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

№ 12 (грудень)

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– №12 (грудень) . – 320 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

«Ресурсний центр ГУРТ уже втретє вивчав потреби українських неурядових організацій (НУО) та публічних бібліотек в інформаційно-комунікаційний технологіях (ІКТ)…

43% НУО, із числа тих, які відповідали на запитання опитування, у 2019-2020 рр. зазнавали проблем із кібербезпекою. Найактуальнішими проблемами протягом цього періоду виявилися неправильні налаштування (20%), а також вірусні атаки та/або встановлення шкідливого програмного забезпечення (15%). При цьому 23% респондентів не знали відповіді на це запитання. Порівнюючи із результатами дослідження 2018 р., слід зауважити, що кількість організацій, які вказали, що впродовж останніх двох років не зазнавали проблем із кібербезпекою, зросла з 28% у 2018 р. до 33% у 2020 р.

Більше половини респондентів (54%), впевнені, що інформаційна система їхньої організації захищена певною мірою. Натомість 29% респондентів вважають, що вона не захищена взагалі, що на 2% вище від результатів дослідження 2018 р. та на 7% вище від результатів дослідження 2016 р.

Лише 6% респондентів вказали, що їхня організація проходила аудит інформаційної безпеки. При цьому 22% вперше чують про таку послугу, що все ж на 6% менше, ніж у 2018 р.

Переважна більшість респондентів (80%) не має внутрішніх інструкцій щодо правил інформаційної безпеки та роботи з даними. Однак, порівнюючи із результатами дослідження 2018 р., можна говорити про мінімальні позитивні тенденції в розробленні внутрішніх інструкцій такого типу.

Незважаючи на брак знань стосовно наявних ІКТ, який респонденти вказали серед основних причин, що заважають використовувати технології в повній мірі, лише 20% НУО зазначили, що їхні представники відвідували тренінги з цифрової безпеки й інформаційних технологій». **(Мазипчук Максим. Від цифровізації до цифрової трансформації: результати дослідження потреб НУО в ІКТ // Ресурсний центр ГУРТ (https://gurt.org.ua/news/recent/65264/). 10.12.2020).**

***

«Україна посіла 25 місце у новій редакції Національного індексу кібербезпеки 2020, опублікованому естонською Академією електронного урядування…

Для розробки нової редакції Національного індексу кібербезпеки було досліджено стан кібербезпеки 160 країн світу. Аналізували:

- законодавство у сфері кібербезпеки;
- кіберінциденти;
- освіту у сфері кібербезпеки;
- забезпечення захисту послуг, зокрема електронних;
- електронну ідентифікацію та довірчі послуги;
- захист персональних даних;
- заходи із реагування на кібератаки та кіберінциденти;
- боротьбу із кіберзлочинністю.

Порівняно з попередньою редакцією рейтингу, що вийшла у 2018 році, Україна покращила свої позиції на 4 сходинки.

Мінцифри разом з Держспецзв'язку продовжують посилювати кібербезпеку в Україні. Зокрема, зараз вже схвалені рішення Уряду щодо затвердження порядків формування переліків об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, а також щодо організації проведення огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. Це дозволить вдосконалити механізм кіберзахисту органів державної влади, інформаційно-телекомунікаційні системи, що перебувають у їх власності або адмініструванні.

Окрім цього, Мінцифри та Держспецзв'язку продовжують ініціювати реформування у законодавстві, яке стосується кібербезпеки. Крім цього, нарощуються потужності Державного центру кіберзахисту та працює урядова команда реагування на кіберінциденти CERT-UA. В Україні також працює один з найпотужніших у Європі кіберполігонів, що дозволяє відпрацьовувати сценарії реагування на кіберінциденти у режимі реального часу». ***(Україна посіла 25 місце у міжнародному рейтингу з кібербезпеки // Новини Закарпаття (https://transkarpatia.net/ukraine/137124-ukraiina-posla-25-msce-u-mzhnarodnomu-reytingu-z-kberbezpeki.html). 10.12.2020).***

***

«8 грудня 2020 року стартує перший етап багбаунті мобільного застосунку "Дія", другий етап планують провести наступного року…

Зазначається, що Мінцифри запустить багбаунті 8 грудня о 21:00, тестування триватиме до 15 грудня.

"1 мільйон гривень або 35 тисяч доларів тим, хто знайде вразливість у Дії. Це буде челендж для білих хакерів з усього світу на платформі Bugcrowd. Тестування триватиме до 15 грудня", - йдеться у повідомленні.

"Мета Мінцифри - зробити так, щоб українці були впевнені в захищеності своїх персональних даних та довіряли нашим сервісам. Ми постійно підтверджуємо захищеність застосунку", - додали у відомстві.

Призовий фонд - 1 мільйон гривень.

"Це можливість для білих хакерів з усього світу "зламати" копію застосунку і знайти уразливості в Дії 2.0. Умови багбаунті прості: чим серйозніша вразливість, тим більша виплата. У кожній категорії складності може бути кілька спеціалістів, які знайдуть уразливості. Тому комісія розробників прийматиме рішення щодо виділення коштів після того, як баги будуть виявлені. У будь-якому разі ми уважно розглянемо кожну вразливість і баг та нагородимо кожного хакера, який знайде недоліки в тестовому застосунку Дія", - пояснили в Мінцифри.

Відповідно винагороду буде поділено за декількома категоріям складності уразливості: перший рівень складності - до 3 500 доларів другий - до 1 200 доларів, третій - до 600 доларів, четвертий - до 250 доларів.

"Bugcrowd бере на себе практично всі операційні витрати, що дозволить команді Мінцифри зосередитися на усуненні виявлених вразливостей (якщо такі будуть).

Після завершення першого етапу багбаунті планується продовжувати цю практику і надалі. Вже наступного року буде проведено другий етап, який триватиме довше і надасть можливість кожному фахівцю з кібербезпеки спробувати свої сили в тестуванні Дії на вразливості", - йдеться у повідомленні». ***("Зламати "Дію": у Мінцифри планують другий етап багбаунті у 2021 році // Економічна правда (https://www.epravda.com.ua/news/2020/12/8/668949/). 08.12.2020).***

***

«Освітні програми з кібербезпеки у вишах мають базуватися на міжнародних стандартах сертифікації та передбачати практичні елементи навчання.

Про це заявили учасники віртуального круглого столу «Вища освіта з кібербезпеки в Україні», що відбувся з ініціативи керівників проекту USAID «Кібербезпека критично важливої інфраструктури України».

«Попри динамічний розвиток ІТ-сектору, українські компанії постійно відчувають брак кваліфікованих та досвідчених фахівців з інформаційної безпеки, зокрема і кібербезпеки, — зазначив під час дискусії заступник міністра освіти і науки Артур Селецький. — Як свідчать роботодавці, випускникам цієї спеціальності часто бракує спеціалізації чи практичних навичок. Тому сьогодні потрібно переглянути наявні освітні програми та запровадити сучасніші підходи у навчанні».

У підготовці таких фахівців МОН розраховує на співпрацю з роботодавцями і, зокрема, з приватним бізнесом. «Крім того, що ми маємо вдосконалити систему підготовки студентів, важливо забезпечити їх успішну адаптацію до професійної діяльності, і це потребує постійного контакту з професійною спільнотою, — цитує Артура Селецького прес-служба МОН. — Тож ми відкриті до співпраці і готові оперативно реагувати на ініціативи».

Сьогодні в Україні фахівців з кібербезпеки готує 51 заклад вищої освіти. Набути навичок з протидії кіберзагрозам та попрактикуватися в умовах, максимально наближених до реальних, студентам допоможуть віртуальні лабораторії для моделювання процесів в інформаційній безпеці та кібербезпеці. Задля покращення рівня практичних навичок проводитимуть стажування та застосовуватимуть дуальну форму навчання.

«Україна стикається з постійними кіберзагрозами, і багато таких атак спрямовані на критичну інфраструктуру України. Цей захід є важливою складовою в процесі трансформації української освіти з кібербезпеки та посилення спроможності України захищати себе від кіберзагроз», — наголосив директор Офісу економічного зростання Місії USAID в Україні та Білорусі Фархад Гауссі.

У рамках проекту USAID планується напрацювати нові підходи до викладання дисциплін за спеціальністю «Кібербезпека». Для цього майже 300 викладачів із щонайменше 12 українських вишів пройдуть навчання у закордонних організаціях, що працюють у сфері кібербезпеки». ***(Фахівців з кібербезпеки готуватимуть по-новому // Голос України (http://www.golos.com.ua/article/339279). 04.12.2020).***

***

«Усі органи влади повинні працювати над покращенням інформаційної та кібербезпеки нашої держави.

Про це заявив очільник СБУ Іван Баканов на нараді з представниками міністерств, інформує пресслужба відомства.

За його словами, системно питаннями кібербезпеки роками ніхто не займався.

“Реальні масштаби проникнення на інформресурси органів влади вражають – атаки відбуваються майже щодня“, – сказав Баканов.

Очільник СБУ повідомив, що переважна більшість кіберзагроз надходить з боку Росії. Понад 70% від загальної кількості всіх кібератак на органи державної влади здійснюють російські хакери.

Баканов зазначив, що несанкціонований доступ до інформаційних систем міністерств і відомств з боку агресора завдає суттєвої шкоди національній безпеці України.

За його прогнозами, у 2021 році головними об’єктами хакерських атак залишатимуться системи електронного документообігу, електронна пошта та інші інструменти дистанційної роботи та корпоративних мереж. Цілями кібератак також можуть стати об’єкти критичної інфраструктури, стратегічні підприємства…». ***(Понад 70% кібератак відбувається з боку Росії, – Баканов // UATV (https://uatv.ua/ponad-70-kiberatak-vidbuvayetsya-z-boku-rosiyi-bakanov/). 18.12.2020).***

***

«Національний координаційний центр кібербезпеки при Раді нацбезпеки і оборони України попереджає про високий рівень кіберзагрози з огляду на масштабну кібератаку в США, йдеться в повідомленні на сайті РНБО.

«Від атаки постраждали майже всі державні установі США. Злам відбувся через сервер оновлень системи управління продуктами SolarWinds Orion Platform (її версії 2019.4 - 2020.2.1 HF1). Атаку пов’язують з діяльністю хакерської групи APT29 або Cozy Bear, яку почасти звинувачують у зв’язках зі службою зовнішньої розвідки РФ. Згідно з інформацією, яку нині має НКЦК, атака дуже схожа з атакою Ransom: Win32/Petya, що мала місце в Україні у 2017 році», – йдеться в повідомленні.

У РНБО вказують: враховуючи те, що продукти SolarWinds не є розповсюдженими у використанні державними органами в Україні, ризики для ураження державних українських систем не є критичними. Однак «висока активність хакерських угруповань, які пов’язують з російськими спецслужбами, загрожує тим суб’єктам господарювання, які використовують цей продукт, відтак і в Україні, яка перебуває з Російською Федерацією у стані гібридної війни. Суб’єктам господарювання, які використовують цей продукт, рекомендовано перевірити свої мережі на наявність показників компрометації», додали в РНБО…». ***(РНБО попередила про високий рівень загрози через масштабну кібератаку в США // Радіо Свобода (https://www.radiosvoboda.org/a/news-khakery-rnbo-zagrozy-poperedzhennia/30999966.html). 14.12.2020).***

***

«Національний координаційний центр кібербезпеки (НКЦК) України попереджає, що через кібератаку на провідну американську компанію у сфері кібербезпеки FireEye збільшилась кількість загроз для українських інформаційних систем.

Про це повідомляє пресслужба центру.

«Внаслідок атаки були викрадені цифрові інструменти, за допомогою яких фахівці Red Team раніше виявляли уразливості в системах захисту інших компаній і урядів. Викрадені інструменти варіюються від простих скриптів для автоматизації збору даних про ціль до цілих фреймворків, аналогічних засобам CobaltStrike і Metasploit, і не містять експлойтів нульового дня. Вони зазвичай використовуються для активної перевірки стану безпеки мереж та імітації кібератак під час проведення кібернавчань. Такий інструментарій може бути використаний для втручання в мережі та інформаційні системи, та за певних умов бути використаний в якості кіберзброї», - зазначили у НКЦК.

За даними FireEye, до кібератаки можуть бути причетні спецслужби РФ.

«НКЦК разом з основними суб'єктами кібербезпеки здійснюють інформування органів державної влади та об'єктів критичної інфраструктури про способи виявлення та протидії викраденому інструментарію FireEye», - додали в НКЦК…» ***(Українські інформсистеми опинились під загрозою через кібератаку на компанію FireEye у США – НКЦК // MediaSapiens (https://ms.detector.media/kiberbezpeka/post/26181/2020-12-13-ukrainski-informsystemy-opynylys-pid-zagrozoyu-cherez-kiberataku-na-kompaniyu-fireeye-u-ssha-nktsk/). 13.12.2020).***

***

«В Україні за три місяці зафіксували більше 22 млн кіберінцидентів. Про це повідомляє пресслужба Ради національної безпеки та оборони України.

Серед інцидентів - 371 кібератака критичного та високого рівня. Також кіберспеціалистами було виявлено більше 18 тис. вразливостей.

За типами кіберінцидентів найбільш поширеними були сканування ресурсів (майже 15,5 млн випадків), bruteforce-атаки (більше 4 млн) та мережеві атаки (майже 1,2 млн).

Найбільше атак здійснювалось із США, Китаю, Франції, Росії, Чехії, Німеччини та Болгарії. При цьому хакерами були використані орендовані або скомпроментовані системи для приховування реального місця розташування, тому дані щодо кількості атак співвідносяться із розвитком ІТ-інфраструктури (в тому числі кількістю та доступністю дата-центрів) у певній державі…» ***(В Україні за три місяці зафіксували більше 22 млн кібератак – РНБО // MediaSapiens (https://ms.detector.media/kiberbezpeka/post/26180/2020-12-13-v-ukraini-za-try-misyatsi-zafiksuvaly-bilshe-22-mln-kiberatak-rnbo/). 13.12.2020).***

***

«17 грудня Комітет цифрової трансформації провів слухання на тему: «Про імплементацію Дорожньої карти інтеграції України до Єдиного цифрового ринку ЄС».

Заступник голови Комітету цифрової трансформації Єгор Чернєв, відкриваючи слухання, зазначив, що стратегія єдиного цифрового ринку побудована на трьох напрямах: кращий доступ споживачів і бізнесу до товарів та послуг, створення належних умов до просування інформаційно-комунікаційних технологій і послуг, максимізація зростання потенціалу цифрової економіки.

«За шість років ми значно проснулися з точки зору імплементації стандартів і нормативів Європейського Союзу. Але питання, що стосуються саме цифрової економіки, фрагментовані та розрізнені. Законодавчий рівень залишається застарілим. Ми ставимо за мету трансформувати ресурсну економіку в цифрову, яка потребує єдиного бачення та стратегії», - зазначив Єгор Чернєв.

За його словами, Комітет працює над оновленням законодавства, зокрема мова йде про законопроекти про віртуальні активи, кібербезпеку, персональні дані. Але ще потрібна комплексна єдина державна стратегія розвитку цифрової економіки, яка реалізовувалася б всіма органами влади.

Заступник голови Комітету Олександр Федієнко зазначив, що важливо максимально наблизити чинне українське законодавство до європейського законодавчого поля. «Але ми не повинні його копіювати, бо галузь має свої традиції та технології», - наголосив він.

Олександр Федієнко нагадав, що 16 грудня прийнято Закон про електронні комунікації №3014. Його внесено до дорожньої карти Угоди про асоціацію з ЄС. Наступним шляхом є Закон про незалежний регулятор. «Ми напрацювали законопроект про Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектру та надання послуг поштового зв'язку України, який сподіваюся, буде внесений на наступній сесії. Це фундаментальні закони, без яких неможлива європейська інтеграція», - зазначив він.

Директорка Міжнародної громадської організації «Європейська Медіа Платформа» Оксана Приходько наголосила на необхідності розробки глосарію з цифрової економіки, аби уникати двозначності трактувань.

«Створення Дорожньої карти — це багатофазовий та багатосторонній процес, тому лише спільними зусиллями всіх стейкхолдерів, включаючи наших європейських партнерів, це стало можливим» - зауважила Генеральний Директор директорату євроінтеграції Міністерства цифрової трансформації Гульсанна Мамедієва.

Учасники слухань відзначили важливість прийняття Парламентом Закону України «Про електронні комунікації», який дозволить здійснювати реформи одночасно з країнами ЄС.

За результатами комітетських слухань буде напрацьовано відповідні рекомендації». ***(Відбулися слухання щодо імплементації Дорожньої карти***

інтеграції України до Єдиного цифрового ринку ЄС // Голос України (http://www.golos.com.ua/news/127180). 18.12.2020).

***

«10 грудня Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України та Державне підприємство "Український державний центр радіочастот" уклали Меморандум про організацію взаємодії у сфері кібербезпеки та кіберзахисту. Меморандум укладено з метою співробітництва в сфері кібербезпеки та кіберзахисту, розвитку спроможності із забезпечення кіберзахисту інфраструктури.

Меморандум окрім іншого передбачає:

– консультування фахівців підприємства з питань забезпечення виконання загальних вимог до кіберзахисту об'єктів критичної інфраструктури, віднесення об'єктів до об'єктів критичної інфраструктури, їх категоризації, побудови системи управління інформаційною безпекою та застосування політик інформаційної безпеки;

– апробацію процесів взаємодії Security Operations Center (далі – SOC) Державного центру кіберзахисту з галузевим SOC, інтеграції Security Information and Event Management систем;

– проведення пілотного проекту з надання Державним центром кіберзахисту сервісу кіберзахисту "SOC-as-a-Service";

– набуття спроможності командою реагування на надзвичайні комп'ютерні події підприємства через взаємодію з CERT-UA та практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів;

– вивчення особливостей галузі телекомунікацій для формування вимог до технологічної інфраструктури організаційно-технічної моделі кіберзахисту національної системи кібербезпеки.

Законодавство України у сфері кібербезпеки та кіберзахисту визначає необхідність забезпечення кіберзахисту об'єктів критичної інфраструктури. Кіберзахист об'єкта критичної інфраструктури забезпечується власником та/або керівником об'єкта критичної інфраструктури відповідно до Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року №518, та законодавства в сфері захисту інформації та кібербезпеки». ***(Державний центр кіберзахисту Держспецзв'язку та ДП "Український державний центр радіочастот" уклали Меморандум про організацію взаємодії у сфері кібербезпеки та кіберзахисту // ITUA.info (http://itua.info/press/40519.html). 15.12.2020).***

***

«КП «Київтеплоенерго» розпочало створення комплексної системи кіберзахисту теплоенергетичної інфраструктури Києва. Мета проєкту – запобігти кібератакам і підвищити рівень енергобезпеки. Про це повідомляє комунальне підприємство.

Зокрема, за інформацією підприємства, посилять захист систем управління генерацією тепла та електроенергії, диспетчерського управління, систем

телемеханіки, релейного захисту тощо. У разі стороннього втручання додатковий рівень захисту енергетичного комплексу Києва фактично відіграватиме роль щита для зупинки хакерських атак і вірусів. Це дозволить підвищити стабільність постачання тепла та електроенергії до сотень тисяч київських квартир.

«Сьогодні разом із автоматизацією управління енергосистемою зростає загроза кібератак на енергокомпанії. Це може призвести до дестабілізації роботи, аварій і навіть надзвичайних ситуацій. Перша зареєстрована кібератака на енергокомпанії в Україні сталася в грудні 2015 року. Тоді постраждали три енергокомпанії. Тільки в Київській області через втручання в систему управління без світла повністю або частково лишились 50 населених пунктів. Аби попередити подібне в Києві, слід забезпечити кіберзахист критично важливих об'єктів інфраструктури», – зазначив директор КП «Київтеплоенерго» Вячеслав Бінд.

Планують реалізувати проєкт упродовж 2021-2022 років. Аудит інформаційної безпеки і впровадження нових IT-систем буде здійснено за технічної підтримки USAID Проєкту енергетичної безпеки.

Нагадаємо, що «Київтеплоенерго» впроваджує систему SCADA – більше тисячі київських об'єктів енергетики об'єднають в єдину систему диспетчерського управління та збору даних.

В управлінні підприємства нині розгалужена теплова та енергетична інфраструктура міста: близько 200 великих і малих теплоджерел, тисячі одиниць обладнання, 2,7 тис. км тепломереж, якими тепло отримують близько мільйона клієнтів. Дві теплоелектроцентралі № 5 і № 6 забезпечують 48% потреб у теплі та майже 60% – в електроенергії столиці». ***(«Київтеплоенерго» посилює кіберзахист столичної енергосистеми // Офіційний портал Києва (https://kyivcity.gov.ua/news/kivteploenergo_posilyuye_kiberzakhist_stolichno_energosistemi/). 16.12.2020).***

***

Правове забезпечення кібербезпеки в Україні

«Кабінет міністрів (Кабмін) схвалив Концепцію розвитку сфери штучного інтелекту в Україні. Реалізація Концепції передбачена протягом 2020-2030 років.

Розпорядження прийнято на засіданні уряду 2 грудня. Документ схвалений з умовою доопрацювання, пише РБК-Україна.

Як зазначається в пояснювальній записці до проекту, для розробки першочергових заходів з розвитку та впровадження штучного інтелекту в Україні на державному рівні на період 2021-2023 років потрібно фінансування з держаного бюджету у розмірі 14,390 млн грн.

Пріоритетними напрямами реалізації Концепції є:

- зайняття Україною значного сегмента світового ринку технологій штучного інтелекту та провідних позицій у міжнародних рейтингах (AI Readiness Index by Oxford Insights, AI Index by Stanford University тощо);

- впровадження технологій штучного інтелекту у сфері освіти, економіки, публічного управління, кібербезпеки, оборони та інших сферах для забезпечення довгострокової конкурентоспроможності України на міжнародному ринку;
- забезпечення доступу до інформації (баз даних, електронних реєстрів тощо), її використання під час розроблення технологій штучного інтелекту для виробництва товарів та надання послуг;
- захист інформаційного простору від несанкціонованого втручання, забезпечення безпечного функціонування інформаційно- телекомунікаційних систем тощо.

"Враховуючи фактичну відсутність на сьогодні в Україні нормативно-правових актів, що регламентують цю галузь, Україна як держава, а також українські науковці та продуктові компанії у галузі штучного інтелекту не мають змоги брати активну участь у розвитку світового ринку технологій штучного інтелекту", – йдеться в документі…» ***(Уряд схвалив Концепцію розвитку штучного інтелекту до 2030 року // Рубрика (https://rubryka.com/2020/12/02/uryad-shvalyv-kontseptsiyu-rozvytku-shtuchnogo-intelektu-do-2030-roku/). 02.12.2020).***

***

«Кабмін ухвалив постанову, яка визначає заходи для забезпечення функціонування системи кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури.

