мировой лидер в разработке решений для кибербезопасности, объявляет о том, что программное обеспечение Trend Micro Cloud One™ – Conformity теперь доступно и для пользователей платформы Azure. Это поможет глобальным организациям лучше справляться с ошибками

конфигурации, проблемами соответствия требованиям и киберрисками, возникающими в облачных средах.

Также компания добилась соответствия показателю CIS Microsoft Azure Foundations Security Benchmark. Это означает, что Conformity имеет встроенные правила для проверки на соответствие более чем 100 рекомендациям CIS (Center for Internet Security).

«За безопасность облака в целом отвечает поставщик облачных услуг, но безопасность операций и данных в облаке — ответственность клиента, которому мы помогаем, — говорит Венди Мур (Wendy Moore), вице-президент Trend Micro по продуктовому маркетингу. — Наша платформа Cloud One тесно интегрируется с Microsoft Azure, что делает возможным для DevOps-команд лёгкое развёртывание в любой гибридной облачной среде во время миграции в облако».

Компетентные в этой сфере сотрудники компаний часто перегружены проблемами управления гибридными облаками. Распространение теневых ИТ-проектов в организациях также приводит к тому, что ИБ-отдел последним узнаёт о том, что другие подразделения создали новые учётные записи в облаке, причём сделали это без должных предосторожностей и не уделив достаточного внимания соответствию требованиям, безопасности и управлению.

Решение Conformity решает эти проблемы, предоставляя мощные возможности контроля сред Azure и управления ими. Оно способно управлять облачной безопасностью и соответствием требованиям и предупреждает клиентов о состоянии рисков, а также предоставляет простые для выполнения рекомендации по исправлению ошибок. Это может помочь предотвратить такие распространённые ошибки, как предоставление несанкционированного доступа к базе данных и открытый доступ к учётным записям хранилища BLOB-объектов.

Внедряя API Conformity в конвейер CI/CD и существующие рабочие процессы, команды DevOps получают возможность идентифицировать потенциальные риски в своей облачной инфраструктуре, прежде чем те попадут в реальную среду. Так реализуется автоматизированное проактивное предотвращение уязвимостей.

Trend Micro Cloud One — Conformity ежедневно выявляет около 230 миллионов неправильных конфигураций облачных вычислений для пользователей Azure и AWS по всему миру.

Опыт Trend Micro по защите мультиоблачных сред — ключевой фактор для многих организаций. «Trend Micro — один из немногих вендоров, который предоставляет одинаковые возможности по обеспечению полной безопасности и мониторинга как в Microsoft Azure, так и в AWS, — говорит Марио Мендоса (Mario Mendoza), руководитель группы, работающей с архитектурой кибербезопасности и взаимодействием в компании Blackbaud. — Blackbaud использует подход DevOps, поэтому любое изменение поставщика системы безопасности требует участия команд DevOps. Тот факт, что решения Trend Micro способны защитить гибридную облачную среду Blackbaud без задержек в работе команд DevOps, имел решающее значение при выборе вендора. Trend Micro помогает Blackbaud постоянно следить за безопасностью облачных операций и всегда знает о новых угрозах, и мы рады

быть частью этого процесса. Это именно то, что мы как лидеры рынка ищем в партнёре».

Пробную версию Trend Micro Cloud One – Conformity можно получить бесплатно, как и быструю проверку работоспособности облака…» ***(Trend Micro представляет облачное решение для усиления защиты от ошибок конфигурации Microsoft Azure // AMC Ukraine (https://channel4it.com/publications/trend-micro-predstavlyaet-oblachnoe-reshenie-dlya-usileniya-zashchity-ot-oshibok-konfiguracii-microsoft-azure.html). 24.06.2020).***

****