Як передає кореспондент Укрінформу, відповідне рішення уряд підтримав на засіданні 23 грудня.

Згідно з пояснювальною запискою до постанови, вона передбачає заходи щодо забезпечення функціонування системи виявлення вразливостей і реагування на кібератаки та кіберінциденти.

Зокрема, документ передбачає здійснення заходів із: затвердження Порядку функціонування системи виявлення вразливостей і реагування на кібератаки та кіберінциденти; визначення відповідальними за функціонування такої системи Державний центр кіберзахисту та Державну служби спеціального зв'язку та захисту інформації України; доручення міністерствам та іншим центральним органам виконавчої влади забезпечення встановлення на об'єктах кіберзахисту комплектів обладнання підсистем збору телеметрів інформаційно-телекомунікаційних систем; доручення Держспецзв'язку щороку до 10 січня подавати до Кабміну інформацію про стан функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки». ***(Уряд схвалив заходи проти кібератак на критичну інфраструктуру // Укрінформ (https://www.ukrinform.ua/rubric-society/3160122-urad-shvaliv-zahodi-proti-kiberatak-na-kriticnu-infrastrukturu.html). 23.12.2020).***

***

«З 2 по 8 грудня система захищеного доступу державних органів до мережі Інтернет заблокувала 11 DDoS-атак, переважна більшість з яких — на сайти Офісу Президента України. Про це повідомляє УНН із посиланням на пресслужбу Державної служби спеціального зв'язку та захисту інформації України.

"Система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури на об'єктах моніторингу зафіксувала 468 366 підозрілих подій. Переважна більшість зафіксованих підозрілих подій стосується спроб мережевого сканування (71%), застосування нестандартних протоколів (26%) та виявлення мережевого ШПЗ (2%)", — сказано у повідомленні.

Зазначається, що система захищеного доступу державних органів до мережі Інтернет заблокувала 54 184 атак різних видів, що приблизно на рівні попереднього тижня. Переважна більшість — це мережеві атаки прикладного рівня (95%) та атаки типу "Harvest Attack" (3%).

"Також зафіксовано і заблоковано 11 DDoS-атак, зокрема на вебресурси Офісу Президента України та Держспецзв'язку", — йдеться у повідомленні.

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA у цей період зареєструвала та опрацювала 2 179 кіберінцидентів, що на 14% більше, ніж попереднього тижня.

Переважна більшість опрацьованих інцидентів стосується недержавного сектору (близько 99%). Основна кількість інцидентів стосується розповсюдження ШПЗ (98%)…». ***(Валерія Гуржий. За тиждень зафіксовано понад 10 кібератак на держоргани, більшість - на сайти ОПУ // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1906796-za-tizhden-zafiksovano-ponad-10-kiberatak-na-derzhorgani-bilshist-na-sayti-opu). 08.12.2020).***

***

«Хакери здійснили атаку на мережі секретаріату Уповноваженого з захисту державної мови. Атаку вдалося зупинити штатним ІТ-фахівцям.

Про це повідомляє прес-служба Уповноваженого з захисту державної мови на своїй сторінці у Facebook.

«На комп'ютерні системи нашого Секретаріату зловмисниками була здійснена кібератака з метою отримати несанкціонований доступ до пристроїв мережевої ІТ-інфраструктури та вивести їх з ладу», - йдеться у повідомленні.

Також зазначено, що атака була оперативно припинена силами ІТ-фахівців секретаріату.

У секретаріаті вважають це не просто спробою пошкодити пристрої, а атакою на українську мову і тих, хто її захищає. За словами пресслужби, це спроба паралізувати діяльність, але у відомстві здатні відбивати як інформаційні, так і хакерські напади.

Нещодавно в СБУ заявили, що російські хакери залишаються головною загрозою в кіберпросторі України.

Між іншим, спецслужби США підтвердили масштабну кібератаку на урядові структури. Згідно з їх інформацією, організували атаку російські хакери…». ***(Хакери атакували сайт мовного омбудсмена // Українські медійні системи (https://glavcom.ua/news/hakeri-atakuvali-sayt-movnogo-ombudsmena-725245.html). 14.12.2020).***

***

«Приблизно 500 тисяч українців щодня стикаються з шахраями в інтернеті. Найчастіше аферисти використовують схеми з передоплатою і сайтами-двійниками популярних платформ. Напередодні новорічних покупок OLX запускає освітній сайт Онлайн[за]хист, щоб допомогти мільйонам українців прокачати свої навички безпечного шопінгу.

За підрахунками Української міжбанківської асоціації членів платіжних систем ЕМА, щодня 1-2% українців (приблизно 500 тисяч) стикаються з кіберзлочинцями. Улюбленими місцями аферистів стали сайти з продажу товарів. Так, під виглядом псевдопокупця чи псевдопродавця жертву намагаються заманити на сайт-копію та, застосовуючи методи соцінженерії, отримати персональні та платіжні дані.

Щоб запобігти шахрайству в інтернеті та ефективніше боротися з недобросовісними користувачами, компанія OLX вирішила створити освітній сайт Онлайн[за]хист. Мета проєкту — підвищити кіберграмотність населення та поширити правила безпеки з купівлі-продажу товарів в інтернеті.

На освітньому сайті доступна інформація про методи кіберзлочинців, особистий досвід зустрічі з шахраєм і поради щодо безпечного онлайн-шопінгу. Завдяки проєкту користувачі зможуть прокачати знання, навчитися захищати свої персональні дані в інтернеті та насолоджуватися безпечним онлайн-шопінгом.

Результати нещодавнього дослідження OLX показали, що українці недостатньо обізнані навіть щодо найпоширеніших схем, які застосовують шахраї. Майже 15% опитаних думають, що фішинг — це рибалка, а 40% українців готові відправити передоплату за товар. Загалом, за оцінкою Асоціації ЕМА, за допомогою соцінженерії цього року інтернет-шахраї «заробили“ вже 116,5 млн грн.

“У більшості випадків люди самі наражають себе на небезпеку: через незнання базових правил вони повідомляють свої платіжні дані шахраям, переходять за сторонніми посиланнями чи надсилають передоплату при замовленні товару, — розповідає Віктор Нобіуз, керівник відділу бізнес-аналітики OLX Україна. — Ми в OLX прагнемо захистити наших користувачів і вживаємо різних заходів. Вони спрямовані як на посилення IT-безпеки платформи (робота 24/7 моделей штучного інтелекту, щоденний аналіз 15 000 профілів на фішинг, постійний процес виявлення та блокування приблизно 30 фішингових сайтів на день), так і на підвищення обізнаності українців. Саме тому ми запускаємо освітній проєкт Онлайн[за]хист, щоб навчити українців правилам безпеки в інтернеті та показати, що кожен може стати майстром безпечного шопінгу»…» ***(Напередодні Новорічних свят для українців запустився сайт з кібербезпеки // ProPro (http://propro.com.ua/archives/21099). 15.12.2020).***

***

«З 23 по 29 грудня система захищеного доступу державних органів до мережі Інтернет заблокувала 19 DDoS-атак на сайти Офісу Президента України та Держспецзв'язку. Про це повідомляє УНН із посиланням на пресслужбу Державної служби спеціального зв'язку та захисту інформації України.

"Система захищеного доступу державних органів до мережі Інтернет заблокувала 51 630 атак різних видів, що на 4% більше, ніж попереднього тижня. Переважна більшість — це мережеві атаки прикладного рівня (96%) та атаки типу „Harvest Attack" (2%). Також зафіксовано і заблоковано 19 DDoS-атак, зокрема на вебресурси Офісу Президента України та Держспецзв'язку", — сказано у повідомленні.

Зазначається, що система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури на об'єктах моніторингу зафіксувала 4 204 714 підозрілих подій, що на 27% більше, ніж попереднього тижня. Переважна більшість зафіксованих підозрілих подій стосується підозрілого виконувального коду (6%).

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA у цей період зареєструвала та опрацювала 2 985 кіберінцидентів, що на 18% менше, ніж попереднього тижня.

Переважна більшість опрацьованих інцидентів стосується недержавного сектору (близько 99%). Основна кількість інцидентів стосується розповсюдження ШПЗ (99%)…». ***(Валерія Гуржий. За тиждень зафіксовано близько 20 кібератак на сайти ОПУ та Держспецзв'язку // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1910079-za-tizhden-zafiksovano-blizko-20-kiberatak-na-sayti-opu-ta-derzhspetszvyazku). 29.12.2020).***

***

Боротьба з кіберзлочинністю в Україні

«Октябрьский районный суд г. Запорожье признал мужчину виновным в распространении компьютерного вируса и назначил наказание в виде штрафа в размере 8500 гривен…

В марте 2019 года подсудимый загрузил ранее созданный вредоносный файл под названием «ver6.0.rar» в облачное хранилище в Интернете, доступ к которому был открыт всем пользователям, распространив таким образом вредоносную программу неопределенному кругу лиц.

Согласно заключению эксперта по результатам компьютерно-технической экспертизы вышеуказанный файл определяется как вредоносное программное обеспечение класса троян (типа "BackDoor"), то есть тип вредосного программного обеспечения, предназначенного для обхода стандартных процедур аутентификации, несанкционированного удаленного доступа и предоставляет возможность получения информации из баз данных (такие как логины и пароли пользователей, зарегистрированных на сайтах), оставаясь при этом незамеченным.

Суд квалифицировал действия обвиняемого по ст.361-1 ч.1 УК Украины (создание и распространение вредоносных программных средств, предназначенных

для несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей.

На основании ст.474 ч.1 УПК Украины в суд до начала подготовительного судебного заседания поступило соглашение о признании виновности, заключенное между прокурором и обвиняемым. Согласно соглашению стороны согласились на назначение подсудимому наказания по ст.361-1 ч.1 УК Украины в виде штрафа в размере 500 необлагаемых минимумов доходов граждан в сумме 8500 гривен.

На подготовительном судебном заседании обвиняемый признал свою вину и предоставил суду согласие на назначение согласованного наказания.

Суд признал мужчину виновным в совершении уголовного правонарушения и на основании соглашения о признании виновности назначил ему наказание в виде штрафа в размере 8500 гривен…» ***(Артем Сереженок. Украинец заплатит штраф за распространение вредоносного ПО // Internetua (https://internetua.com/ukrainec-zaplatit-shtraf-za-rasprostranenie-vredonosnogo-po). 03.12.2020).***

***

«Поліцейські відділу протидії кіберзлочинам в області встановили причетність 33-річного житомирянина до правопорушень у сфері інтелектуальної власності. За місцями розташування його інтернет-магазина та проживання були проведені санкціоновані обшуки. Триває подальше розслідування.

Досудове розслідування проводиться слідчими Житомирського відділу поліції за ознаками правопорушення, передбаченого 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.

Попередньо встановлено, що житель обласного центру, маючи спеціальну підготовку та володіючи знаннями у сфері ІТ-технологій, створив інтернет-магазин, де серед іншого надав послуги із перепрограмування ігрових консолів Playstation. Тобто несанкціоновано втручався у програмне забезпечення компанії SIEE, змінюючи його та створюючи можливість уникати необхідності використовувати ліцензовану версію продукту. За приблизними підрахунками сума завданого збитку складає близько 50 тисяч гривень.

Під час обшуків було вилучено низку гаджетів, оптичні та жорсткі диски, мобільні телефони, флеш-накопичувачі, ігрові консолі, бухгалтерські документи, гроші та інше. Усі носії інформації буде направлено на відповідне експертне дослідження. За результатами його проведення вирішуватиметься питання щодо остаточної кваліфікації події». ***(У Житомирі поліцейські викрили молодика у несанкціонованому втручанні у програмне забезпечення // Кіберполіція України (https://cyberpolice.gov.ua/news/u-zhytomyri-policzejski-vykryly-molodyka-u-nesankczionovanomu-vtruchanni-u-programne-zabezpechennya-2983/). 04.12.2020).***

***

«Суд приговорил к году тюрьмы украинца, который при помощи специального ПО взламывал учетные записи пользователей Интернета…

В феврале 2020 года житель Запорожья загрузил на свой ноутбук специальное ПО под названием «SteamChecker», которое согласно заключению судебного эксперта является вредоносным программным обеспечением, предназначенным для преодоления логической защиты данных, которые хранятся на интернет-ресурсах.

После загрузки обвиняемый создал и добавил к «SteamChecker» файлы-проекты для осуществления атаки путем перебора логинов и паролей, чем согласно заключению судебного эксперта создал отдельное вредоносное программное обеспечение с возможностями осуществления атак перебором по созданным сценариям.

В период с 13 февраля по 3 мая 2020 года мужчина осуществлял атаки с помощью имеющегося у него вредоносного ПО, в результате которых получал данные с логинами и паролями от учетных записей пользователей всемирной сети Интернет.

Действия обвиняемого суд квалифицировал по ч. 1 ст. 361-1 УК Украины, как создание с целью использования вредоносного программного обеспечения, предназначенного для несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров), автоматизированных систем и компьютерных сетей.

29 сентября между прокурором и обвиняемым было заключено соглашение о признании виновности. Согласно условиям которого, обвиняемый безоговорочно признает вину в совершении преступления и стороны согласились на назначении наказания в виде 1 года лишения свободы. Суд утвердил данное соглашение о признании виновности.

В соответствии с положениями ст. 75, 76 УК Украины мужчину освободили от отбывания наказания с условием, если он в течение испытательного срока один год не совершит нового преступления и выполнит возложенные на него определенные обязанности». ***(Артем Сереженок. Суд приговорил украинца к году тюрьмы за взлом учетных записей пользователей Интернета // Internetua (https://internetua.com/sud-prigovoril-ukrainca-k-godu-tuarmy-za-vzlom-ucsetnyh-zapisei-polzovatelei-interneta). 14.12.2020).***

***

«Фігурант зламував облікові записи мобільних телефонів і збирав персональні дані користувачів. Використовуючи ці дані, він здійснював віддалений перевипуск сім-карт та надалі отримував доступ до онлайн-банкінгу. Від злочинних дій постраждали близько 100 осіб.

Шахрайську діяльність громадянина викрили співробітники відділу протидії кіберзлочинам Полтавщини спільно зі слідчим відділом кременчуцької поліції.

Встановлено, що 31-річний чоловік використовував шкідливе програмне забезпечення для зламу облікових записів та доступу до телефонних книг користувачів. Серед контактів фігурант обирав номери близьких родичів потерпілої

особи. Використовуючи таку інформацію, він здійснював віддалений перевипуск сім-карт через оператора мобільного зв’язку.

Разом із доступом до сім-карт потерпілих зловмисник отримував доступ і до їхнього онлайн-банкінгу, звідки привласнював гроші.

Попередньо встановлено, що від шахрайських дій фігуранта постраждали близько 100 осіб. Загальна сума збитків сягає мільйона гривень.

За місцем проживання зловмисника правоохоронці провели обшук та вилучили комп’ютерну техніку, мобільні телефони та банківські картки. Усе вилучене направлено на проведення відповідних експертних досліджень.

До проведення обшуків також було залучено батальйон поліції особливого призначення місцевого управління поліції.

Чоловікові оголошено про підозру у вчинені правопорушення, передбаченого ч. 3 ст. 190 (Шахрайство) Кримінального кодексу України. Зловмиснику загрожує позбавлення волі на строк від трьох до восьми років.

Вирішується питання щодо обрання запобіжного заходу. Слідчі дії тривають.

Процесуальне керівництво у справі здійснює Кременчуцька місцева прокуратура…» ***(Кіберполіцейські викрили зловмисника, який за допомогою «вірусу» привласнив майже мільйон гривень громадян // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpoliczejski-vykryly-zlovmysnyka-yakyj-za-dopomogoyu-virusu-pryvlasnyv-majzhe-miljon-gryven-gromadyan-4543/). 16.12.2020).***

***

«…Співробітники відділу протидії кіберзлочинам Київщини спільно зі слідчим підрозділом Дарницького управління поліції Києва викрили громадянина у несанкціонованому втручанні в роботу комп’ютерів.

Встановлено, що 26-річний житель столиці розробив «вірус», суть роботи якого полягала у підміні веб-гаманців та викраденні персональних даних користувачів.

Шкідливе програмне забезпечення потрапляло на комп’ютерну техніку у вигляді електронного листа, а далі – надавало доступ зловмисникам до крипто-гаманця користувача.

Свою розробку фігурант продавав на тематичних форумах. Коштував один такий примірник понад 5 тисяч гривень. Також фігурант пропонував безкоштовну версію, яка працювала безпосередньо на нього.

Наразі кіберполіцейські встановлюють коло потерпілих від такої діяльності осіб та суму збитків.

За місцем мешкання фігуранта правоохоронці провели обшук та вилучили комп’ютерну техніку та банківські картки, які використовувалися у протиправній діяльності.

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. Максимальне покарання, яке передбачає санкція статті, - позбавлення волі на строк до шести років. Слідчі дії тривають.

Процесуальне керівництво у справі здійснює столична прокуратура № 2». ***(Кіберполіція Київщини викрила хакера у розповсюджені «вірусу», що привласнює гроші з крипто-гаманців громадян // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-kyyivshhyny-vykryla-xakera-u-rozpovsyudzheni-virusu-shho-pryvlasnyuye-groshi-z-krypto-gamancziv-gromadyan-6162/). 23.12.2020).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Україна приєдналася до рішення Ради ЄС запровадити обмежувальні заходи проти ще двох людей, які причетні до кібератак проти Євросоюзу або його країн-членів…

У зазначеному рішенні Ради ЄС йдеться про включення двох громадян КНР до санкційного списку осіб, на яких поширюються обмежувальні заходи, заборона в'їзду на територію ЄС та заморожування активів.

"Країни-кандидати Республіка Північна Македонія, Чорногорія і Албанія, країни Європейської зони вільної торгівлі Ісландія і Норвегія, члени Європейського економічного простору, а також Україна і Грузія приєдналися до цього рішення Ради ЄС", – йдеться в документі.

Вказані країни забезпечать відповідність національної політики цьому рішенню Ради ЄС…» ***(Кібератаки: Україна підтримала розширені санкції ЄС // UA\|TV (https://uatv.ua/kiberataky-ukrayina-pidtrymala-rozshyreni-sanktsiyi-yes/). 10.12.2020).***

***

«Соединенные Штаты и Австралия подписали первое в истории двустороннее соглашение, которое позволяет Киберкомандованию США (USCYBERCOM) и Подразделению информационной войны (IWD) Сил обороны Австралии совместно разрабатывать и совместно использовать виртуальную платформу кибер-обучения.

Министерства обороны двух стран добьются этого, включив отзывы IWD в моделируемую учебную область USCYBERCOM, известную как постоянная кибер-учебная среда (PCTE).

«Эта договоренность по проекту является важной вехой для американо-австралийского сотрудничества. Это первая кибернетическая договоренность, заключенная между армией США и союзной страной, которая подчеркивает ценность партнерства Австралии в области моделирования обучения», - заявила Элизабет Уилсон, подписавшая контракт с США.

«Чтобы противостоять известным и потенциальным угрозам противника, армия изменила свое стратегическое мышление; мы приняли разумные решения, чтобы переориентировать наши усилия на инвестирование в новые, появляющиеся

и умные технологии, которые укрепят нашу способность сражаться и побеждать в войнах нашей страны. "

Новый подход резко сокращает время, необходимое киберсилам США и их союзников для разработки совместных виртуальных обучающих платформ, что раньше занимало месяцы для каждого конкретного сценария.

PCTE теперь предоставляет платформу для совместной подготовки, которую USCYBERCOM, IWD и союзные силы (включая, помимо прочего, партнеров Five Eyes по разведке) могут повторно использовать и развивать во время индивидуального и совместного обучения.

«Долгосрочная цель PCTE - предоставить сотрудникам киберпространства DOD возможность создавать и проводить комплексные, комбинированные и совместные тренинги, упражнения, сертификацию и репетиции миссии в учебной среде», - заявили в USCYBERCOM.

«Требования к среде обучения, обусловленные целями обучения и определяемыми пользователем спецификациями, должны имитировать реалистичную рабочую среду, которая обеспечивает объем, масштабируемость и точность».

Этот виртуальный учебный полигон был запущен в феврале 2020 года как компонент Совместной архитектуры кибервойны вооруженных сил США и представляет собой безопасную и распределенную реконфигурируемую среду, которая позволяет одновременно проводить несколько независимых кибер-тренировок.

Это позволяет операторам министерства обороны практиковать свои навыки в закрытых реалистичных операционных средах, имитирующих живые сети.

Соглашение по проекту возможностей кибер-обучения, подписанное сегодня Австралией и США, «является примером того, как силы кибер-миссий США и Австралии работают вместе и демонстрируют успех в сотрудничестве в области вооружений», - добавили в USCYBERCOM.

«Схема проекта, оцениваемая в 215,19 миллиона долларов на шесть лет, обеспечивает гибкость для развития возможностей кибер-обучения в будущем». ***(Sergiu Gatlan. US and Australia to develop shared cyberattack training platform // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/us-and-australia-to-develop-shared-cyberattack-training-platform/). 04.12.2020).***

***

«Україна та Іспанія провели перші в історії міжвідомчі кіберконсультації, покликані зміцнити кібезбезпеку ЄС та українсько-іспанські відносини. Про це у своєму Twitter написав заступник міністра закордонних справ Василь Боднар…

“Відбулися перші в історії міжвідомчі кіберконсультації з Іспанією. Така співпраця покликана зміцнити не лише українсько-іспанські відносини, але й кібербезпеку ЄС, враховуючи наявний досвід України у цій сфері”, — зазначив він…». ***(Валерія Гуржий. Україна провели перші в своїй історії міжвідомчі кіберконсультації з Іспанією // Інформаційне агентство «Українські***

Національні Новини» (https://www.unn.com.ua/uk/news/1907749-ukrayina-proveli-pershi-v-svoyiy-istoriyi-mizhvidomchi-kiberkonsultatsiyi-z-ispaniyeyu). 14.12.2020).

***

«Ростелеком» в лице дочерней компании «Ростелеком-Солар», национального провайдера кибербезопасности, заключил соглашение с компанией «Сименс». В рамках сотрудничества решения компании «Сименс» используются для построения индустриального киберполигона, который предоставит промышленным предприятиям возможность отрабатывать практические навыки отражения кибератак.

«Обеспечение информационной безопасности на объектах электроэнергетики становится все более острой темой. Повышение квалификации обслуживающего персонала – одно из основных направлений в вопросе создания защищенной инфраструктуры объекта. На наш взгляд, подобные киберполигоны позволяют наиболее эффективным образом осуществить обучение специалистов методам защиты от киберугроз», - говорит Александр Трофимов, руководитель направления технической поддержки подразделения «Автоматизация в энергетике» компании «Сименс».

По данным центра мониторинга и реагирования на кибератаки Solar JSOC, в 2019 году киберпреступники сменили вектор интересов. Количество атак, направленных на кражу денежных средств, снизилось на 15%. И виден отчетливый рост (на 40%) хакерской активности, направленной на получение контроля над инфраструктурой, В случаях атак на критическую информационную инфраструктуру (КИИ) более 16% из них были нацелены на АСУ ТП или закрытые сегменты. Это ставит перед промышленными предприятиями задачу по отработке защиты критичных сегментов промышленных сетей на практике. Решение данной задачи – одна из целей создания национального киберполигона.

Техническая инфраструктура индустриального киберполигона выполняется в соответствии с пятиуровневой моделью университета Пердью (Purdue Reference Model, PRM). При этом для организации уровней 1 - «Базовые системы контроля» и 2 - «Системы диспетчерского управления и сбора данных» применяются реальные компоненты систем промышленной автоматизации. В соответствии с заключенным соглашением, «Ростелеком-Солар» будет использовать устройства релейной защиты и автоматики семейства SIPROTEC 5 производства компании «Сименс», предназначенные для своевременной автоматической ликвидации аварийных режимов работы электрооборудования и управления им. Также на инфраструктуре киберполигона была установлена система промышленной автоматизации SIMATIC WinCC V7.5, основным назначением которой является сбор и визуализация параметров технологического процесса и оперативное управление им.

«При проектировании индустриального киберполигона мы выбрали решения «Сименс» ввиду их широкой распространенности в электроэнергетике как в Российской Федерации, так и за рубежом. Мы также учитывали значительные усилия компании по внедрению в устройства встроенных средств защиты информации. В дальнейшем компания «Сименс» сможет воспользоваться одним из сервисов киберполигона - «охотой за уязвимостями» (bug bounty), которая

проводится в интересах и по запросу вендоров программного и аппаратного обеспечения» - комментирует Михаил Климов, директор по развитию направления «Национальный Киберполигон» компании «Ростелеком-Солар». ***(Владимир Бахур. «Ростелеком» использует аппаратные и программные решения «Сименс» при создании киберполигона // CNews (https://www.cnews.ru/news/line/2020-12-15_rostelekom_ispolzuet). 15.12.2020).***

***

«Україна розраховує, що кіберсанкції стануть одним з пунктів порядку денного двосторонньої співпраці з Європейським Союзом.

Про це заявив представник України при ЄС Микола Точицький на онлайн-брифінгу в рамках конференції керівників закордонних дипломатичних установ…

«Надзвичайно важливою для нас залишається співпраця з Європейським Союзом у так званому кібердіалозі. Ми очікуємо, що кіберсанкції стануть одним з пунктів порядку денного нашої двосторонньої співпраці з ЄС», - сказав Точицький.

Він також зазначив, що попри пандемію COVID-19, діалог України з ЄС у цьому році був дуже інтенсивним, і практично всі завдання, які ставив собі Київ, попри ситуацію з коронавірусом, були виконані.

«Залишається на основі висновку Венеційської комісії завершити питання з тією конституційною кризою, яка виникла наприкінці цього року. Я сподіваюсь, що наші законодавці після ґрунтовної і доволі ефективної роботи Венеційської комісії врахують усі її пропозиції і побажання», - резюмував посол.

Як повідомляв Укрінформ, Євросоюз 22 жовтня оголосив про рішення застосувати обмежувальні заходи проти двох росіян та однієї установи РФ за кібератаку на Бундестаг, скоєну 2015 року.

Як указується на сайті Європейської ради, під санкції потрапили офіцери ГРУ Генштабу ЗС РФ Дмитро Бадін з 85-го головного центру спеціальних служб, та Ігор Костюков, керівник головного директорату ГРУ.

Санкційні обмеження також запроваджено безпосередньо проти 85-го головного центру спецслужб ГРУ.

Як зазначається, санкції передбачають заборону на подорожі, а також заморожування активів фізичних осіб та установ, включених до переліку. Окрім того, особам та організаціям ЄС заборонено надавати їм будь-яке фінансування.

Після цього рішення санкційний список за кібератаки проти Євросоюзу або його країн загалом охоплює вісьмох осіб та чотири установи.

Правові рамки для запровадження санкцій за кібератаки проти Євросоюзу були прийняті Європейською радою у травні 2019 року, а вперше застосовані - у липні 2020-го». ***(Україна хоче включити у діалог з ЄС питання кіберсанкцій – посол // Укрінформ (https://www.ukrinform.ua/rubric-polytics/3158541-ukraina-hoce-vkluciti-u-dialog-z-es-pitanna-kibersankcij-posol.html). 21.12.2020).***

***

«У Міністерстві охорони здоров'я зауважили, що продовжують співпрацювати з американськими партнерами з приводу багатьох питань, зокрема й кібербезпеки. Таким чином Київ відреагував на ініціативу щодо

фінансової допомоги від Вашингтона, аби замінити обладнання компанії Huawei у міністерстві. Про це повідомляє ONLINE.UA з посиланням на пресслужбу зовнішньополітичного відомства. За оприлюдненими даними, співпраця України та США водночас поширюється на політичну, економічну, військову сфери. "Одним з важливих напрямків такої співпраці є взаємодія у сфері кіберзахисту і кібербезпеки. Ми високо цінуємо допомогу, яку американська сторона надає на посилення кіберздібностей нашої держави. Така допомога може передбачати, зокрема, і заміну застарілого обладнання новими зразками", — пояснили в МЗС, Дипломати додали, відповідне питання вже було на обговоренні з Вашингтоном. Подальшу перспективу заміни комп'ютерної техніки визначать після оцінки "фінансових ресурсів і за результатами двосторонніх консультацій". Нагадаємо, компанія Huawei знаходиться під американськими санкціями, державні установи країни відмовилися від продукції китайського виробника через ризики для кібербезпеки.

Між США та КНР упродовж останніх років тривають регулярні зіткнення у галузі технологій і торгівлі. Як повідомляв ONLINE.UA, в американському уряді виступили із заявою про готовність допомогти фінансово Україні, аби на її території не встановлювали 5G-обладнання від компанії Huawei. Йдеться про покриття різниці в ціні під час придбання відповідної техніки від іншого постачальника. Вашингтон оцінює Huawei як розробника шпигунської техніки». ***(Олексій Грушевський. МЗС відреагувало на ідею США про фінансову допомогу з кібербезпеки // ONLINE.UA (https://novyny.online.ua/mzs-vidreaguvalo-na-ideyu-ssha-pro-finansovu-dopomogu-z-kiberbezpeki_n828453/). 23.12.2020).***

***

Коронавірус COVID-19 та питання кібербезпеки

«Американська корпорація IBM – один із найбільших світових виробників усіх видів комп'ютерів і програмного забезпечення – виявила ознаки того, що кіберзлочинці збирають інформацію щодо ланцюжка поставок вакцин проти COVID-19…

В IBM заявили, що її фахівці виявили "глобальну фішинг-кампанію", націлену на організацію зі зберігання і транспортування вакцин проти COVID-19.

Зокрема підрозділ кібербезпеки IBM заявив про виявлення групи хакерів, яка працює над збором інформації про різні аспекти «холодового ланцюга» - технології безперервного дотримання оптимальної низької температури при зберіганні та транспортуванні біологічних препаратів, зокрема вакцин, від підприємства-виробника до споживача.

Зловмисники розсилають своїм жертвам фішингові електронні листи, нібито, від імені китайської компанії Haier Biomedical, що є постачальником холодових ланцюгів. Метою кіберзлочинців є викрадення облікових даних для авторизації в електронній пошті та інших додатках.

Хакери доклали «надзвичайних зусиль», сказала аналітик IBM Клер Забоєва.

«Той, хто проводив цю кампанію, був у курсі того, які продукти були задіяні в ланцюзі поставок для доставки вакцини», - сказала вона.

В Haier Medical не прокоментували дану інформацію…». ***(IBM попереджає, що хакери збирають дані про шляхи доставки вакцин проти COVID-19 // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (https://day.kyiv.ua/uk/news/041220-ibm-poperedzhaye-shcho-hakery-zbyrayut-dani-pro-shlyahy-dostavky-vakcyn-proty-covid-19). 04.12.2020).***

***

«В результаті кібератаки в Естонії хакери отримали доступ до даних тисяч хворих COVID-19…

"23 листопада хакерам вдалося отримати доступ до даних 9 158 хворих на коронавірус, що стосувалися обставин їхнього зараження. Агентство охорони здоров'я обіцяє сконтактувати з такими пацієнтами", - йдеться у повідомленні.

За інформацію Управління з інформаційних систем, йдеться про три окремі кібератаки на три міністерства - Міністерство економіки й комунікацій, Мінсоцполітики і Міністерство закордонних справ, а також системи Агентства охорони здоров'я (Terviseamet).

Відповідальний за національну політику кібербезпеки у Міністерстві економіки й комунікацій Рауль Рікк повідомив, що наразі загрози для нормального функціонування систем усіх цих відомств немає.

За словами Рауля Рікка, зловмисники не отримали доступу до інформації, що становить державну таємницю.

Поліція за фактом атаки відкрила кримінальне провадження». ***(В Естонії хакери отримали доступ до даних тисяч людей інфікованих COVID-19 // Espreso.tv (https://espreso.tv/news/2020/12/01/v_estoniyi_khakery_otrymaly_dostup_do_danykh_tysyach_lyudey_infikovanykh_covid_19). 01.12.2020).***

***

«Хакери змогли зламати базу даних вакцини від коронавірусу.

Йдеться про документи на реєстрацію вакцини, створеної Pfizer і BioNTech. Поки невідомо, чи отримали зловмисники доступ до персональних даних учасників випробувань вакцини.

Європейське агентство з лікарських засобів (EMA) пообіцяло провести розслідування того, що сталося, йдеться в заяві BioNTech.

Яке хакерське угруповання здійсниле атаку, не повідомляється…

В останні місяці кількість хакерських атак на виробників вакцин і органи охорони здоров'я зросла. Зокрема, компанія Microsoft в листопаді заявила, що за останні місяці сім компаній-розробників вакцини від коронавірусу в Канаді, Франції, Індії, Південної Кореї і США піддалися атакам хакерів з Росії та Північної Кореї». ***(Хакери дісталися до даних про вакцину від коронавірусу Pfizer і BioNTech // Ракурс (https://racurs.ua/ua/n147583-hakery-distalysya-do-danyh-pro-vakcynu-vid-koronavirusu-pfizer-i-biontech.html). 10.12.2020).***

***

«Правительственные чиновники и группы здравоохранения все больше обеспокоены национальными государствами и преступными хакерами, нацеленными на цепочку поставок вакцин COVID-19.

Опасения усилились по мере того, как США готовятся к выпуску первых вакцин в конце этого месяца, а группы, участвующие в создании и доставке вакцин, являются основной целью для потенциальных кибератак.

«Мы заметили рост атак на все аспекты цепочки поставок вакцин, от исследований до производства и распространения», - сказал The Hill в пятницу Марк Роджерс, исполнительный директор по кибербезопасности в программной группе Okta.

Роджерс, который помогает руководить лигой COVID-19 CTI, которая отслеживает и помогает защищаться от кибератак, нацеленных на группы здравоохранения, отметил, что в Лиге наблюдались «усиленные» кибератаки, направленные на медицинские учреждения, что соответствует все более позитивным новостям о разработке вакцин.

«Я подозреваю, что все стороны киберпреступного подполья, от обычных преступников до национальных государств, признают, что вакцины представляют собой прекрасную возможность, и реагируют соответствующим образом», - сказал Роджерс.

Северная Корея была среди таких стран: The Wall Street Journal недавно сообщил, что северокорейские хакеры атаковали по крайней мере шесть фармацевтических групп в США, Великобритании и Южной Корее, участвовавших в разработке вакцины, включая Johnson & Johnson и Novavax.

«Все директора по информационной безопасности [главные сотрудники по информационной безопасности] в сфере здравоохранения наблюдают попытки проникновения со стороны национальных государственных субъектов, а не только Северной Кореи, каждую минуту каждого дня, - заявила ранее Марен Эллисон на виртуальном киберсаммите Института Аспена эта неделя.

Представитель Novavax сообщил The Hill в заявлении в пятницу, что компания «осведомлена о продолжающихся иностранных угрозах, выявленных в новостях».

«Мы уверены, что сможем продолжить работу над нашим кандидатом на вакцину COVID-19 без каких-либо сбоев, и что эти вторжения не представляют опасности для целостности наших данных», - сказал представитель.

Но поскольку в последние недели возросли опасения по поводу процесса хранения, доставки и доставки вакцин COVID-19 после их утверждения, хакеры все чаще рассматривают группы, не относящиеся к здравоохранению, в цепочке поставок вакцин в качестве потенциальных целей.

Группы холодного хранения, необходимые для транспортировки и хранения кандидатов на вакцины COVID-19 при чрезвычайно низких температурах, например, недавно представленная Pfizer, все чаще оказываются под прицелом.

Отчет на прошлой неделе от IBM предупреждает о «глобальной фишинг кампании» группы таргетинга, связанные с холодильниками для процесса вакцины COVID-19. Исследователи писали, что «точное нацеливание на руководителей и

ключевые глобальные организации является потенциальным признаком торгового мастерства нации и государства».

Агентство кибербезопасности и безопасности инфраструктуры (CISA) Министерства внутренней безопасности выпустило соответствующее предупреждение, побуждающее организации США, участвующие в распространении вакцины в рамках операции Warp Speed, ознакомиться с выводами IBM.

По крайней мере, одна крупная группа холодного хранения уже была атакована до того, как были выпущены эти предупреждения.

Americold, крупнейший поставщик холодильных складов в США и глобальный оператор холодильных складов, в ноябре сообщил Комиссии по ценным бумагам и биржам (SEC), что обнаружил, что его сети подверглись кибератаке.

«Компания приняла незамедлительные меры для сдерживания инцидента и реализовала планы обеспечения непрерывности бизнеса, где это было необходимо, для продолжения текущих операций», - написала компания в заявке. «Компания уведомила и тесно сотрудничает с правоохранительными органами, экспертами по кибербезопасности и юрисконсультами».

Андре Пиенаар, основатель фирмы C5 Capital, которая помогала сформировать группу из около 40 крупных компаний в области кибербезопасности, известных как Cyber Alliance to Defend Our Healthcare, указал на атаку на Америкольд как на пример слабого звена в цепочке поставок вакцин.

«Точкой атаки в цепочке поставок, на которую нацелились хакеры, были холодильные склады», - сказал Пиенаар изданию The Hill. «Компании холодного хранения ужасающе мало инвестируют в кибербезопасность, и хакеры могут проникнуть в их системы, взломав промышленные средства контроля, а не фишинговые электронные письма».

Группы холодильного хранения - не единственные организации, связанные с вакцинами и лечением COVID-19, на которые были направлены меры.

Мередит Харпер, директор по информационной безопасности фармацевтической группы Eli Lilly, которая работала над разработкой препарата на основе антител против COVID-19, заявила на саммите Института Аспена, что в ее компании произошел значительный всплеск атак на сторонние группы, связанные с выполнением работы Эли Лилли.

«Вероятно, в этом году мы совершили намного больше инцидентов, связанных с нашими третьими сторонами, чем мы видели за последние несколько лет», - сказал Харпер.

Правительственные чиновники говорят, что они знают об угрозах цепочке поставок вакцин и работают над их устранением.

Исполняющий обязанности директора CISA Брэндон Уэльс сказал, что его агентство работает с Агентством национальной безопасности и ФБР, чтобы гарантировать безопасность процесса поставок вакцины Operation Warp Speed. Он отметил, что иностранные страны нацелены на инициативы по исследованию и разработке вакцины COVID-19 с момента начала пандемии.

«Нам нужно сделать еще больше, чтобы продвигаться все глубже и глубже в эти цепочки поставок, причем не только крупных компаний, стоящих за вакциной, но и компаний, которые будут иметь важное значение для получения этой вакцины от производства через распространение, эту последнюю милю до американского народа», - сказал Уэльс на саммите Института Аспена на прошлой неделе.

Пиенаар сказал, что помимо цепочки поставок вакцины его группа также отслеживала угрозы для сбора данных о пациентах, связанные с иммунизацией.

«Эффективные программы иммунизации зависят от точных систем сбора данных и программного обеспечения», - сказал Пиенаар. «Согласно нашим данным, это будет следующий вектор атаки хакеров».

Роджерс отметил, что, хотя предстоящее одобрение и внедрение вакцины COVID-19 является хорошей новостью для общественного здравоохранения, угроза кибератак, прерывающих этот процесс, остается высокой.

«Возможно, мы приближаемся к тому, что выглядит как финиш, но сейчас не время для нас отвлекаться от мяча», - сказал Роджерс. «Нам необходимо удвоить бдительность и обеспечить круглосуточное наблюдение и охрану ключевых организаций, занимающихся распространением этих столь необходимых вакцин». ***(MAGGIE MILLER. Hackers threaten to disrupt COVID-19 vaccine supply chain // CAPITOL HILL PUBLISHING CORP. (https://thehill.com/policy/cybersecurity/528852-hackers-threaten-to-disrupt-covid-19-vaccine-supply-chain). 06.12.2020).***

***

«Moderna Inc. сообщила в понедельник, что Европейское агентство по лекарственным средствам (EMA) сообщило, что некоторые документы, связанные с переговорами перед подачей заявки на вакцину от COVID-19, были незаконно доступны в результате кибератаки на регулятор лекарственных средств.

EMA, занимающееся оценкой лекарств и вакцин для Европейского Союза, сообщило ранее в этом месяце, что оно подверглось кибератаке, которая также предоставила хакерам доступ к документам, связанным с разработкой вакцины COVID-19 Pfizer Inc и BioNTech.

Moderna сообщила, что ее представление в EMA не включало никакой информации, идентифицирующей отдельных участников исследования, и в настоящее время нет информации о том, что какие-либо участники были идентифицированы каким-либо образом». ***(Moderna COVID-19 vaccine documents accessed in EMA cyberattack // Reuters. (https://www.reuters.com/article/us-ema-cyber-moderna/moderna-covid-19-vaccine-documents-accessed-in-ema-cyberattack-idUSKBN28P00E?il=0). 15.12.2020).***

***

«В связи с ростом числа случаев COVID-19, школы и университеты нависают над очередным витком атак, поскольку они переходят на каникулы и готовятся к весеннему семестру. Согласно недавней статье в Wall Street Journal, с начала пандемии в марте было «около трех десятков атак программ-вымогателей

на школьные округа». Конечно, это не полная картина, поскольку, как указывает журнал, некоторые школы переходят на «резервные серверы, которые [избегают] атак, или незаметно платят выкуп, никогда не предавая его гласности».

В условиях ограниченности ресурсов службами безопасности, особенно когда государственные и общественные школы и университеты сталкиваются с нехваткой ресурсов из-за коронавируса, образовательные учреждения и другие организации должны найти способ повысить свою безопасность, чтобы уменьшить распространение угроз, таких как вымогатели. Достаточно плохо бороться с биологическим вирусом, таким как COVID-19, но еще хуже, когда компьютерные и сетевые вирусы также начинают распространяться.

Постоянно увеличивающиеся поверхности угроз

Согласно недавнему отчету о тенденциях в области безопасности приложений, 20 процентов компаний, занимающихся разработкой программного обеспечения, не тестируют программные угрозы. Это означает, что на рынке появляется множество программного обеспечения с неизвестными уязвимостями, которые могут создать лазейку в сети организации.

Кроме того, данные Palo Alto Networks показывают, что четыре из пяти открытых эксплойтов публикуются до публикации CVE, что означает, что злоумышленники могут нанести удар до того, как будут выпущены официальные отчеты об уязвимостях или патчи. В среднем эти эксплойты публикуются за 23 дня до выпуска CVE. Другими словами, у злоумышленников есть почти месяц, чтобы воспользоваться уязвимостью, прежде чем будут выпущены CVE и обновления, чтобы остановить атаки. Это не сулит ничего хорошего для тех, кто пытается защитить свои сети, тем более, что количество атак программ-вымогателей выросло из-за попыток хакеров получить прибыль.

Согласно статье, опубликованной в сентябре прошлого года, хакеры обнародовали информацию о студентах недалеко от Лас-Вегаса после того, как официальные лица не заплатили выкуп. То, что когда-то было простым выбором - заплатить выкуп или нет - теперь не так просто, потому что хакеры не только шифруют данные на серверах, но и крадут данные, чтобы опубликовать их позже, если выкуп не будет уплачен.

Похоже, что эти постоянно растущие угрозы не замедляются, и организации, учебные заведения и сотрудники должны быть уверены, что защитят себя и уменьшат поверхность для атак.

Как повысить уровень безопасности

По мере того как злоумышленники становятся все более и более хитрыми, простых потоковых данных уже недостаточно для обнаружения постоянно меняющихся шаблонов вредоносного ПО, которое они пишут. Машинное обучение - действительно единственный способ обнаружить некоторые из самых умных вредоносных программ.

В недавнем отчете, опубликованном этим летом, Gartner обнаруживает, что «применение машинного обучения и других аналитических методов к сетевому трафику помогает предприятиям обнаруживать подозрительный трафик, который отсутствует у других инструментов безопасности».

Чтобы обеспечить безопасность сети и проверить, как вредоносные программы могут перемещаться по ней, учебным заведениям и предприятиям необходимо развернуть аналитику сетевого трафика, способную использовать машинное обучение для быстрого определения уязвимостей безопасности и выявления нарушений. Уже недостаточно просто собирать метаданные трафика и надеяться, что аналитики заметят аномалии.

Люди: по-прежнему большая проблема

Обнаружение сети и реагирование на нее, аналитика сетевого трафика и аналогичные платформы вместе с технологиями SIEM помогают командам безопасности и сетям определять, когда и где вредоносное ПО проникло в сеть. Но люди также должны быть обучены тому, как предотвратить эти атаки. Большинство сотрудников, студентов и других пользователей корпоративных сетей не всегда осведомлены о правильном использовании и сами могут представлять угрозу для сети.

Организации должны предоставить своим пользователям некоторый уровень образования в отношении передовых методов для дальнейшего уменьшения поверхности угрозы. CIOReview с использованием данных из Центра управления безопасностью F5 обнаружил, что количество фишинговых атак увеличилось на 220 процентов во время пика COVID-19. Согласно статье, «[я] лиц и [организации] также должны постоянно обучаться новейшим методам, используемым мошенниками. Важно отметить, что необходимо сделать большой акцент на том, как злоумышленники используют новые тенденции, такие как COVID-19».

Обучая людей, использующих сеть, обнаруживать фишинг и другие злонамеренные попытки, организации могут повысить уровень своей безопасности и общую осведомленность о вредоносных угрозах.

Воспользовавшись возможностями машинного обучения на множестве сегодняшних платформ, обучая сотрудников, студентов и пользователей лучшим методам предотвращения фишинга и других атак, а также продолжая использовать многоуровневый подход к безопасности, учреждения, которые изо всех сил пытаются оставаться открытыми во время этой пандемии, могут эффективно повышать свою сетевую безопасность, чтобы обеспечить безопасную и надежную сеть, которая снижает риск воздействия внешних хакеров». ***(Justin Jett. How to Increase Your Security Posture with Fewer Resources // Threatpost (https://threatpost.com/increase-security-posture-fewer-resources/162382/). 17.12.2020).***

***

«Хакеры из северокорейского национального государства, которых проследили как Lazarus Group, недавно взломали организации, участвующие в исследованиях COVID-19 и разработке вакцин.

Для этого они проникли в сети фармацевтической компании и государственного министерства здравоохранения в сентябре и октябре соответственно.

После проникновения в свою сеть хакеры из штата Северной Кореи развернули вредоносное ПО Bookcode (которое используется исключительно Lazarus) и wAgent с возможностями бэкдора.

Бэкдоры, используемые для постэксплуатации

«В обеих атаках использовались разные кластеры вредоносных программ, которые не сильно пересекаются», - сказал эксперт по безопасности Kaspersky Сонсу Пак в отчете APT.

«Тем не менее, мы можем подтвердить, что оба они связаны с группой Lazarus, и мы также обнаружили совпадения в процессе постэксплуатации».

Последней полезной нагрузкой в атаке на министерство здравоохранения стал wAgent, вредоносная программа, разработанная для развертывания дополнительных полезных данных с командно-контрольного сервера, включая постоянный бэкдор, и загрузки их в память скомпрометированных систем.

Во время атаки 27 октября вредоносное ПО wAgent имело «ту же схему заражения, что и вредоносное ПО, которое группа Lazarus ранее использовала для атак на криптовалютные предприятия».

В атаке на фармацевтическую компанию 25 сентября операторы Lazarus использовали вредоносное ПО Bookcode для сбора системной информации, «дампа реестра, содержащего хеши паролей» и информации Active Directory.

Несмотря на то, что в прошлом хакеры использовали это вредоносное ПО для атаки на цепочку поставок и с помощью целевого фишинга, в этом случае вектор атаки не был обнаружен.

«Лаборатория Касперского» не раскрыла личность фармацевтической компании, скомпрометированной в результате этих атак, но они рассказали, что она участвует в разработке вакцины от COVID-19, а также «уполномочена производить и распространять вакцины против COVID-19».

Хотя в настоящее время в разработке находится несколько вакцин против COVID-19, только те, которые разработаны этими организациями, достигли статуса разрешения / одобрения в США, Великобритании, России, Китае и других странах (следовательно, цель должна быть среди них):

Pfizer-BioNTech

Moderna, Sinovac

Уханьский институт биологических продуктов

Гамалея НИИ

Пекинский институт биологических продуктов

ФГБНУ Государственный научный центр вирусологии и биотехнологии

«Эти два инцидента свидетельствуют об интересе группы Lazarus к разведывательной информации, связанной с COVID-19», - добавил Пак.

«Хотя группа в основном известна своей финансовой деятельностью, это хорошее напоминание о том, что она может заниматься и стратегическими исследованиями.

«Мы считаем, что все организации, которые в настоящее время занимаются такими видами деятельности, как исследования вакцин или урегулирование кризисных ситуаций, должны быть в состоянии повышенной готовности к кибератакам».

Исследование COVID-19 во главе нескольких целевых списков

С самого начала пандемии информация, которая могла бы ускорить разработку вакцины против COVID-19, постоянно находилась под пристальным вниманием спонсируемых государством субъектов угроз.

Например, организации по исследованию вакцин из Канады, Великобритании и США в течение года подвергались нескольким атакам, которые координировала российская хакерская группа APT29, спонсируемая государством.

Субъекты угроз, связанные с Китайской Народной Республикой (КНР), также были причастны к аналогичным атакам, о чем сообщили ФБР и DHS-CISA в совместном объявлении общественной службы.

Microsoft также конфисковала домены, используемые для киберпреступлений, связанных с COVID-19, и предупредила на этой неделе о новых схемах мошенничества, в которых мошенники используют интерес общественности к вакцине COVID-19 для сбора личной информации и кражи денег.

Ранее в этом месяце злоумышленники также атаковали организации, участвующие в исследованиях COVID-19, Европейское агентство по лекарственным средствам (EMA) и Комиссию ЕС, а также организации, связанные с холодовой цепью вакцины COVID-19, включая хранение и доставку в безопасном месте. Температуры». ***(Sergiu Gatlan. North Korean state hackers breach COVID-19 research entities // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/north-korean-state-hackers-breach-covid-19-research-entities/). 24.12.2020).***

***

«По прогнозам экспертов HP Inc., в 2021 году негативное влияние пандемии COVID-19 на безопасность ИТ-инфраструктур компаний продолжится, что сформирует ряд актуальных тенденций.

Радикальные изменения рабочих процессов и другие последствия COVID-19 стали причиной ослабления защиты ИТ-инфраструктуры. Неэффективная реализация удаленного доступа, уязвимости в VPN и нехватка персонала, способного решить эти проблемы, привели к тому, что корпоративные данные оказались под угрозой несанкционированного доступа.

Повышенному риску подвержены и домашние устройства: возросшее число удаленных сотрудников создало такие условия, когда злоумышленники легко подключаются к корпоративным ПК через незащищенные локальные сети, а пользователи не имеют возможности оперативно связаться с ИТ-специалистами и предотвратить угрозу несанкционированного вторжения.

При удаленной работе у сотрудников размывается грань между выполнением рабочих и личных задач на корпоративном устройстве, а безобидные действия — например, чтение личной электронной почты — могут иметь серьезные последствия. Компании будут все чаще сталкиваться с эмоциональным выгоранием сотрудников, что может привести к росту ошибок.

Программы-вымогатели стали излюбленным инструментом киберпреступников, и эта тенденция продолжится в следующем году. Рост числа

программ-вымогателей стимулирует развитие целой экосистемы преступных инструментов. Вредоносные ПО рассылаются по электронной почте, а такие вирусы, как Emotet, TrickBot и Dridex, часто предшествуют внедрению этих программ. Многие криминальные группы с помощью агрессивных инструментов взламывают контроллеры доменов, которые часто оказываются самыми подходящими точками для внедрения программ-вымогателей.

Рост числа двухэтапных вымогательских кампаний, в рамках которых данные о жертве фильтруются перед шифрованием, особенно сильно ударит по государственным структурам, располагающим большим количеством персональных данных.

В 2021 году появится больше инновационных фишинговых приманок, предназначенных для обмана пользователей и усложнения идентификации атак. Самый инновационный метод массового фишинга, который наблюдается сегодня, это перехват электронной почты ботнетом Emotet. Ботнет автоматически создает письма-приманки, используя данные, украденные из взломанных сервисов электронной почты. Эти данные впоследствии используются в переписках, что делает их очень убедительными и подталкивает жертвы открывать файлы с вредоносным ПО.

Перспектива продолжения режима самоизоляции побуждает людей обмениваться большим количеством личной информации в Интернете, которая может стать оружием в руках киберпреступников. «Уэйлинг» — вид фишинга, нацеленный на руководителей высшего звена, станет еще более опасным, поскольку киберпреступники смогут использовать персональную информацию, найденную или украденную в Интернете, для создания убедительных писем-приманок на адреса корпоративной почты. При этом хакеры будут активно эксплуатировать острые темы 2020 года, чтобы подтолкнуть людей к открытию вредоносных электронных писем. Это может быть информация о вакцинах от COVID, предупреждения о финансовых проблемах или политической нестабильности.

Одной из отраслей, подверженной наибольшему риску в 2021 году, станет сфера здравоохранения. Медицинские организации, как правило, не имеют достаточных ресурсов для защиты ИТ-инфраструктур, не склонны к изменениям и медленно внедряют инновации. Образование также соответствует критериям уязвимости и может стать одной из основных мишеней. При этом угроза распространяется не только на больницы и медицинские учреждения, но и на более крупные исследовательские центры. Участвуя в гонке за созданием новой вакцины, фармацевтические компании и исследовательские центры будут сталкиваться с повышенными рисками.

Производители автомобилей, специализирующиеся на электрическом транспорте, также станут мишенями для кибератак в связи с ростом их престижа и прибыли. Кроме того, можно ожидать рост числа хакерских атак на критические инфраструктуры и промышленный Интернет вещей (IIOT).

Традиционные способы защиты доступа к корпоративной сети, приложениям и данным больше не работают, стратегия построения защиты сети по периметру устарела. Кроме того, с годами децентрализованность персонала привела к росту

популярности модели SaaS — это означает, что критически важные данные оказываются за пределами локальных корпоративных серверов. Организациям приходится защищаться от неизвестных ранее угроз, поэтому такие технологии, как биометрия, будут активно использоваться компаниями в будущем.

Нулевое доверие — лучший подход для обеспечения защиты информации при удаленной работе, однако для эффективного управления идентификацией и доступом, система должна быть простой в использовании. Ключевой приоритет модели нулевого доверия — качественные методы аутентификации, например, биометрия.

2020 год продемонстрировал острую необходимость внедрения новых подходов обеспечения безопасного удаленного доступа к оконечным устройствам и защищенного управления распределенной инфраструктуры конечных точек. В будущем каждый элемент ИТ-инфраструктуры станет полем битвы за кибербезопасность, от ПК и смартфонов удаленных сотрудников до промышленных компонентов Интернета вещей. Организациям необходимо адаптировать системы безопасности и управления, внедрять необходимые технологические инновации в рабочие процессы.

Такие технологии, как микровиртуализация, прозрачны для конечных пользователей. Это означает, что они с уверенностью могут открывать вложения электронной почты и загружать файлы, зная, что система защитит их устройство от проникновения вируса. Этот подход к защите не оставляет хакерам шансов, помогая организациям справляться с любыми угрозами как в 2021 году, так и в долгосрочном будущем.

«Этот год выдался тяжелым как для частного бизнеса, так и для государственных и социальных структур. Особенно активным атакам подверглись госучреждения, производственные предприятия, медицинские и образовательные организации, а также финансовая отрасль. Переход к удаленной работе расширил фронт атак и усложнил жизнь службам информационной безопасности. Это означает, что дни, когда основная задача состояла в защите сети по периметру, остались позади. Сегодня необходимо смещать акценты на обеспечение защиты конечных точек. Весь 2020 год мы были свидетелями повышения целенаправленности хакерских атак, использования изощренных приманок, побуждающих пользователей совершать рискованные действия. В следующем году мы увидим дальнейшее развитие этих тенденций, увеличение числа хитроумных целевых взломов, направленных на пользователей и конечные точки, — прокомментировал Павел Анохин, генеральный директор HP Inc. в России. — Организации не могут позволить себе игнорировать возрастающую угрозу и просто надеяться на улучшение ситуации, поэтому крайне важно обеспечить защиту оконечных устройств, что позволит им всегда быть на шаг впереди киберпреступников». ***(Владимир Бахур. Эксперты HP определили 6 основных тенденций в области кибербезопасности на 2021 год // CNews (https://www.cnews.ru/news/line/2020-12-22_eksperty_hp_opredelili_6_osnovnyh). 22.12.2020).***

***

«Commvault публикует прогнозы ведущих экспертов компании по рынку управления и хранения данных на 2021 год.

Дон Фостер, вице-президент по глобальным продажам, отметил: «Технологии Deep Fake простимулируют рост рынка решений для тестирования целостности и верификации данных».

Благодаря совершенству искусственного интеллекта (AI) технологии Deep Fake на базе AI способны создавать реалистические фотографии и видео, на которых люди делают вещи, которых они в действительности никогда не делали. Эти технологии создают новые риски – компаниям становится сложнее гарантировать, что их картинки, видео и другие потоки данных не были изменены с помощью AI.

Риск ошибки из-за использования данных, измененных с помощью технологий Deep Fake растет каждый день. В 2021 году компаниям потребуются решения для проверки целостности данных и их верификации, позволяющие выявить изображения, видео и другие потоки данных, измененные с помощью AI. Лидеры ИТ-индустрии и стартапы выпустят новые решения для проверки целостности данных и их верификации, которые защитят эти компании от мошенников, использующих технологии Deep Fake.

COVID-19 заставил многие компании ускорить переход в облачные инфраструктуры, однако теперь компании вынуждены тратить значительную часть своего ИТ-бюджета на оплату хостинга в публичных облаках приложений, изначально разработанных для развертывания во внутренней ИТ-инфраструктуре, а не в облаке.

Пандемия COVID-19 еще раз продемонстрировала гибкость и масштабируемость, а также необходимость в разработке долговременной стратегии развития предприятия, ориентированной на использование облаков. В 2021 году ИТ-отделы начнут преобразовывать свои приложения и рабочие нагрузки в “родной” для облаков формат и сделают это переформатирование одним из главных задач цифровой трансформации бизнесу. После такой оптимизации компании смогут сократить затраты на оплату облачных сервисов.

Из-за COVID-19 цифровая трансформация мировой экономики значительно ускорилась, и руководители компаний осознали, что теперь цифровые бизнесы уже не только помогают основному бизнесу, но сами стали основным бизнесом их компаний. Теперь судьба бизнеса зависит от того, сможет ли команда DevOps компании предоставить потребителям цифровые сервисы сразу же как только в них возникнет потребность.

Мэттью Тайрер, руководитель направления продуктового маркетинга, сказал: «Информационная безопасность, Governance и другие средства аналитики данных придут в облака».

В 2020 году предприятия по всему миру ускоренно переносили приложения и рабочие нагрузки в облака в связи с переходом многих сотрудников на работу из дома, однако эти компании обнаружили, что в облаках у них нет возможности применять те средства защиты данных, выполнения требований governance и других инструментов аналитики, которые они раньше использовали внутри своей корпоративной инфраструктуры. А тем временем киберпреступники

совершенствуют свои инструменты, регулирующие органы требуют выполнять требования GDPR и других законов независимо от того, хранятся данные в корпоративном дата-центре или в публичном облаке.

Для многих наших клиентов одной из главных задач в новом году будет применение в облаках основных средств защиты данных, управления данными и аналитики, которые используются в их корпоративных дата-центрах. Мы ожидаем быстрый рост спроса на решения для аналитики данных, с помощью которых компании смогут проводить аудит своих данных, выполнять требования законодательства о защите персональных данных, защитить данные от программ-вымогателей и других киберугроз, и быстро восстанавливать данные после аварий независимо от того, хранятся они внутри корпоративной инфраструктуры или в облаке.

Манодж Наир, глава направления Metallic, сказал: «Перевод сотрудников на удаленку создаст для их компаний новую проблему «гравитации данных».

Из-за COVID-19 часть персонала компаний перешла на удаленный режим работы из дома, а многие сотрудники продолжат работать из дома даже после окончания пандемии, а это значит, что их данные будут храниться вне офиса компании. В 2021 года резко возрастут инвестиции корпораций в технологии и сервисы, которые решают проблему «гравитации данных». Например, в корпоративном секторе есть большой спрос на внедрение новых технологий 10-гигабитных проводных и 5-гигабитных беспроводных сетей, с помощью которых можно обеспечить быструю, гибкую, надежную и безопасную связь между данными на границе сети компании и используемыми ею облаками. В следующем году будут активно внедряться решения Backup as a Service (BaaS) и другие решения интеллектуального управления данными, которые обеспечат защиту, хранение в соответствии с требованиями законодательства и другие средства контроля для работы с распределенными данными, остающимися на границе сети компании.

COVID-19 еще больше обострил проблему кибератак – после начала пандемии число атак выросло до 4000 в день. Для отражения новых угроз предприятия будут применять стратегию многоэшелонной обороны Defense-In-Depth, сочетающую обнаружение атак, безопасность данных и их резервное копирование, которое позволяет при наихудшем варианте развития событий быстро восстановить данные после нападения программ-вымогателей и других кибератак. Компании будут активно внедрять новые решения Backup as a Service (BaaS), которые позволяют быстро восстановить данные если отдельные решения информационной безопасности и встроенные функции безопасности приложений не смогли отразить кибератаку. Компании, у которых есть все три компонента стратегии многоэшелонной обороны (обнаружение угроз, защита данных и резервное копирование данных), смогут успешно отразить любые типы кибератак.

Ранжа Раджагопалан, вице-президент по продуктовому менеджменту, сказал: «Компании поняли, что для защиты от атак ransomware нужен план обеспечения непрерывности бизнеса».

Компании наконец осознали, что нет идеальной системы информационной безопасности, поэтому нужно быть готовым к тому, что в результате атаки

вымогателей и кибератаки другого типа их данные будут зашифрованы или удалены. В следующем году компании начнут разрабатывать процедуры обеспечения непрерывности бизнеса и внедрять решения послеаварийного восстановления в расчёте не только на природные катаклизмы, но и аварии из-за кибератак. Все это позволит существенно уменьшить риски, связанные с атаками вымогателей.

Хотя руководители компаний хорошо понимают необходимость цифровых сервисов для успешного бизнеса, большинство из них рассматривает закупки и эксплуатацию корпоративной ИТ-инфраструктуры и приложений как не приносящие доход операции. Сегодня ИТ-руководители пытаются перейти на использование решений SaaS для управления кадрами, планирования ресурсов предприятия (ERP) или других бизнес-приложений, которые не являются критически-важными для их предприятия. Следует ожидать бурный рост решений SaaS, в том числе для управления данными, которые предназначены для типичных задач бизнеса. В 2021 году станет очевидно, что мы живём в мире SaaS». ***(Владимир Бахур. Эксперты Commvault представили прогнозы на 2021 год // CNews (https://www.cnews.ru/news/line/2020-12-24_eksperty_commvault_predstavili). 24.12.2020).***

***

Світові тенденції в галузі кібербезпеки

«…По результатам опроса Future of Secure Remote Work Report компании Cisco, в котором приняли участие 3000 руководителей ИТ-служб, выяснилось, что большинство организаций в лучшем случае «в какой-то мере» готовы к поддержке удаленного персонала. Безопасный доступ назвали главной проблемой кибербезопасности, с которой сталкиваются 62% организаций при поддержке удаленных работников.

В то же время ускорилось внедрение технологий, которые позволяют безопасно работать где угодно на любом устройстве, что позволит предприятиям гибко решать возможные проблемы в будущем. 66% респондентов указали, что пандемия COVID-19 приведет к наращиванию инвестиций в кибербезопасность.

Работников беспокоит безопасность средств удаленной работы, и они сомневаются в том, что компании делают все возможное для защиты их данных. Наблюдается некоторое противоречие. Потребители не хотят «никаких» или «почти никаких» изменений в том, что касается защиты персональных данных. При этом они же считают, что компании должны быть более открытыми в плане того, как они используют данные своих клиентов. Любопытно что 56% уверены, что основную роль в защите личных данных должно играть правительство, и что потребители во всем мире поддерживают законы о защите личных данных, принятые в их странах.

«Безопасность личных данных — это гораздо больше, чем просто выполнение законодательства о соответствии требованиям регулятора. Это одно из базовых прав человека, соблюдение которого обязательно для бизнеса, и которое

критично для завоевания и поддержания доверия заказчиков, — говорит Харви Янг (Harvey Jang), вице-президент и главный директор Cisco по защите личных данных. — В новом цифровом мире мы будем руководствоваться фундаментальными этическими принципами прозрачности, справедливости и подотчетности». ***(Переход на удалёнку ожидаемо принесёт проблемы с безопасностью доступа // СофтПресс (https://hi-tech.ua/perehod-na-udalyonku-ozhidaemo-prinesyot-problemy-s-bezopasnostyu-dostupa/). 08.12.2020).***

***

«Разбивка истинной стоимости программных инструментов в контексте обратного проектирования и отладки может быть не такой четкой, как кажется.

Каким критериям вы должны следовать при поиске программного обеспечения для нужд бизнеса? Цена обычно возглавляет список. И конечно же, бесплатное программное обеспечение, такое как ОС Linux, обеспечивает экономию средств, стабильность, гибкость и постоянное развитие. Никаких аргументов. Но когда дело доходит до декомпиляторов, которые используются для обратного проектирования вредоносных программ, решения становятся сложнее.

У каждого, от профессионалов кибербезопасности до любителей, есть широкий выбор отличных декомпиляторов. Но найти лучшее сочетание функций оказалось непросто. Когда дело доходит до выбора инструментов декомпиляции, в уравнение входит множество факторов, помимо цены.

Исследование Forrester на SecOps показало, что только 46 процентов компаний удовлетворены их способность обнаруживать угрозы кибербезопасности, обвиняли - отчасти - сложный инструмент безопасности.

Кроме того, меняющиеся тенденции вредоносного ПО теперь требуют большего от профессионалов в области кибербезопасности и инструментов, на которые они полагаются. Например, согласно отчету Verizon 2020 Data Breach Investigations Report, количество кибератак с использованием вредоносных программ немного снизилось. Однако вредоносное ПО, использованное во многих из этих атак, стало более сложным, сообщает Verizon. Впоследствии интерес к вредоносному ПО для обратной инженерии усилился.

Реальная стоимость программного обеспечения

Действительно, существует множество бесплатных и недорогих декомпиляторов, которые могут помочь обычному человеку или малому бизнесу перепроектировать код - будь то вредоносное ПО или (воссоздание) потерянный исходный код из двоичного исполняемого файла. Существует Ghidra, инструмент, который, как известно, был разработан для внутреннего использования Агентством национальной безопасности США вместе с OllyDbg, x64dbg и Radare2. Но внимательно взвесьте свои варианты, говорят эксперты, и убедитесь, что вы учитываете скрытые затраты в уравнении.

Учитывайте стоимость использования нестабильных или неподдерживаемых инструментов или время, необходимое для преодоления кривой обучения при использовании неправильного декомпилятора. В то время как Интернет способствовал появлению ряда недорогих и бесплатных решений, многие из них

имеют компромисс, а именно отсутствие поддержки и отсутствующие функции. Прежде чем вкладывать время в какой-либо инструмент обратного проектирования, сделайте свою домашнюю работу. Убедитесь, что вы не увязнете в поисках недокументированных функций декомпилятора и не будете вынуждены искать обходные пути для сбоев в работе инструментов.

Во что обходится компании, когда исследователи тратят время на очистку выходного кода или ждут, пока задания просто закончатся?

Прелесть ниши реверс-инжиниринга в разнообразии инструментов. Цена никогда не должна быть единственным определяющим фактором. Современные тенденции в области вредоносных программ и новые приоритеты SecOps заставляют многих выходить за рамки цены. Надежность программного обеспечения, быстрота выполнения и поддержка поставщика становятся частью обсуждения прибылей и убытков бизнес-подразделения.

Для небольших разработчиков более надежные решения - это просто естественная эволюция. Для любителей и случайных пользователей часто достаточно бесплатных или недорогих инструментов. У таких разработчиков обычно нет мегабайтов кода, о которых нужно беспокоиться, а также у них достаточно времени для анализа.

Однако для профессионалов в области кибербезопасности предоплата за решение, которое обеспечивает быстрое расширение проектов, быстрое выполнение и оптимизированный пользовательский интерфейс, в конечном итоге приведет к лучшим результатам, довольным клиентам и более безопасным сетям.

Эти команды ограничены во времени и требуют убедительных результатов.

Приверженность будущему: команды IDA

К сожалению, бесплатные инструменты часто представляют собой разовые проекты поставщика, которым иногда не хватает текущей разработки или даже дорожной карты продукта.

Для Hex-Rays семейство инструментов IDA для обратного проектирования представляет собой особый фокус. Компания гордится тем, что удовлетворяет текущие и будущие потребности рынка. Для Hex-Rays будущее ясно. Речь идет о расширении возможностей команд, а не только об одном исследователе, копающемся в сотнях мегабайт кода функции.

Скоро появятся команды IDA, которые могут использовать возможности многих участников - из рабочих групп, часовых поясов и географических регионов. Где-то в первой половине 2021 года Hex-Rays развернет многопользовательскую поддержку для IDA вместе с поддержкой управления версиями в предстоящем выпуске команд IDA». ***(Reverse Engineering Tools: Evaluating the True Cost // Threatpost (https://threatpost.com/hex-rays-reverse-engineering-tools-evaluating-the-true-cost/161767/). 03.12.2020).***

***

«Хэнк Шлесс из Lookout обсуждает возросшие угрозы для мобильных оконечных устройств в эпоху удаленной работы, вызванной COVID-19.

Смартфоны, планшеты, приложения для совместной работы и другие современные инструменты инфраструктуры критически важны для поддержания

производительности удаленно, но они также требуют интегрированной стратегии безопасности, специально разработанной для мобильных устройств.

Пандемия коронавируса полностью изменила то, как мы работаем, обучаемся и общаемся. Вскоре после стремительного распространения вируса организации были вынуждены полностью внедрить модели работы на дому и другие удаленные модели. К счастью, сотрудники быстро доказали, что они могут быть продуктивными и успешными без прямого подключения к корпоративной сети.

Фактически, в середине марта, когда большинство организаций отправили своих сотрудников домой, в Lookout наблюдался 25-процентный скачок в использовании устройств iOS. В то же время количество мобильных фишинговых атак на частных и корпоративных пользователей резко возросло во всех регионах и отраслях. В связи со скачком iOS в период с четвертого квартала 2019 года по первый квартал 2020 года количество попыток мобильного фишинга увеличилось на 37 процентов. Киберпреступники пользуются социальной неопределенностью и тем фактом, что мы больше полагаемся на мобильные устройства, чтобы оставаться продуктивными.

Вероятно, вы уже адаптировали свою стратегию безопасности для защиты настольных компьютеров и ноутбуков сотрудников, но если вы еще не защитили мобильные устройства, еще не поздно наверстать упущенное. Вот несколько методов атаки, о которых следует помнить при выборе стратегии защиты мобильных устройств.

Вредоносные злоумышленники нацелены на мобильные устройства по определенной причине

Попытки фишинга выявить на мобильном устройстве гораздо сложнее. Кампании спарфишинга используют человеческие уязвимости, такие как наше доверие к нашим телефонам и планшетам. Они также используют небольшие мобильные экраны, чтобы скрыть контрольные знаки, которые мы привыкли идентифицировать на настольных компьютерах. Злоумышленники могут выдавать себя за законную сторону, используя, например, телефонные номера VoIP или упрощенный дизайн приложения для обмена сообщениями.

Злоумышленники также будут подделывать URL-адреса и использовать тот факт, что мобильные браузеры сокращают URL-адреса, чтобы скрыть истинную идентичность веб-страницы. Кроме того, многие люди не думают о предварительном просмотре ссылки, потому что мы привыкли просто нажимать на все, что нам присылают. В отличие от ноутбуков, выпущенных компанией, на мобильных устройствах редко устанавливаются средства защиты от фишинга или вредоносного ПО. Учитывая, что смартфоны и планшеты имеют такой же доступ к корпоративным ресурсам, они должны получать такой же уровень защиты, как и традиционные конечные точки.

Остерегайтесь Вишинга

Недавнее предупреждение от ФБР и CISA показало, что киберпреступники обратились к «вишингам», чтобы воспользоваться отсутствием защиты мобильных устройств и атаковать удаленных сотрудников. Вишинг, или голосовой фишинг, - это форма фишинга, при которой злоумышленники обманом заставляют вас передать информацию по телефону; часто выдает себя за службу поддержки или

ИТ-персонал. Поскольку вишинг основан на человеческой ошибке, меры безопасности, такие как VPN, многофакторная аутентификация и одноразовые пароли, не могут защитить от атак такого типа.

Вишинг выводит социальную инженерию на новый уровень, но цепочка уничтожений для доступа к корпоративным данным ничем не отличается от атак со сбором учетных данных через Интернет. Как только злоумышленник успешно фишит учетные данные, он может быстро получить доступ к инфраструктуре и выполнить атаку, нанеся огромный ущерб в короткие сроки. Поскольку пользователя атакуют и убеждают поделиться своими учетными данными, уязвимость заключается в человеческом поведении. Предприятиям необходимо обучать и информировать всех сотрудников о том, как выглядят мобильные фишинговые атаки, и о передовых методах, как избежать их попадания.

Фишинг и Chromebook: защитите своих удаленных учеников

Chromebook стал важным и экономичным инструментом для систем образования, предлагающих дистанционное обучение. Они соединяют студентов и преподавателей с ресурсами и помогают студентам с домашними заданиями и обучением в сочетании с Google Classroom, Google Workspace для образования и другими приложениями.

Chrome OS со всеми встроенными функциями безопасности имеет репутацию более безопасной, чем устаревшие операционные системы. Доступ к ядру недоступен, и приложения работают изолированно, что затрудняет взлом устройства при нормальном использовании. Он также имеет автоматические обновления для исправления уязвимостей. Но как бы нам ни нравилась ОС Chromebook для безопасного дистанционного обучения, Chromebook - это современное оконечное устройство, которое сталкивается с теми же проблемами безопасности, что и любые другие типы устройств.

Другими словами, фишинг и атаки на веб-контент представляют такую же угрозу для Chromebook, как и для смартфонов и планшетов. Кроме того, Chromebook использует магазин Google Play для загрузки приложений, а это означает, что если вредоносное приложение проникнет в магазин, оно также может повлиять на устройства Chrome OS. Наконец, Chromebook подвержен сетевым угрозам.

Куда мы идем отсюда?

Поскольку большинство из нас работает вне офиса, каждый из нас теперь представляет собой удаленный офис, который необходимо защитить вашей организации. Многие организации обратились к VPN при переходе на удаленную работу, но это оставляет ряд пробелов в безопасности, включая тот факт, что многие из нас не используют VPN при использовании своих мобильных устройств.

Теперь, когда работа выполняется везде, где проживает сотрудник, вы должны переместить безопасность с периметра на конечные точки. Теперь безопасность должна быть везде, где бы ни находились сотрудники. Поскольку мы продолжаем переходить к миру, ориентированному на мобильные устройства, это прекрасная возможность переосмыслить, как обеспечить постоянную безопасность вашей организации». ***(Hank Schless. As Modern Mobile Enables Remote Work, It***

Also Demands Security // Threatpost (https://threatpost.com/mobile-remote-work-security/161842/). 03.12.2020).

***

«Победители конкурса Pwnie Awards 2020 были объявлены ранее сегодня на конференции по безопасности Black Hat Europe.

Награды в области кибербезопасности - это то же самое, что премии «Оскар» и «Раззи» в совокупности для киноиндустрии.

Каждый год профессионалов в области кибербезопасности приглашают номинировать, а затем голосовать как за лучших, так и за худших в своей отрасли. Это включает в себя выбор лучших и наиболее оригинальных уязвимостей, обнаруженных за последние двенадцать месяцев, а также наихудшие отзывы поставщиков и эпические неудачи, которые в конечном итоге подвергают пользователей риску.

В течение последнего десятилетия церемония вручения наград Pwnie Awards проходила во время конференции по безопасности Black Hat USA, каждый август, в отеле Лас-Вегаса, где организаторы обычно раздают победителям в своих категориях пластмассовых кукол-пони с розовыми волосами.

Однако в этом году впервые с момента основания награда Pwnie Awards проводилась в виртуальном формате, а также была перенесена на европейскую конференцию Black Hat, которая обычно проходит в конце ноября - начале декабря. Причины? Конечно, пандемия COVID-19.

Но без лишних слов, вот победители этого года, а также ссылки на их исследования, если они доступны в Интернете:

Лучшая ошибка на стороне сервера: BraveStarr - эксплойт удаленного кода в демоне Telnet на серверах Fedora 31.

Лучшая сторона клиента ошибка: Для нулевого щелчка MMS атаки на телефонах Samsung, ошибка обнаружена командой Google Project Zero.

Лучшая ошибка повышения привилегий: Checkm8 - аппаратный джейлбрейк без исправлений для семи поколений микросхем Apple.

Лучшая криптографическая атака: Zerologon - ошибка в протоколе аутентификации Microsoft Netlogon, которая может быть выполнена путем добавления группы нулевых символов в определенные параметры аутентификации Netlogon.

Самое инновационное исследование: TRRespass - обход защиты TRR на современных картах RAM для выполнения атак Rowhammer.

Самый неубедительный ответ поставщика: Дэниел Дж. Бернштейн - за неправильное обращение с ошибкой еще в 2005 году.

Самое недооцененное исследование: Габриэлю Негрейре Барбоса, Родриго Рубира Бранко (BSDaemon), Джо Чихула (Intel) за обнаружение CVE-2019-0151 и CVE-2019-0152 в режимах Intel System Management Mode (SMM) и Trusted Execution Technology (ТЕКСТ).

Самый грандиозный провал: Microsoft для CurveBall, ошибка в том, как компания реализовала сигнатуры эллиптических кривых в Windows, позволяя легко подделывать HTTPS-сайты и законные приложения.

Эпическое достижение: Гуан Гун, известный китайский охотник за ошибками, за обнаружение CVE-2019-5870, CVE-2019-5877, CVE-2019-10567, трех ошибок, которые позволили удаленно захватить устройства Android Pixel». ***(Catalin Cimpanu. Pwnie Awards 2020 winners include Zerologon, CurveBall, Checkm8, BraveStarr attacks // ZDNet (https://www.zdnet.com/article/pwnie-awards-2020-winners-include-zerologon-curveball-checkm8-bravestarr-attacks/). 10.12.2020).***

***

«Команды по кибербезопасности должны иметь разноплановый образ мышления, чтобы обеспечить наилучшие средства защиты предприятий, правительств и других лиц от кибератак, и это сотрудничество является ключом к объединению различных точек зрения в борьбе с киберпреступностью.

Именно такой подход к сотрудничеству необходим, чтобы помочь в борьбе с вызовами и снизить киберриски для общества, - говорит Пит Купер, заместитель директора по киберзащите Кабинета министров Великобритании и руководитель государственного сектора Национальной программы кибербезопасности.

Бывший пилот скоростного реактивного самолета RAF, ставший советником по кибероперациям, основал первое в Великобритании междисциплинарное соревнование по кибербезопасности и считает, что лучшее сотрудничество и разнообразие являются ключом к решению международных проблем кибербезопасности.

«У всех нас разные взгляды на то, каковы наши проблемы, и у всех нас есть свои индивидуальные горизонты, и настоящая ценность сотрудничества заключается в том, чтобы видеть мир с этих разных точек зрения», - сказал Купер, выступая во время своей основной сессии на Black Hat Europe 2020.

«Потому что, делая это, вы затем начинаете создавать общие точки зрения, вы начинаете расширять свои общие горизонты, чтобы вы могли видеть дальше и развивать гораздо лучшее совместное понимание всего».

Он объяснил, что смешение различных точек зрения может изменить то, как можно использовать ресурсы и какие действия предпринять, и, возможно, даже найти новые способы работы с известными и ранее неизвестными сценариями.

«Это создает уникальное сотрудничество, так что вы можете идентифицировать те препятствия, возможности и идеи, которые вы не смогли бы реализовать ранее - и это то, что на самом деле означает сотрудничество», - сказал Купер.

«При сотрудничестве этих разнообразных команд лучшие решения - это совместные решения, и для этого требуется такое сотрудничество».

Предотвращение кибератак и утечек данных и реагирование на них - ключевая часть кибербезопасности, но это далеко не единственная часть работы, и культура отрасли и группы информационной безопасности в организациях должны это отражать.

«Инциденты - это лишь верхушка айсберга, и мы должны иметь отличную и заинтересованную культуру, чтобы заглядывать под поверхность и понимать, в чем

заключаются проблемы, понимать, что это за события, и понимать, какие идеи могут быть, чтобы их увидеть, "Объяснил Купер.

И хотя объединение этих разных точек зрения требует времени и усилий, как он отметил во время сессии, сотрудничество и разнообразие ценны для всего, что пытается достичь кибербезопасность.

«Потому что, если мы это сделаем, мы начнем делиться этими общими взглядами и расширим наши горизонты», - сказал Купер.

«Чем больше мы узнаем об этих общих горизонтах, работая вместе, тем лучше для всех, поскольку мы пытаемся справиться с ключевыми рисками в будущем», - добавил он». ***(Danny Palmer. What's the key to tackling cyberattacks? Building a diverse team to think smarter // ZDNet (https://www.zdnet.com/article/whats-the-key-to-tackling-cyber-attacks-building-a-diverse-team-to-think-smarter/). 09.12.2020).***

***

«Компания NSS Labs может и прекратила свою деятельность 15 октября нынешнего года, однако ее ранее не публиковавшиеся данные тестирования теперь будут использованы в новой организации, созданной бывшим генеральным директором Викрамом Фатаком (Vikram Phatak). Об этом сообщил ресурс Dark Reading.

Фатак, проработавший 11 лет в NSS Labs, открыл организацию CyberRatings.org в Остине, штат Техас, которая будет составлять рейтинги, отчеты и анализировать продукты и услуги безопасности. Первым выпуском новой организации будут рейтинги продуктов, основанные на новых и неопубликованных данных тестирования NSS Labs для предложений поставщиков программно-конфигурируемых глобальных сетей (SD-WAN), а за ними последуют рейтинги межсетевых экранов нового поколения и систем предотвращения взломов. По словам Фатака, организация CyberRatings.org стремится предоставить более открытый и всеобъемлющий источник оценок продуктов безопасности, который также охватывает потребительский сектор.

CyberRatings.org будет включать в свои рейтинги стратегическую информацию об ИБ-фирмах, например, об их финансовом состоянии, найме и увольнении руководителей высшего звена.

При создании CyberRatings.org Фатак отказался от «островной» модели NSS Labs, которая, по его словам, часто создавала атмосферу противостояния NSS Labs и поставщиков средств безопасности.

Несколько бывших сотрудников NSS Labs присоединились к Фатаку в новой организации, в том числе бывший вице-президент по маркетингу и корпоративным отношениям Кэти Мэйн (Cathy Main), а также некоторые аналитики по тестированию, которые работали в ныне закрытой компании.

Бесплатное членство CyberRatings.org в сообществе включает тестирование продуктов и услуг безопасности, а также сводные рейтинги. Фирма также предлагает членство на более высоком уровне с более широким доступом к данным тестирования и анализу. Например, стоимость персонального членства составляет $100 в год и включает подробные отчеты о рейтингах продуктов.

Вскоре организация планирует предлагать профессиональное членство за $500 в год, членство для малого бизнеса за $1 тыс. в год и членство для корпоративных клиентов и поставщиков услуг за $10 тыс. в год». ***(Бывший гендиректор NSS Labs создал организацию по тестированию безопасности // SecurityLab.ru (https://www.securitylab.ru/news/514528.php). 03.12.2020).***

***

«Джон Гримм, вице-президент по стратегии и развитию бизнеса Entrust, делится своими советами о том, как организации здравоохранения могут минимизировать шансы нарушения безопасности в то время, когда ресурсы ограничены как никогда.

Пандемия COVID-19 и последующая изоляция стали катализатором беспрецедентного глобального перехода к методам удаленного ухода и телездравоохранения, ускорив внедрение устройств с поддержкой Интернета вещей (IoT) для лечения и оценки. Быстрые темпы принятия, чтобы просто поддерживать определенный уровень ухода и лечения, возможно, привели к неизвестным цифровым угрозам, которые могли угрожать наиболее уязвимым людям Великобритании.

Поскольку правительства не рекомендуют личные консультации, а медицинские центры принимают только самые неотложные случаи, технологии постепенно сокращают этот пробел. Исследование, проведенное McKinsey, выявило 65% -ный рост числа поставщиков медицинских услуг, заинтересованных в предложении вариантов телездравоохранения в будущем в форме виртуальных консультаций и / или подключенных устройств - и вполне вероятно, что эти технологии станут постоянным элементом здравоохранения.

Использование подключенных устройств IoT растет: 24% пациентов в исследовании Ipsos Mori сообщили, что они в настоящее время используют устройство IoT или использовали его в прошлом. В настоящее время поставщики медицинских услуг вкладывают значительные средства в подключенные устройства, от имплантированных инсулиновых помп до носимых устройств для удаленного мониторинга сердечного ритма. контролировать пульс удаленно. По прогнозам компании Deloitte, к 2022 году отрасль подключенного медицинского оборудования будет стоить более 158 миллиардов долларов по сравнению с 41 миллиардом долларов в 2017 году.

На первый взгляд кажется, что это история успеха технологий, решающих как краткосрочные, так и давние трудности при оказании медицинской помощи растущему населению. Однако есть явные пробелы в безопасности устройств IoT. Личная информация может быть использована злоумышленниками или украдена злоумышленниками через скомпрометированные уязвимые устройства, использована для шпионажа или как часть ботнета. Однако распространение этой технологии в здравоохранении привело к тому, что физическая безопасность пользователей подверглась такой же тщательной проверке.

Исследование Entrust 2020 PKI и IoT Trends, проведенное среди почти 2000 опрошенных профессионалов в области ИТ-безопасности со всего мира, показало, что более двух третей (68%) специалистов по ИТ-безопасности считают

«изменение функции устройства» самой большой угрозой для устройств IoT. Более половины (52%) дополнили это опасением, что устройства могут быть взломаны и удаленно управляться злоумышленниками. С точки зрения медицины, это может означать угон инсулиновых помп по всему миру или нарушение работы учреждений по уходу с целью нанесения ущерба национальной инфраструктуре. Последствия этих кибератак могут нанести ущерб национальным медицинским учреждениям и подвергнуть тысячи, если не миллионы, людей риску серьезных телесных повреждений.

Большинство респондентов в опросе Entrust оценили меры противодействия этим угрозам безопасности как наименее важные для безопасности Интернета вещей. Подобное несоответствие приоритетов усугубляет общие проблемы безопасности, связанные с невероятными темпами развертывания устройств Интернета вещей, поскольку могут возникнуть пробелы в безопасности, вызванные несоответствием между угрозой и мерами противодействия.

Сектор здравоохранения часто оказывается в центре согласованных кибератак, таких как атаки программ-вымогателей WannaCry на NHS в 2017 году, поскольку провайдеры часто работают со старым оборудованием и испытывают невероятные операционные нагрузки. Атака 2017 года парализовала NHS и в мгновение ока поставила национальную систему на колени; что побудило правительство выделить 50 млн фунтов стерлингов на экстренные меры для восстановления наиболее уязвимых отделов Государственной службы здравоохранения и еще 150 млн фунтов стерлингов, обещанных до 2020 года. Такая атака становится более вероятной из-за уже действующих мер безопасности, которые, по мнению недавних расследований, находятся под угрозой из-за множество уязвимостей, которые, если их не устранить, могут привести к повторению сбоев на уровне 2017 года.

Недавнее исследование возможностей обеспечения безопасности в более широкой отрасли здравоохранения выявило ряд уязвимостей, с которыми в настоящее время сталкиваются поставщики медицинских услуг. От терминалов и оборудования под управлением неподдерживаемых версий Windows до отсутствия мобильной безопасности - треть (33%) организаций сообщила, что в 2018 году у них произошел инцидент с безопасностью, связанный с использованием мобильных устройств. Однако большую озабоченность вызывают 0,4% полностью незащищенных устройств из-за неподдерживаемой ОС или производства до того, как поставщики полностью осознали проблемы кибербезопасности. Хотя численно небольшой процент, эти устройства часто являются наиболее важными в сети поставщиков медицинских услуг, и, по прогнозам, это число не изменится без значительных финансовых вложений, что указывает на сохраняющуюся уязвимость системы безопасности в будущем. Любое устройство, программное обеспечение которого не может быть обновлено, представляет собой значительный риск, поскольку уязвимости постоянно обнаруживаются, а возможность установки исправлений безопасности жизненно важна для обеспечения безопасности жизненного цикла устройства и безопасности пациентов.

Когда здоровье и благополучие населения находятся под угрозой, поставщики медицинских услуг должны действовать быстро и решительно для

борьбы с угрозами кибербезопасности. Однако может показаться, что сообщество ИТ-безопасности одновременно остается обеспокоенным и вносит свой вклад в ситуацию с таким явным несоответствием между предполагаемыми цифровыми угрозами и тем, что можно сделать, чтобы их остановить. По мере того как мир приближается к постпандемическому периоду, медицина и технологии становятся общепринятой частью лечебной процедуры; промышленность и сообщество безопасности должны работать вместе, чтобы обеспечить безопасность наиболее уязвимых». ***(Rise in remote care puts medical equipment at risk of cyber attacks // Open Access Government (https://www.openaccessgovernment.org/medical-equipment-cyber-attacks/100445/). 17.12.2020).***

***

«Компания Alstom завершила сделку по приобретению за 7 млн долларов миноритарного пакета акций израильской компании Cylus, специализирующейся на обеспечении кибербезопасности на железнодорожном транспорте…

Сообщается, что Alstom получит одно место в совете директоров компании. Кроме того, сделка включает соглашение о стратегическом партнерстве, позволяющем участникам объединить усилия и компетенции для создания наилучших решений по кибербезопасности на железнодорожном рынке.

Созданная в 2017 году Cylus разработала набор сервисов для защиты объектов железнодорожного транспорта от киберугроз под общим названием CylusOne.

Партнеры совместно интегрируют технологию кибербезопасности в процессы, компоненты и решения для отрасли. Сначала ее внедрят на сети линий трамвая Тель-Авива, суточный пассажиропоток на которой составляет 200 тысяч человек.

Отмечается, что разработанные для сложных и разнообразных условий железных дорог и метрополитенов сервисы CylusOne совместимы с системой управления движением поездов по радиоканалу CBTC и европейской системой управления движением поездов ETCS.

Технология использует машинное обучение для ускорения обнаружения вредоносного программного обеспечения и несанкционированного проникновения.

В системе реализованы функции искусственного интеллекта для определения поведения после обнаружения угрозы и эффективного противодействия. CylusOne выявляет киберугрозы для сетей сигнализации и управления движением поездов, связи, бортовых и напольных систем». ***(Alstom и израильская Cylus займутся обеспечением кибербезопасности на ж/д транспорте // ЦТС (https://cfts.org.ua/news/2020/12/14/alstom_i_izrailskaya_cylus_zaymutsya_obespecheniem_kiberbezopasnosti_na_zh_d_transporte_62398). 14.12.2020).***

***

«Компания Check Point Software Technologies представила результаты нового исследования, в котором показала основные приоритеты и проблемы кибербезопасности организаций до 2023 г., а также основные изменения в их

стратегиях кибербезопасности, возникшие из-за пандемии Covid-19. Опрос был проведен компанией Dimensional Research для Check Point и охватил 613 ИТ- и ИБ-специалистов по всему миру. Ниже приведены ключевые выводы опроса.

Основные проблемы безопасности в 2021 г.:

Обеспечение безопасности сотрудников, работающих удаленно – это отметили 47% респондентов;

Защита от фишинга и атак с использованием социальной инженерии – 42%;

Предоставление безопасного удаленного доступа – 41%;

Защита облачных приложений и инфраструктуры – 39%.

Ключевые задачи безопасности на следующие два года:

Обеспечение удаленной работы – 61% респондентов;

Безопасность конечных точек и мобильных устройств – 59%;

Защита публичных и гибридных облаков – 52%.

Новая реальность: 50% всех респондентов считают, что их подход к безопасности не вернется к прежним нормам; 29% заявили, что в какой-то момент в будущем ожидают возвращения к тем нормам, которые были до Covid-19.

С начала пандемии организации сталкиваются с растущим количеством атак: 58% респондентов заявили, что их организации испытали рост атак и угроз с начала вспышки Covid-19; 39% полагают, что объем атак остался прежним.

Перемены в стратегиях безопасности в 2020 г.:

95% респондентов заявили, что их стратегии изменились во второй половине года. При этом самым крупным изменением стала возможность массовой удаленной работы – об этом рассказали 67% опрошенных;

39% отметили, что теперь для сотрудников проводится обучение базовым правилам кибербезопасности;

37% рассказали, что улучшили сетевую безопасность и предотвращение угроз;

37% заявили, что расширили безопасность конечных точек и мобильных устройств;

31% отметили быстрое внедрение облачных технологий;

27% заявили, что они ускорили текущие ИТ-проекты в течение года – для большинства меры, предпринятые из-за пандемии, включали незапланированное переосмысление их бизнес-модели». ***(С начала пандемии 58% компаний столкнулись с ростом числа кибератак // Компьютерное Обозрение (https://ko.com.ua/s_nachala_pandemii_58_kompanij_stolknulis_s_rostom_chisla_kiberatak_135682). 17.12.2020).***

***

«Исследователи прогнозируют, что в новом году безопасность программного обеспечения будет продолжать бороться за то, чтобы идти в ногу с облаком и IoT.

Специалисты по ИТ-безопасности в основном потратили год, управляя сменой персонала из офиса в дом в 2020 году, который происходит раз в поколение. Эксперты прогнозируют, что с первоначальным продвижением вперед 2021 год будет сосредоточен на укреплении облака и переосмыслении рабочих

процессов организации. под этим новым нормальным. В этой среде решающее значение будет иметь безопасность программного обеспечения.

Об этом говорят исследователи из Checkmarx, которые только что опубликовали свой отчет о безопасности программного обеспечения на 2021 год. Он предвидит новую эру для команд разработчиков программного обеспечения, в том числе сосредоточение внимания на улучшенных инструментах безопасности приложений, масштабировании локальных инструментов безопасности до облака и лучшей защите устройств Интернета вещей (IoT).

Адаптация к облаку

Checkmarx советует командам разработчиков программного обеспечения, которым они должны будут идти в ногу с развитием приложений в облаке.

«Вы не можете отправить код, а затем выполнить откат, чтобы исправить уязвимости, так как это дает возможность злоумышленникам проникнуть в ваши системы», - сказал в своем отчете технический директор Checkmarx Мэти Симан. «В 2021 году инструменты, используемые для обеспечения безопасности приложений, которые интегрируются в цепочку инструментов, должны работать намного быстрее, масштабироваться до облачных сред и предоставлять практические результаты в формате, который разработчики могут понять и использовать для быстрых исправлений».

Это сообщение приходит по мере того, как облачные приложения и среды все чаще попадают в поле зрения злоумышленников. Например, на этой неделе Агентство национальной безопасности выпустило предупреждение о том, что злоумышленники разработали методы использования уязвимостей в доступе к локальной сети для компрометации облака.

«Злоумышленники злоупотребляют доверием к средам федеративной аутентификации для доступа к защищенным данным», - говорится в сообщении. «Эксплуатация происходит после того, как субъекты получили первоначальный доступ к локальной сети жертвы. Акторы используют привилегированный доступ в локальной среде, чтобы нарушить механизмы, которые организация использует для предоставления доступа к облачным и локальным ресурсам и / или для компрометации учетных данных администратора с возможностью управления облачными ресурсами».

Уязвимости с открытым исходным кодом

Между тем, открытый исходный код будет продолжать привлекать атаки.

«Редко бывает неделя без обнаружения вредоносных пакетов с открытым исходным кодом», - пишет Симан. «Да, организации понимают, что им необходимо защитить компоненты с открытым исходным кодом, которые они используют, и существующие решения помогают им удалять пакеты, которые по ошибке являются уязвимыми (когда разработчик случайно помещает уязвимость в пакет). Но они по-прежнему слепы к случаям, когда злоумышленники злонамеренно вставляют зараженный код в пакеты. Это необходимо изменить в 2021 году».

Он посоветовал держаться подальше от новых разработок и придерживаться более «зрелых», хорошо известных компонентов с открытым исходным кодом.

Инфраструктура как код

Разработчики лихорадочно создают приложения с использованием новых сред «инфраструктура как код», что, по словам Симана, оставило серьезные пробелы в безопасности. В будущем это потребует дополнительного обучения безопасности IaC.

«Я ожидаю увидеть, как злоумышленники воспользуются ошибками разработчиков в этих гибких средах. Для борьбы с этим мы увидим, что основное внимание будет уделяться обучению облачной безопасности, передовым методам IaC и дополнительным расходам, направленным на безопасность программного обеспечения и приложений для поддержки потребностей удаленной рабочей силы и более сложных программных экосистем», - добавил он.

Безопасность будет отчитываться перед разработкой

«Разработчики Diva - это факт жизни, и для обеспечения безопасности на протяжении всего процесса разработки программного обеспечения командам безопасности придется ориентироваться в группах разработчиков на расширение сотрудничества», - пояснил Сима.

«Разработчики самоуверенны и становятся все более влиятельными, и вы не можете заставить их делать или использовать то, на что они не покупаются», - написал он. «Чтобы способствовать сотрудничеству между безопасностью и развитием, безопасность в 2021 году необходимо будет интегрировать в цепочку инструментов разработки таким образом, чтобы последний был наиболее удобен».

Целостный взгляд на безопасность

По словам Симана, командам все чаще требуется всестороннее представление о состоянии их безопасности во всей организации, что вызывает потребность в инструментах, обеспечивающих полное представление об экосистеме.

Когда дело доходит до безопасности открытого исходного кода, в частности, более полные представления позволят организациям не только узнать, используют ли они уязвимый пакет, но также, что более важно, будет ли способ, которым потребляет приложение, совершает атаку. или возможна уязвимость.

Облачная безопасность

По словам соавтора отчета и директора Checkmarx по исследованиям в области безопасности Эреза Ялона, в настоящее время облачная безопасность недостаточно используется и не полностью изучена в сообществе безопасности, но в 2021 году мы увидим толчок к уделению приоритетного внимания блокировке облачных сред.

«Если 2020 год был годом API, то 2021 будет годом, когда облачная безопасность станет центром внимания», - написал Ялон в своем отчете. «API-интерфейсы играют важную роль в облачной безопасности, но основное внимание будет уделено тому, как облачные технологии продолжают распространяться и распространяться в организациях. Обеспечение безопасности образовавшихся экосистем взаимосвязанных облачных решений станет приоритетом».

Уязвимые API

Это подводит Ялона к следующему зловещему предсказанию, что эти незащищенные API-интерфейсы станут самым легким местом для взлома систем злоумышленниками.

«По мере того, как злоумышленники продолжают наращивать свои атаки, нацеленные на API, а организации пытаются наверстать упущенное в понимании того, как можно использовать эти программы, злоумышленники в ближайшем будущем воспользуются этим пробелом, вынуждая разработчиков быстро определять способы улучшения безопасные процессы аутентификации и авторизации API», - сказал он.

Уязвимые устаревшие устройства

Ялон добавил, что старые устройства Интернета вещей, о которых часто забывают, когда они спокойно работают в фоновом режиме, в 2021 году останутся привлекательными целями для злоумышленников.

«По мере того, как эти устройства стареют, но продолжают использоваться, многие производители перестали поддерживать их с помощью обновлений программного обеспечения и исправлений, поскольку они отдают предпочтение новым моделям, что делает старые модели основной мишенью для злоумышленников, ищущих удобные точки доступа», - написал Ялон. «Со временем уязвимости в этих устаревших продуктах будут обнаружены и использованы».

В соответствии с этим, промышленное, заводское и медицинское оборудование, по сообщениям Armis, оставалось в основном без исправлений для защиты от групп вредоносных программ URGENT / 11 и CDPwn, несмотря на то, что исправления были доставлены. Исследователи просмотрели и обнаружили, что 97 процентов устройств OT, на которые воздействует СРОЧНЫЙ / 11, например, не были исправлены.

Медленный прогресс в области безопасности Интернета вещей

По словам Ялона, принятие в США в прошлом месяце Закона о совершенствовании кибербезопасности IoT было шагом в правильном направлении, но предстоит еще много работы.

Двухпартийное законодательство требует, чтобы федеральные устройства отвечали минимальным стандартным требованиям безопасности. Но Ялон добавил, что реального прогресса невозможно добиться без сильного давления со стороны потребителей.

«До тех пор, пока потребители не окажут реальное давление на правительства и производителей с целью повышения безопасности устройств IoT, или пока производители не будут уделять большое внимание безопасности IoT, это будет постоянным поводом для беспокойства», - сказал он». ***(Becky Bracken. Cloud is King: 9 Software Security Trends to Watch in 2021 // Threatpost (https://threatpost.com/cloud-king-software-security-trends-2021/162442/). 18.12.2020).***

***

«Инсайдерская угроза» или «человеческая ошибка» часто является основной причиной утечки данных во всех типах отчетов. Но часто это не определено или четко не определено, поэтому люди придумывают собственное определение.

Что инсайдер угроза действительно является

Идея «инсайдерской угрозы» звучит как некий двойной агент, который прячется в кабине - кого-то наняли, чтобы украсть секреты компании и схватить вас. Звучит довольно интересно, но не совсем точно. Когда мы говорим об инсайдерских угрозах, на самом деле мы обычно говорим о людях, которые совершили ошибку, которая привела к утечке информации компании. Но то, что их действия причинили вред, не означает, что они виновны в злонамеренных действиях.

Определение внутренней угрозы

«Инсайдерская угроза» или «человеческая ошибка» часто является основной причиной утечки данных во всех типах отчетов. Но часто это не определено или не определено четко, поэтому люди придумывают собственное определение.

Когда вы слышите истории об инсайдерских угрозах, это основные из них:

Недовольный сотрудник предпочитает утечку данных и причиняет вред компании

Это самое прямое действие, которое может предпринять человек. Они хотят навредить вам и вашей компании, сделав вас жертвой утечки данных.

К сожалению, это происходит не только после ухода сотрудника из компании. Это может произойти во время работы так же легко, как и после выхода на пенсию.

Лучший способ бороться с этим - иметь четко определенные процедуры приема на работу и увольнения, а также использовать систему управления паролями. У сотрудников не должно быть возможности доступа к чему-либо с помощью личной электронной почты, и после того, как они уйдут из компании, вы должны полностью отключить их доступ. Система управления паролями позволяет вам закрыть доступ одновременно к нескольким системам после того, как кто-то покинет компанию: вы также знаете все, к чему у них когда-либо был доступ, чтобы вы могли выполнять необходимую уборку.

Другой очевидный способ избежать этого - создать хорошую корпоративную культуру. Это может показаться не советом по кибербезопасности, но когда сотрудники довольны, они с меньшей вероятностью будут тратить время на выработку способов вас обмануть. Если вы чувствуете, что сотрудник недоволен, обратитесь к нему и обязательно поговорите с ним.

Сотрудник срезает угол

Еще в мае появился отчет о том, что половина сотрудников признают, что срезают углы, в том числе игнорируют протоколы безопасности. Насколько сильно это может навредить вашей компании?

Просто посмотрите новости за примерами.

Посмотрим на KeepNet Labs. Только в этом году они пострадали от массивной утечки данных, в результате которой было скомпрометировано 5 миллиардов записей. Это произошло потому, что специалист по безопасности, кто-то, работавший на поставщика средств безопасности, нанятого KeepNet, отключил брандмауэр всего на 10 минут! Они хотели ускорить передачу базы данных с этими 5 миллиардами записей, и это им дорого обошлось.

Можно даже утверждать, что Центральный банк Бангладеш стал жертвой срезания углов. Отсутствие у них базовых методов кибербезопасности позволило

хакерам сделать 35 переводов со счета в Бангладешском банке в Федеральный резервный банк Нью-Йорка, что привело к потере в общей сложности 81 миллиона долларов.

Существует множество способов, которыми компании могут «срезать углы». Вы должны предоставить инструменты и процедуры для безопасного обмена информацией или передачи данных. И о важности следующей процедуры нужно рассказать вашим сотрудникам. Никто не хочет быть тем, кто обходит простую процедуру, чтобы сэкономить несколько минут, чтобы обойтись компании в миллионы долларов.

Кто-то принимает неверное решение в Интернете

Все мы получали фишинговые письма и натыкались на вредоносные веб-сайты. Возможно, мы даже испытали эти вещи, даже не осознавая этого. Может нам просто повезло:

Мы открыли фишинговое письмо и просто не нажали

Мы перешли на вредоносный сайт и не перешли на страницу с вредоносным ПО.

Нам представили мошенническую сделку и просто не заинтересовались

Мы оказались на дубликате нашего банковского сайта, но у нас не было причин для входа

Все это вполне реальные возможности, которые для нас легко могли бы пойти другим путем. Когда Anthem был взломан в 2015 году, это произошло потому, что кто-то попался на фишинговое письмо. Для сотрудников, у которых нет такой же подготовки в области кибербезопасности, как у всех нас, эти ситуации становятся еще страшнее. Если они недостаточно осторожны, они могут предпринять действия, которые могут привести к личному или профессиональному нарушению.

Давайте представим финансового сотрудника, попавшего на тот поддельный банковский сайт, о котором я упоминал выше. Что, если они ввели данные учетной записи вашей компании? Или это фишинговое письмо: что, если в нем просят перевести деньги от компании клиенту?

Это ситуации, которые случались с реальными людьми. Обучение тому, как выглядит мошенничество, - хороший первый шаг, но не менее важно обеспечить правильную защиту. В конце концов, даже если вы больше всех осведомлены о кибербезопасности на планете, вы все равно можете попасться на действительно хорошую аферу.

Итак, что нужно сделать?

Установите защиту DNS, чтобы каждый щелчок, сделанный вами и вашими сотрудниками в Интернете, был защищен. Сотрудникам может быть заблокирован доступ к фишинговым и вредоносным сайтам. Хорошая защита DNS даст вам возможность развертывания либо в сети, либо на отдельных устройствах, в зависимости от потребностей вашей компании.

Неясные термины в отношении публичной и частной информации

В каждой компании есть вещи, которыми можно поделиться с широкой публикой, и есть вещи, которые не подходят. Некоторые из них очевидны, например, учетные данные для входа и ключи API. Но некоторые вещи менее

очевидны, например, инструменты, которые вы используете, или ссылки на определенные хранилища информации.

Допустим, сотрудник поделился ссылкой на что-то публично, что каким-то образом было доступно людям за пределами компании, но этого не должно было быть. Возможно, кто-то создал публичный репозиторий GitHub в своей личной учетной записи, а не в учетной записи компании. Или, может быть, они поделились ссылкой на какие-то отчеты, не предназначенные для клиентов. Эти типы активов могут содержать информацию, которая может побудить внешнюю сторону обнаружить уязвимость в вашей компании. И все потому, что ваш сотрудник не знал, что можно, а что нет.

Простое решение этой проблемы - иметь политику в отношении того, что приемлемо, а что неприемлемо для передачи внешним сторонам. Убедитесь, что сотрудники никогда не используют свои личные учетные записи, когда размещают уязвимую информацию о компании, и что у вас есть специальные места для них для создания новых проектов или контента. Правила должны быть установлены, и вам также нужно поощрять вопросы. Если они не уверены в правильности следующего шага, они должны спросить, а не предполагать. Это поможет вам не стать жертвой утечки данных». ***(Insider Threats: What Are They, Really? // Threatpost (https://threatpost.com/dnsfilter-insider-threats-what-are-they-really/162261/). 18.12.2020).***

***

«Коммуникационный альянс обратился к правительству с просьбой избегать дублирования при введении новых обязательств перед поставщиками услуг связи в соответствии с реформами безопасности в телекоммуникационном секторе (TSSR).

Согласно TSSR, все перевозчики и назначенные поставщики услуг перевозки (C / NCSP) должны уведомлять Координатора доступа к связи (CAC) о предлагаемых изменениях в своих телекоммуникационных системах или услугах, если им станет известно о любых предлагаемых изменениях, которые могут иметь «существенное неблагоприятное воздействие» на их способность соблюдать обязательства по обеспечению безопасности.

В соответствии с обязательствами TSSR в настоящее время телекоммуникационным компаниям необходимо «делать все возможное» для защиты инфраструктуры.

В своем представлении [PDF] в Объединенный парламентский комитет по разведке и безопасности (PJCIS) и его обзоре TSSR, Comms Alliance просил отменить обязательство по уведомлению TSSR или освободить от этого обязательства для организаций, подпадающих под действие позитивного обязательства безопасности. (PSO) в соответствии с недавно принятым национальным законопроектом о критической инфраструктуре.

По утверждению Comms Alliance, PSO, содержащееся в Законе о безопасности критической инфраструктуры (SoCI Act), должно привести к тому же результату, что и TSSR. В нем говорится, что наложение PSO на организации, уже подпадающие под обязательства TSSR по безопасности и уведомлению, приведет к

дублированию режимов регулирования, которые имеют такой же предполагаемый результат.

«Поэтому мы рекомендуем либо отменить обязательство по уведомлению TSSR, либо освободить от этого обязательства для юридических лиц, подпадающих под действие этого PSO», - говорится в сообщении.

«При пересмотре TSSR необходимо учитывать развивающиеся горизонтальные нормативные акты, такие как Закон о SoCI, и гарантировать, что правила этих нормативных актов избегают дублирования, дублирования или даже несоответствия с существующими отраслевыми нормативными актами.

«Поставщики услуг, которые уже подпадают под требования кибербезопасности в отраслевом законодательстве, должны оставаться исключенными из сферы действия горизонтальных требований или добиваться отмены отраслевых нормативных требований, которые могут привести к дублированию».

Отраслевой орган заявил, что это исключение необходимо для обеспечения правовой ясности, определенности и соразмерности обязательств.

«Мы утверждаем, что, по сути, это делает требования к уведомлению TSSR излишними, поскольку оценка рисков предлагаемых изменений обязательно будет частью более широкого, ежегодно утверждаемого и сообщаемого плана управления рисками», - продолжил он.

«Подчинение юридических лиц требованиям об уведомлении TSSR (и последующее снижение риска, если это будет сочтено необходимым), а также PSO пересмотренного Закона о SoCI приведет к существенному дублированию и неэффективности, что противоположно заявленной правительством цели».

Он также сказал, что выполнение обоих наборов обязательств создаст дублирующие усилия для CAC / Critical Infrastructure Center.

«Мы считаем, что должен быть только один орган, назначенный для CSP в сфере безопасности. В настоящее время законодательная и нормативная среда в области безопасности, кибербезопасности и защиты данных довольно перегружена», - добавлено в заявлении.

Вместо этого Comms Alliance поддержал «высокоуровневый подход к обеспечению безопасности, основанный на принципах». В нем говорится, что такой подход позволяет операторам связи получить необходимую гибкость для реализации мер, соответствующих их бизнесу, и при этом иметь возможность быстро адаптироваться к технологическим изменениям.

«Этот подход также с большей вероятностью позволит избежать дублирования или несоответствия с существующими (или будущими) международными стандартами и передовой практикой и обеспечивает необходимую гибкость для глобально действующих организаций, чтобы соответствовать более ограниченному набору спецификаций безопасности, тем самым способствуя повышению операционной эффективности. и правовая определенность», - говорится в сообщении.

Что касается двустороннего обмена угрозами, Comms Alliance заявила, что информация об угрозах, связанных с коммуникациями, не была передана его членам.

«Следовательно, наши члены понесли существенные затраты на реализацию реформ - и правительственных решений, которые были приняты в результате реформ - без обещанной выгоды в виде дополнительной информации о рисках и угрозах для принятия инвестиционных решений», - говорится в сообщении.

«Это прискорбно и должно быть исправлено в срочном порядке, особенно в свете дополнительного уровня регулирования безопасности, который пересмотренный Закон SoCI (даже в его «самой легкой версии»), вероятно, будет представлять для нашего сектора».

Comms Alliance добавила, что сектор связи уже понес значительные расходы в ходе внедрения TSSR и продолжает нести высокие нормативные расходы за постоянное соблюдение различных законодательных и нормативных требований, связанных с безопасностью.

«На этом фоне и с учетом дополнительных затрат, которые могут возникнуть в результате требований пересмотренного Закона о SoCI, мы призываем комитет рассмотреть варианты возмещения затрат для поставщиков телекоммуникационных услуг, подпадающих под эти расширенные режимы безопасности», - говорится в сообщении. «Мы считаем важным, чтобы реформы критически важной инфраструктуры и TSSR сохранили принцип возмещения затрат, который четко закреплен в Законе о телекоммуникациях». ***(Asha Barbaschow. Comms Alliance argues TSSR duplicates obligations within Critical Infrastructure Bill // ZDNet (https://www.zdnet.com/article/comms-alliance-argues-tssr-duplicates-obligations-within-critical-infrastructure-bill/). 23.12.2020).***

***

«Когда организации используют API-интерфейсы - следующий рубеж в киберпреступности - для взаимодействия с третьими сторонами, очень важно, чтобы они понимали связанные с ними риски безопасности, которые они представляют. Для этого они должны думать как хакеры, чтобы оценить, создают ли они проблему или предлагают решение для своих клиентов и своей организации. Оттуда они могут двигаться вперед, выбирая варианты, которые обеспечивают бесперебойную работу для клиентов и в то же время защищают критически важные данные.

Возьмем, к примеру, розничных торговцев. Многие розничные торговцы теперь используют стороннюю обработку кредитных карт для своих онлайн-транзакций. Таким образом, розничные торговцы сокращают количество держателей карт и риски, связанные со стандартами индустрии платежных карт (PCI). Однако в то же время они передают эти данные потенциально незащищенной третьей стороне.

Это вызывает некоторые ключевые вопросы. Предоставила ли передача третьей стороне решение или возникла новая проблема? Как розничные торговцы могут обеспечить бесперебойное обслуживание клиентов, при этом защищая важные данные, которым они доверяют?

Проблема: злоупотребление API и атаки перечисления

Чтобы понять суть проблемы, проще всего рассмотреть сценарий из реальной жизни. Рассмотрим рабочий процесс обработки кредитной карты для онлайн-заказа

еды. Человек помещает свои товары для покупки в корзину и начинает процесс оформления заказа, вводя информацию об оплате и доставке.

Хакеры (как хорошие, так и плохие) на этом этапе могут отправить транзакцию из своего веб-браузера на прокси-сервер перехвата для проведения анализа рабочего процесса. Недавно я прошел через этот анализ, пытаясь понять, как розничные продавцы могут лучше противодействовать этим угрозам.

Рабочий процесс, который я рассмотрел на этом этапе в прокси-сервере перехвата, показал платежную информацию, которая была отправлена для совершения покупки, как и должно быть. Тем не менее, он также показал, что дополнительные новые конечные точки API выходят в онлайн. Изучая эту транзакцию дальше, я заметил HTTP-POST с данными кредитной карты, который был отправлен третьей стороне через API. Ответ стороннего API включал токен, который этот конкретный продавец продуктов питания должен будет использовать для сопоставления этой транзакции и в конечном итоге получить оплату.

Думая, как потенциальный злоумышленник, я сделал шаг назад, чтобы оценить риск. Если бы у меня была платежная информация, включая номер кредитной карты и дату истечения срока действия, но не было значения подтверждения кредита (CVV), могу ли я использовать метод перечисления, чтобы предварительно получить токены и попробовать их один за другим?

Чтобы найти ответ на этот вопрос, я удалил из запроса все файлы cookie, токены, трекеры и т. Д. И обнаружил, что все еще могу получить обратно токен. Я загрузил запрос службы токенизации API в прокси-сервер перехвата и настроил серию вызовов, соединив все возможные CVV с картой и датой истечения срока действия, что позволило мне создать поддельные токены, которые будут содержать правильные значения. Отсюда я настроил ротацию, которая создает запросы от 100 до 999 в последовательном порядке. Скрипт токенизации работал безупречно.

Если бы я был действительно злоумышленником, последним шагом здесь было бы подавать эти сгенерированные токены в процесс оформления заказа один за другим, пока не будет успешного совпадения.

Решение: понимание API-интерфейсов для блокировки злонамеренного поведения

Используя API розничного продавца и сторонние API, злоумышленники могут совершать этот вид мошенничества на высокой скорости. И если эти действия распределены по нескольким IP-адресам с использованием пуленепробиваемых прокси, розничному продавцу будет сложно заметить, что происходит.

Итак, какое решение? Первый шаг - проверить функциональность и поведение API. Если можно отправить несколько токенов, чтобы найти правильные пропущенные значения, тогда должен быть установлен счетчик транзакций, который учитывает ошибки пользователя и вызывает повторную аутентификацию в рамках рабочего процесса оформления заказа после заданного количества попыток. Точно так же рекомендуется работать с поставщиком, чтобы потоки проверки исходили только из действительных заказов. За этим следует внимательно следить на предмет потенциальных злоупотреблений.

Крайне важно постоянно отслеживать это злонамеренное поведение, автоматически блокировать несколько подозрительных материалов и создавать обманчивую среду, чтобы сбить с толку потенциального злоумышленника. Эти типы атак происходят в течение длительного периода времени и могут включать тысячи ошибочных запросов. Для защиты организаций критически важно, чтобы группы безопасности выявляли потенциальные области риска, учились определять закономерности этого типа деятельности и обращались за помощью к внешним источникам, обладающим опытом в этих областях. Только в этом случае у организаций появится сильная позиция безопасности, которая поможет снизить эти риски». ***(Jason Kent. Third-Party APIs: How to Prevent Enumeration Attacks // Threatpost (https://threatpost.com/third-party-apis-enumeration-attacks/162589/). 23.12.2020).***

***

«У відповідь на підвищення популярності електронних технологій у фермерському господарстві Національний центр кібербезпеки (NCSC) та Союз фермерів NFU видали вказівки, як захиститись від хакерів.

Про це пише farminguk.com. Ферми все частіше користуються перевагами сучасних технологій ведення сільського господарства, таких як GPS, дистанційні датчики та програмне забезпечення для управління фермами. У зв'язку з цим зростає кількість хакерів, бажаючих заволодіти активами агрокомпаній. Так, мануал «Кібербезпека для фермерів» має на меті допомогти сільгоспвиробникам захиститися від найпоширеніших кібератак, включаючи шахрайські електронні листи та небезпечне програмне забезпечення. «Технологія відіграє величезну роль у сучасному сільському господарстві та пропонує безліч переваг, які допоможуть галузі процвітати», — зазначила Сара Лайонс, заступниця директора з питань суспільства NCSC. Стюарт Робертс, заступник президента NFU, сказав, що кіберзлочинність — є величезною проблемою для сільського господарства. «Надзвичайно важливо, щоб фермери сприймали це серйозно, саме тому ми об'єдналися з експертами Національного центру кібербезпеки. Я закликаю всіх фермерів прочитати цей мануал та вжити необхідних заходів для посилення своєї кібербезпеки та захисту свого фермерського бізнесу», — підкреслив пан Стюарт». ***(У Великобританії вийшов перший в світі мануал по кібербезпеці для аграріїв // IAC Аграрії разом (https://agrarii-razom.com.ua/news-agro/u-velikobritanii-viyshov-pershiy-v-sviti-manual-po-kiberbezpeci-dlya-agrariiv). 25.12.2020).***

***

Сполучені Штати Америки

«Согласно Cyberseek, интерактивному картографическому инструменту, который отслеживает текущее состояние рынка труда в сфере безопасности, только в США доступно более полумиллиона открытых вакансий в сфере кибербезопасности (522 000).

Массовый переход на удаленную работу заставил руководителей службы информационной безопасности переосмыслить, что означает «безопасность», и изменить приоритеты в наборах навыков, необходимых в их группах информационной безопасности. Это создает проблемы для компаний, но также создает широко открытые возможности для тех, кто хочет подготовиться к новому кадру открытых должностей в области кибербезопасности.

Кибер-рабочая сила всегда пользуется большим спросом - настолько высоким, что наблюдается постоянная и широко известная нехватка квалифицированных специалистов для заполнения имеющихся вакансий. Но смена работы на дому привела к беспрецедентному нарушению кибербезопасности, что повлекло за собой нехватку рабочей силы.

Новый набор опасений

Практически в мгновение ока компании внезапно перешли от преимущественно локальной рабочей силы к конфигурации большей части для работы на дому. И эксперты говорят, что большая часть этих сотрудников будет оставаться удаленной на неопределенный срок, что обусловлено экономией средств и предпочтениями сотрудников.

Это изменение приносит с собой множество новых проблем с безопасностью. Например, основная проблема заключается в обеспечении безопасности удаленных сотрудников, которые используют домашние сети, личные устройства и личные приложения для подключения к активам компании, а не работают за корпоративным брандмауэром.

С этим сдвигом новые приоритеты кибербезопасности, такие как фишинг, атаки вредоносных программ и целостность / соответствие данных, стали более предметными.

Более 53% участников недавнего опроса IBM Security заявили, что они используют свои личные устройства для работы, в том числе свои ноутбуки и мобильные устройства. 90% ведут бизнес через свои домашние сети. Однако, как показал опрос, эта деятельность часто выполняется без каких-либо новых средств защиты.

Также наблюдается ускоренный рост облака, но из-за отсутствия инвестиций в надлежащие меры безопасности критически важные данные остаются незащищенными, а организации становятся уязвимыми для атак программ-вымогателей. Отчет об устойчивости к программам-вымогателям за 2020 год [PDF], подготовленный компанией Veritas по защите данных, показал, что 36% организаций ускорили использование общедоступного облака в 2020 году. В отчете также говорится, что многие из этих фирм имеют недостаточную безопасность, которая «не работает». измерять», оставляя данные, хранящиеся в облаке, открытыми. Почти две трети респондентов заявили, что, по их мнению, меры безопасности на их предприятии не соответствовали сложности их ИТ-инфраструктуры.

Многие отделы изо всех сил стараются включить приложения для совместной работы для всех - от Zoom до Slack и от Teams до Webex. Но без надлежащей безопасности они могут представлять большой риск, о чем

свидетельствует рост числа атак социальной инженерии и фишинга с участием этих приложений.

«Злоумышленник может создать надстройку Slack, которая рекламирует некоторые замечательные функции, но также считывает данные каналов», - сказал Мэтт Гэйфорд, главный консультант Crypsis Group. «Если конечный пользователь по ошибке установит надстройку, он может открыть злоумышленнику все каналы Slack».

Одним из основных способов решения проблем удаленной безопасности для компаний является использование VPN, но это создает свои проблемы.

«Некоторые приложения можно настроить так, чтобы к ним можно было получить удаленный доступ только через VPN», - сказал Кен Прести, вице-президент по исследованиям и аналитике AVANT Communications. «Однако об этом нужно активно сообщать, иначе ваши группы поддержки будут завалены сообщениями о проблемах от людей, которые не понимают, что они не подключаются к необходимому ресурсу, потому что они не запустили VPN. Хотя VPN могут значительно повысить безопасность, вашей команде также может потребоваться обучение. Это особенно актуально на начальном этапе, когда люди привыкают к нему».

Все это выявляет краткосрочные пробелы в навыках, а также изменения в навыках кибербезопасности, которые потребуются в долгосрочной перспективе.

«Самые востребованные навыки сосредоточены на защите приложений SaaS, федеративной идентичности, навыках, ориентированных на управление данными (классификация, шифрование, защита), анализе угроз и нулевом доверии, которые действительно ориентированы на идентификацию, но могут называться по-другому», - сказал Брэндон. Хоффман, главный специалист по информационной безопасности NetEnrich.

Новые требования заставляют фирмы обращаться к программам получения степени в области кибербезопасности в надежде привлечь новых сотрудников, среди которых растет число женщин, обладающих новейшими востребованными навыками.

«Это не сильно отличается в том смысле, что эти навыки сейчас необходимы, а раньше не были», - сказал Хоффман. «Он отличается в том смысле, что эти навыки будут иметь приоритет над традиционными навыками, такими как реагирование на инциденты, навыки сетевой безопасности и защита конечных точек».

По словам Мохита Тивари, соучредителя и генерального директора Symmetry Systems, решения облачной безопасности будут иметь решающее значение для будущей команды ИТ-безопасности.

«По мере того, как сети и уровни приложений становятся эфемерными, наиболее важным постоянным активом для любого предприятия, вероятно, будут их собственные данные и данные их клиентов, поэтому безопасность данных в облаке станет основной темой в будущем», - сказал он.

Дефицит навыков в цифрах

Согласно Cyberseek, инструменту интерактивного картирования, который отслеживает текущее состояние рынка труда в сфере безопасности, только в США

доступно более полумиллиона открытых вакансий в сфере кибербезопасности (522 000). Фирма также обнаружила, что текущее соотношение имеющихся сотрудников в области кибербезопасности к вакансиям в области кибербезопасности очень низкое, согласно статистике, на каждые восемь открытых вакансий приходится один квалифицированный кандидат. И в среднем, выполнение ролей в сфере кибербезопасности занимает на 21% больше времени, чем выполнение других ИТ-должностей.

Согласно определению Национальной инициативы по обучению кибербезопасности (NICE) Cybersecurity Workforce Framework, наиболее востребованными являются рабочие места в сфере «Безопасное предоставление», где сотрудники «концептуализируют, проектируют, закупают и / или создают безопасные ИТ-системы» (подробнее более 300000 открытых позиций). По данным Cyberseek, с октября 2019 года по сентябрь 2020 года было 166000 вакансий для аналитиков по информационной безопасности, но только 125 570 сотрудников работали на этих должностях - ежегодный дефицит кадров в 40 430 человек для крупнейшей работы в области кибербезопасности.

Еще одна область с более чем 300 000 открытых вакансий (есть совпадения в наборах навыков) - это категория NICE «Эксплуатация и обслуживание», где сотрудники «обеспечивают поддержку, администрирование и обслуживание, необходимые для обеспечения эффективной и действенной производительности и безопасности ИТ-системы».

Эти должности включают специализированные области управления рисками, архитекторов безопасности, системных администраторов, аналитиков данных, разработчиков программного обеспечения, специалистов по сетевым операциям и многое другое.

«Определенные навыки, такие как облачная безопасность и опыт в области киберполитики, пользуются большим спросом из-за повышенного внимания, основанного на сегодняшнем ландшафте, и возобновившегося интереса к операционным технологиям и кибербезопасности ИТ на федеральном уровне», - сказал Курт Джон, главный специалист по кибербезопасности Сименс США.

Хитрость заключается в том, чтобы определить сегодняшние потребности кибербезопасности и спрогнозировать, какие будущие потребности в кибербезопасности не за горами.

Принимая вызов

«Прежде всего, самое большое положительное влияние на кибербезопасность для любой организации - это зрелость и сплоченность их групп безопасности», - советует Марк Симос, ведущий архитектор кибербезопасности в Microsoft, в недавнем сообщении. Это фильтрует то, как команды распознают угрозы и реагируют на них, насколько хорошо внутренние разработчики принимают безопасное кодирование / разработку и как руководители уделяют приоритетное внимание защите критически важной интеллектуальной собственности.

«К сожалению, я считаю, что недавние события усугубили нехватку навыков; однако в то же время они принесли понимание и осознание необходимости в большем количестве киберпрофессионалов», - сказал Джон из Siemens.

Есть возможность для тех, кто желает инвестировать в свои навыки с помощью продвинутой степени кибербезопасности или сертификации в областях с высоким спросом.

«Я считаю, что у компаний и государственного сектора есть возможность решить эту проблему, установив партнерские отношения с колледжами и университетами для увеличения числа студентов, заинтересованных в индустрии кибербезопасности - есть надежда на будущее», - сказал он.» ***(The Remote-Work Transition Shifts Demand for Cyber Skills // Threatpost (https://threatpost.com/wiley-the-remote-work-transition-shifts-demand-for-cyber-skills/162019/). 08.12.2020).***

***

Країни ЄС

«В Бухаресте будет размещен Европейский центр компетенции в области кибербезопасности, будущий центр для распределения средств ЕС и национального финансирования исследовательских проектов в области кибербезопасности по всему блоку после того, как большинство стран ЕС проголосовало за него в среду.

Город был выбран из списка семи городов, претендующих на право размещения центра, включая Брюссель, Мюнхен, Варшаву, Вильнюс, Люксембург и Леон в Испании.

Дипломаты выбрали Бухарест 15 голосами за, как заявили несколько дипломатов ЕС, во втором туре голосования, в котором Брюссель противопоставил столицу Румынии…

Основная задача центра будет заключаться в управлении фондами кибербезопасности из исследовательских бюджетов ЕС, в том числе около 2 миллиардов евро, выделенных в его программе Digital Europe, и многих миллионов других за счет финансирования инноваций и фондов восстановления коронавируса в дополнение к национальным взносам. Блок все еще дорабатывает свой долгосрочный бюджет на 2021-2027 годы.

Центр не будет официальным агентством ЕС, но, как ожидается, принесет в Бухарест десятки рабочих мест - около 30 на начальном этапе и до 80, по некоторым оценкам. Это также должно способствовать развитию бизнеса местных компаний, занимающихся кибербезопасностью, и улучшить репутацию принимающей страны в кибербезопасности.

В Румынии пока нет агентства ЕС, что сыграло в ее пользу. Он также занимает третье место в статистике ЕС по женщинам, работающим в сфере информационных и коммуникационных технологий (ИКТ), и 24 процента выпускников ИКТ в Румынии - женщины, говорится в заявочной книге страны. Национальные столицы также с осторожностью относились к размещению центра в Брюсселе - недалеко от основных институтов ЕС - из-за опасений, что это подорвет национальную компетенцию в вопросах безопасности.

Европейская комиссия, парламент и Совет все еще дорабатывают детали того, как центр будет управляться. Ожидается, что соглашение о новом законе об

учреждении центра будет подписано до конца года, и переговорщики встретятся в эту пятницу, чтобы попытаться заключить сделку». ***(LAURENS CERULUS, LEONIE CATER, VINCENT MANANCOURT. Bucharest to host new EU cyber research hub // POLITICO (https://www.politico.eu/article/bucharest-to-host-eus-new-cyber-research-hub/). 10.12.2020).***

***

«Єврокомісія (ЄК) опублікувала нову стратегію Євросоюзу з кібернетичної безпеки, яка покликана закласти нові принципи розвитку цього сектора на найближче десятиліття.

Документ представили на прес-конференції в Брюсселі заступник голови Єврокомісії щодо захисту європейського способу життя Маргарітіс Схінас, верховний представник ЄС із закордонних справ і політики безпеки Жозеп Боррель, а також єврокомісар з питань внутрішнього ринку Тьєррі Бретон, – інформує 1NEWS.

“Євросоюз є пріоритетною метою для кібернетичних атак у всьому світі, оскільки безліч державних та недержавних структур хочуть, щоб європейський проект провалився, або хочуть використовувати наші слабкості, щоб отримати конкурентні переваги”, — заявив заступник голови ЄК щодо захисту європейського способу життя Маргарітіс Схінас.

“Наявні в наших руках юридичні інструменти щодо забезпечення кіберезопасності застаріли на 10-15 років, вони все створювалися в іншу епоху розвитку цифрових технологій, — продовжив він. — Тому нам необхідно створити новий інструментарій, і саме на це спрямована Стратегія кібернетичної безпеки ЄС”.

Він підкреслив, що Стратегія не замикається на захист інформаційних мереж Євросоюзу та держав ЄС, а включає в себе питання кібернетичного захисту фізичної інфраструктури, яка може зазнавати кібернетичних нападів, включаючи транспорт, енергетику, охорону здоров’я, фінансову систему і багато інших секторів.

“Ми повинні відмовитися від різних підходів до фізичної і кібернетичної безпеки інфраструктури і використовувати запропонований в даній стратегії комплексний підхід”, — зазначив Схінас.

Єврокомісія запропонувала, зокрема, створити оперативний відділ ЄС з кібербезпеки для координації дій всіх країн співтовариства в цій сфері, розгорнути в Євросоюзі мережу оперативних центрів з широким використанням штучного інтелекту для раннього виявлення кібернападів і протидії їм, а також розробити нові інтегровані принципи захисту всієї інфраструктури країн Євросоюзу.

На виконання цих завдань Єврокомісія пропонує залучити до 4,5 млрд євро інвестицій в найближчі 7 років.

Крім того, ЄС буде розширювати міжнародне співробітництво з формування відповідних інтересам і цінностям ЄС норм і стандартів безпеки в світовому цифровому просторі, захисту в ньому прав людини і фундаментальних цінностей євроспільноти, а також буде широко застосовувати санкції та інші методи

покарання щодо іноземних фізичних осіб та організацій, викритих в хакерських атаках.

“Єврокомісія пропонує запустити мережу оперативних центрів безпеки по всьому Євросоюзу з широким використанням систем штучного інтелекту, які будуть представляти собою реальний кіберщит для Євросоюзу, здатний в реальному часі виявляти ознаки кібернетичної атаки досить рано, щоб запустити активні дії у відповідь, перш ніж атака завдасть шкоди”, — йдеться в документі.

“Нам вкрай важливі координація дій і обмін інформацією. Так, в кібербезпеці, як і в медицині, існують архіви і бібліотеки вірусів, тому дуже важливо, як тільки виявляється новий вірус, передавати його всьому міжнародному співтовариству спеціалістів для вивчення і відпрацювання методів протидії”, — заявив в зв’язку з цим єврокомісар Тьєррі Бретон.

У тексті Стратегії також зазначається, що створення нових технічних і інформаційних систем кібербезпеки, так само як і проекти з підготовки кадрів для цієї сфери, будуть розглядатися як проект військового значення, вони можуть розвиватися в рамках європейської програми Постійного структурованого співробітництва в сфері оборони і безпеки (PESCO).

У тому ж документі Єврокомісія із задоволенням відзначила, що в цілому європейські компанії зараз при підготовці до розгортання систем високошвидкісного інтернету нового покоління 5G виконують діючі приписи Єврокомісії, в тому числі в сфері скорочення залежності від іноземних (в першу чергу маються на увазі китайські) поставок обладнання і технологій.

Однак, як зазначив Маргарітіс Схінас, крім фінансового стимулювання та інвестицій в зміцнення кібербезпеки, Єврокомісія має намір розробити систему покарань і великих штрафів для європейських операторів і компаній, які будуть нехтувати виконанням європейських вимог з кібербезпеки. Він підкреслив, що дотримання цих вимог придбає особливе значення при створенні систем наступного покоління — 6G.

Передбачається, що розвиток систем 6G дозволить повністю перейти до використання практично будь-яких електричних та електронних пристроїв — від кавомолок до океанських лайнерів, які будуть працювати з постійним використанням онлайн-з’єднання. У цих умовах кібернетичні напади знайдуть безпрецедентний потенціал нанесення фізичної шкоди шляхом нецільового використання підключених до мережі пристроїв.

“Ми не наївні. Ми бачимо всі ці виклики, і ми працюємо над відповіддю на них. Саме для цього нам необхідна дана стратегія”, — заявив в зв’язку з цим єврокомісар з питань внутрішнього ринку Тьєррі Бретон.

У документі також підкреслюється, що Євросоюз буде працювати з ООН та іноземними партнерами, використовувати санкції для “захисту прав людини і фундаментальних свобод в інформаційному просторі”.

“Євросоюз посилить свою роботу з міжнародними партнерами і ООН щодо зміцнення заснованого на правилах глобального світопорядку, просувати міжнародну безпеку і стабільність в кіберпросторі, захищати права людини і фундаментальні свободи онлайн, розвивати міжнародні норми і стандарти, які повинні відображати базові цінності Євросоюзу, — йдеться в документі. — Для

цього ЄС буде використовувати весь інструментарій дипломатичних заходів, включаючи рестриктивні".

У документі наголошується, що інформаційний простір є глобальним, і кібернетичні загрози також є всесвітнім викликом безпеки, а тому забезпечення кібернетичної безпеки повинно бути міжнародним завданням.

Верховний представник ЄС із закордонних справ і політики безпеки Жозеп Боррель на брифінгу в Брюсселі заявив, що Єврокомісія розробила "20 нових пропозицій по п'яти напрямках в області забезпечення кібернетичної безпеки у зовнішньополітичному вимірі». ***(Євросоюз презентував стратегію кібербезпеки на 10 років // Інформаційне агентство «1NEWS» (https://1news.com.ua/svit/yevrosoyuz-prezentuvav-strategiyu-kiberbezpeky-na-10-rokiv.html). 17.12.2020).***

***

«В среду правительство Германии приняло проект нового закона об ИТ-безопасности, который позволит тщательно проверить надежность поставщиков компонентов для систем критической инфраструктуры, таких как планируемая сверхбыстрая мобильная сеть 5G.

Этот вопрос стал предметом оживленных общественных обсуждений в связи с возможным участием китайской компании Huawei в построении немецкой сети 5G. Есть мнения, что Huawei использует поставляемое оборудование для слежки за пользователями в интересах властей Китая. Представитель правительства Германии Штеффен Зайберт объяснил в среду, что «этот закон определенно касается вопросов безопасности ИТ, а не отдельных производителей».

Согласно формулировке закона, производители должны в будущем подавать декларации, в которых они должны будут заявить, среди прочего, могут ли они и каким образом гарантировать, что критические компоненты не обладают какими-либо техническими характеристиками, которые позволили бы использовать их в целях злоупотребления "в частности, в целях саботажа, шпионажа или терроризма. за счет воздействия на безопасность, целостность, доступность или работоспособность критически важной инфраструктуры Федеральное министерство внутренних дел определит минимальные требования безопасности, которым должен соответствовать производитель. Если окажется, что пользователь не полностью заслуживает доверия, например, не сообщая пользователю об известных недостатках системы, ему будет предложено сотрудничать. В случае постоянного отсутствия доказательств надежности Министерству внутренних дел будет разрешено по согласованию с другими заинтересованными министерствами запретить дальнейшее использование всех компонентов этого производителя.

В законопроект также включен приказ, согласно которому менеджеры критической инфраструктуры сообщают о кибератаках на нее. Кроме того, он вводит единую форму сертификатов безопасности для оборудования, выдаваемых Федеральным управлением по безопасности информационных технологий (BSI)». ***(В Германии прошел проект по усилению ИТ-безопасности // news-lab.org (https://news-lab.org/tehno/2230-v-germanii-proshel-proekt-po-usileniyu-it-bezopasnosti.html). 19.12.2020).***

***

Китай

«Китай присоединяется к Google в заявлении о квантовом превосходстве с новыми технологиями, что усиливает опасения по поводу расшифровки RSA.

Ведущие китайские исследователи квантовых компьютеров сообщили, что они достигли квантового превосходства, то есть способности выполнять задачи, которые традиционный суперкомпьютер не может. И хотя это захватывающее событие, неизбежный рост квантовых вычислений означает, что службы безопасности на один шаг ближе к столкновению с угрозой, более серьезной, чем что-либо прежде.

Исследователи из Университета науки и технологий Китая объяснили в журнале Science, что они смогли получить систему, которую они назвали Jiuzhang, для выполнения вычислений за считанные минуты, на решение которых традиционному суперкомпьютеру потребовалось бы примерно 10 000 лет.

Команда присоединяется к Google, заявившей, что в октябре 2019 года она достигла квантового превосходства, используя «сверххолодный сверхпроводящий металл», согласно WIRED. IBM также вступила в битву с квантовыми вычислениями, одновременно критикуя заявления Google о превосходстве.

Теперь китайские исследователи заявили о квантовом превосходстве, используя квантовые вычисления, называемые выборкой гауссовских бозонов (GBS), как поясняется в их статье, которые используют частицы света, посылаемые через оптическую цепь, для измерения выходного сигнала. Это означает, что в настоящее время существует несколько проверенных технологий квантовых вычислений, и, безусловно, они появятся в будущем.

Проблема безопасности заключается в том, что квантовые компьютеры смогут взламывать шифрование с открытым ключом RSA, используемое для защиты данных при передаче. Это означает, что отделам безопасности придется перейти на новые решения для постквантовой криптографии. По консервативным оценкам из отчета DigiCert за 2019 год, к 2022 году командам потребуется обеспечить защиту от нарушений в области квантовых вычислений.

Чтобы быть ясным, квантовых вычислений пока нет. И китайцы не ближе к способностям расшифровать RSA, чем Google или IBM, но, по мнению экспертов, это только вопрос времени.

«Новый прорыв в области квантовых вычислений в Китае важен по ряду причин», - сказал Threatpost Тим Холлебек, технический стратег DigiCert по отраслям и стандартам. «Во-первых, Китай вложил значительные средства в финансирование исследований в области квантовых вычислений, и этот новый результат показывает, что эти инвестиции окупаются. Во-вторых, это означает, что два разных подхода к созданию квантового компьютера теперь успешно достигли квантового превосходства. Это потенциально могло бы ускорить появление коммерчески полезных квантовых компьютеров, поскольку один подход может

быть успешным, если и когда другой натолкнется на некоторые технические препятствия».

Квантовые вычисления и RSA

Джон Приско из Safe Quantum Inc. сказал, что способность квантовых вычислений превзойти RSA является целью, а не утверждениями о квантовом превосходстве.

«Подход Китая к GSB интересен, но его сложно реализовать», - сказал Приско Threatpost. «Квантовое превосходство не является призом на финише. Если бы это было так, Google и IBM финишировали на световые годы раньше заявленного Китаем. Финишная черта - квантовый простой компьютер, способный взломать известное нам шифрование».

Он добавил, что когда дело доходит до широкого внедрения, у китайского подхода есть проблемы.

«Масштабирование подхода GSB к квантовым первичным уровням маловероятно из-за огромных размеров интеграции классических зеркал и светоделителей», - пояснил он. «Ионная ловушка или сверхпроводящие квантовые компьютеры, отстаиваемые IonQ и IBM соответственно, вероятно, завершат гонку за первыми квантовыми компьютерами, намного опередив подход Китая в этом объявлении».

Тем не менее, Холлебек предупредил, что у групп безопасности остается мало времени, чтобы подготовиться к борьбе со злоумышленниками, сверхмощными благодаря квантовым вычислениям.

«Хотя такие квантовые компьютеры сегодня не представляют угрозы для шифрования, они напоминают нам, что наступает день, когда этого больше не будет», - сказал он. «Важно, чтобы профессионалы в области безопасности начали планировать переход к постквантовой криптографии, поскольку на планирование и реализацию таких переходов уходит много лет. Китайский результат, вероятно, существенно не изменит прогнозов относительно того, как скоро это произойдет, но ведущие организации по-прежнему ожидают, что это произойдет в ближайшие 10 лет или около того. Итак, важно начать подготовку прямо сейчас».

Разумной отправной точкой может быть набор стандартов. Но это происходило медленно.

Стандарты квантовых вычислений

Национальный институт стандартов и технологий (NIST) еще не определил свои рекомендации и в настоящее время участвует в третьем раунде конкурса, чтобы определить окончательный стандарт постквантовой криптологии, который будет развиваться. Согласно предварительному графику NIST, окончательный проект стандартов не ожидается раньше 2022 года .

Но пока стандарты все еще разрабатываются, есть вещи, которые бизнес и ИТ-команды могут сделать, чтобы подготовиться, в том числе получить представление о надвигающемся ландшафте.

«Факторизация больших простых чисел (взлом ключей RSA) с помощью квантовых компьютеров - реальная и огромная проблема», - предупредил Приско. «Квантовая грамотность должна повыситься в государственных учреждениях и

корпорациях, прежде чем появится квантовый основной компьютер. Создание квантово-безопасной среды для защиты данных не произойдет в одночасье.»

Сегодняшняя угроза квантовых вычислений

«Атака сбора урожая прямо сейчас может захватить ключ шифрования RSA, который будет храниться до тех пор, пока квантовые вычисления не догонят», - добавил он.

«Нет времени терять зря из-за других классических проблем безопасности, таких как атаки сбора урожая, которые происходят сегодня», - сказал Приско. «Атака сбора урожая - это кража зашифрованных данных и ключа шифрования RSA, используемого для шифрования этих данных. Хотя сегодня ключ невозможно взломать с помощью доступного в настоящее время квантового компьютера, злоумышленник может украсть данные и ключ, недорого хранить их в памяти и расшифровать информацию, когда у них будет доступ к более мощному квантовому компьютеру, который может взломать ключ.»

Эйприл Бурдхардт из Quantum Xchage посоветовал специалистам по безопасности развертывать решения, достаточно гибкие, чтобы развиваться вместе с обеими угрозами и еще не определенными стандартами NIST - и они должны сделать это сейчас.

«Компании должны начать готовиться к квантовой угрозе прямо сейчас, развертывая квантово-безопасные, крипто-гибкие решения, которые могут идти в ногу с меняющимся ландшафтом угроз, не говоря уже о защите от атак сбора урожая», - сказал Бурдхардт Threatpost. «Мы рекомендуем компаниям и правительственным учреждениям применять многоуровневый или комплексный подход к передаче ключей, защищенный алгоритмами кандидатов на пост-квантовую криптографию NIST и / или [квантовым распределением ключей] в стандарте FIPS 140-2. подтвержденная реализация». ***(Becky Bracken. Chinese Breakthrough in Quantum Computing a Warning for Security Teams // Threatpost (https://threatpost.com/chinese-quantum-computing-warning-security/161935/). 07.12.2020).***

***

Російська Федерація та країни ЄАЕС

«…Минцифры предложило продлить сроки создания в России киберполигона с 2021 г., как планировалось ранее, до 2024 г.

Проект с изменениями в постановлении Правительства опубликован на regulation.gov.ru 27 ноября 2020 г. На 2021-2024 гг. запланировано отраслевое и функциональное развитие инфраструктуры киберполигона, а в опытную эксплуатацию его введут в декабре 2020 г., пишет «Коммерсант».

В частности, в проекте, как следует из пояснительной записки, предлагается увеличить долю трат по направлению «затраты организации на закупку работ (услуг) у третьих лиц, непосредственно связанных с реализацией мероприятий» с 25 до 40% в связи с переходом к созданию, развитию и обеспечению

функционирования и эксплуатации отраслевых сегментов киберполигона на период 2021-2024 гг. на базе сформированной в 2019-2020 г. опорной инфраструктуры.

Цель киберполигона – обучать и тренировать специалистов и экспертов в области информационной безопасности, а также тестировать российские решения.

Киберполигон представляет собой инфраструктуру для тестирования программного и аппаратного обеспечения путем моделирования компьютерных атак и отработки реакций на них, а также отработки практических навыков учащихся, специалистов, экспертов и руководителей по обеспечению информационной безопасности.

Продление сроков связано с расширением числа отраслей, для которых создается инфраструктура. Как следует из проекта Минцифры, потребуется создать сегменты инфраструктуры для проведения киберучений не только для банковской и энергетической отраслей, но и телекоммуникационной, транспортной, нефтяной и других. Бизнес может заинтересовать участие в учениях, так как практическая подготовка специалистов в области ИБ пока отстает от зарубежной, добавляет «Коммерсант».

Создание государственного киберполигона для обучения и тренировки специалистов и экспертов в области ИБ, а также тестирования российских решений из этой области предусмотрено федеральным проектом «Информационная безопасность» национальной программы «Цифровая экономика». В регионах планируется создать четыре опорных центра киберполигона, которые подключатся к инфраструктуре оператора. Объем государственной субсидии на проект в 2019-2020 гг. составил 364,55 млн руб., на 2021-2024 годы в бюджете заложены еще 600 млн руб…» ***(Ирина Пешкова. Минцифры перенесет на три года создание российского киберполигона // CNews (https://www.cnews.ru/news/top/2020-12-03_mintsifry_pereneset_na_tri). 03.12.2020).***

***

«В России могут обязать операторов персональных данных сообщать ФСБ о компьютерных атаках. С таким предложением выступили депутаты из комиссии Госдумы по иностранному вмешательству. На положения внесенного вчера законопроекта о сокрытии данных силовиков и судей обратил внимание "Коммерсант".

По нынешней версии закона "О персональных данных", оператор должен вести "контроль за принимаемыми мерами по обеспечению безопасности" данных. Теперь депутаты хотят прописать там обязанности оператора "осуществлять взаимодействие с государственной системой обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы РФ".

Речь идет о системе ГосСОПКА, которая появилась в 2013 году. Центры этой системы придется создавать у себя организациям, которые относятся к критической информационной инфраструктуре, в том числе из энергетической, банковской и оборонной отраслей. ФСБ отчитывалась, что с помощью системы рассылала им "рекомендации по обеспечению защиты от [компьютерного] вируса" во время кибератаки в 2017 году.

К операторам персональных данных могут относиться также организации и физлица. В соответствующем реестре Роскомнадзора сейчас 416 250 участников.

По мнению экспертов, подключение к ГосСОПКА приведет "к существенным сложностям и затратам для малого и среднего бизнеса". ***(Операторов персональных данных могут обязать сообщать ФСБ о компьютерных атаках // Каспаров.Ru (https://www.kasparov.ru/material.php?id=5FD0802B98CC6). 09.12.2020).***

***

«Под прикрытием «учений по кибербезопасности» правительство Казахстана заставляет жителей Нур-Султана (Астаны) устанавливать цифровой сертификат на свои устройства, если они хотят иметь доступ к иностранным интернет-сервисам. Сертификат позволит правительству отслеживать весь трафик https с пользовательских устройств с помощью техники Man-in-the-middle.

С 6 декабря 2020 года интернет-провайдеры Казахстана (Beeline, Tele2 и Kcell) перенаправляют пользователей из Нур-Султана на веб-страницы с инструкцией по установке сертификата. Утром того же дня жители получили СМС-оповещение о новых правилах.

Пользователи Казахстана сообщили, что они не могут получить доступ к Google, Twitter, YouTube, Facebook, Instagram и Netflix пока не установят сертификат.

Это третья попытка правительства страны установить подобный сертификат на устройства своих граждан. Первая была в декабре 2015 года, вторая – в июле 2019. Обе провалились после того, как разработчики браузеров внесли сертификат в черный список.

В пятницу власти опубликовали заявление, в котором описывали данные меры как учения по кибербезопасности для государственных учреждений и частных компаний. Они сообщили, что кибератаки на «казахстанский сегмент интернета» выросли в 2,7 раза во время пандемии – и это является основной причиной учений. Сколько они продлятся не сообщается. Точно такой же предлог власти страны использовали в 2019 году – «меры безопасности для защиты граждан».

Ожидается, что разработчики браузеров заблокируют сертификат, как и в предыдущие разы». ***(Правительство Казахстана перехватывает трафик https в столице // SecureNews (https://securenews.ru/the-government-of-kazakhstan-intercepts-https-traffic-in-the-capital/). 07.12.2020).***

***

«Google и Apple вместе с Microsoft и Mozilla заблокировали в своих браузерах шпионский сертификат, который власти Казахстана начали навязывать пользователям в декабре 2020 г. Он позволяет правительству контролировать весь интернет-трафик, и разработчики посоветовали не ставить его или пользоваться VPN-сервисами, если установка все же была произведена.

Бойкот слежке за пользователями

Компании Apple, Google, Microsoft и Mozilla выступили против решения властей Казахстана отслеживать любой, даже шифрованный трафик своих граждан и гостей страны. Чиновники хотят контролировать все перемещения людей по интернету и угрожают блокировкой доступа к зарубежным веб-сервисам в случае отказа пользователей подчиняться.

Как сообщал CNews, в начале декабря 2020 г. на телефоны абонентов казахстанских операторов связи стали поступать сообщения о необходимости установки специального сертификата безопасности, который и предназначен для контроля веб-трафика с мобильных устройств. Портал Engadget пишет, что Apple, Google, Microsoft и Mozilla приняли совместное решение блокировать сертификат в своих браузерах Safari, Chrome, Edge и Firefox.

Правительство Казахстана объяснило свои усилия по перехвату HTTPS-трафика как учения по кибербезопасности для государственных учреждений, телекоммуникационных компаний и частных компаний. Они сослались на тот факт, что кибератаки, нацеленные на «казахстанский сегмент Интернета», выросли в 2,7 раза во время пандемии коронавируса COVID-19.

Рекомендации ИТ-компаний

Жители и гости Казахстана, выполнившие требование властей по установке их сертификата, пишет Engadget, при попытке выйти в интернет через Safari, Chrome, Edge и Firefox увидят на экране своего гаджета сообщение об ошибке. В нем будет сказано, что установленному сертификату нельзя доверять. Пока неизвестно, смогут ли пользователи обходить это сообщение и посещать сайты вопреки рекомендациям разработчиков.

Mozilla также опубликовала заявление, в котором уведомила всех своих пользователей об опасности установки казахстанского сертификата. Всем, кто все же установил его, Mozilla, Google, Apple и Microsoft рекомендуют выходить в интернет через VPN-сервис, чтобы власти не могли отследить их трафик, или установить защищенный браузер Tor. Самый быстрый способ воспользоваться VPN на «зараженном» сертификатом устройстве – это скачать браузер Opera, в котором по умолчанию есть такой сервис (активируется в настройках, не требует авторизации, работает в инкогнито-вкладках).

Как власти ломали интернет в Казахстане

CNews писал, что некоторые жители Казахстана, а также граждане России, отказались ставить на свои смартфоны сомнительный сертификат. Последствия, о которых предупреждали власти страны (блокировка иностранных сервисов) настигли некоторых из них – пользователи стали жаловаться на недоступность YouTube, Facebook и Instagram. Другие отмечали, что у них все эти ресурсы работали в прежнем режиме.

В 2019 г. чиновники Казахстана уже предпринимали попытку заставить граждан установить сертификат. Но на тот момент о коронавирусе COVID-19 еще никто не слышал, и власти пытались убедить граждан выполнить их «просьбу» якобы для защиты их от киберугроз и противоправного контента.

Схема распространения сертификата была идентичной – операторы уведомляли своих абонентов о необходимости его установки в SMS-сообщениях и давали прямую ссылку на его скачивание. Массовая рассылка сообщений началась

в июле 2019 г., и на тот момент разработчикам браузеров потребовалось около месяца, чтобы отреагировать.

Google и Mozilla выступили решительно против инициативы правительства Казахстана лишь в августе 2019 г. Они заблокировали сертификат в Chrome и Firefox и предупредили пользователей об опасности, которую он несет. К примеру, Google, как пишет портал ArsTechnica, внесла его в список отозванных сертификатов (CRLSets), который используется в браузере Chrome для быстрой блокировки сертификатов в экстренных ситуациях. Более того, Google заявила тогда, что «сертификат будет добавлен в черный список в исходном коде Chromium и, следовательно, должен быть включен в другие браузеры на основе этого него.

Идеи тотального контроля

Планы по контролю всего веб-трафика граждан и гостей страны руководство Казахстана вынашивает годами. Началось все осенью 2015 г., но не с еще одного сертификата безопасности, а с точечного изменения законодательства.

Чиновники приняли поправки к закону Казахстана «О связи», в соответствие с которыми на телеком-операторов была возложена обязанность уже с начала 2016 г. «осуществлять пропуск трафика с использованием протоколов, поддерживающих шифрование, с применением сертификата безопасности, за исключением трафика, шифрованного средствами криптографической защиты информации на территории республики». Первый сертификат власти были намерены подготовить для рассылки не позднее декабря 2015 г., но этот план по неустановленным причинам провалился. В итоге идею тотального контроля в стране отложили на 3,5 года, до июля 2019 г». ***(Эльяс Касми. Chrome, Edge, Firefox и Safari не будут работать с ПО, которым власти Казахстана шпионят за гражданами // CNews (https://safe.cnews.ru/news/top/2020-12-18_itkorporatsii_vosstali_protiv). 18.12.2020).***

***

Інші країни

«Госконтролер Матаньягу Энгельман заявил 7 декабря, что его сотрудники проводят проверку готовности Центральной избирательной комиссии к кибератакам.

Как сообщает «Маарив», ведомство госконтролера сейчас завершает всестороннюю проверку компьютерных систем ЦИК к отражению нападений в киберпространстве. По словам госконтролера, угрозы еврейскому государству, его институтам и учреждениям как в обычном, так и в компьютерном мире становятся все более серьезными». ***(ЦИК Израиля: проверка готовности противостоять киберугрозам // ISRAland Online (http://www.isra.com/news/253195). 07.12.2020).***

***

«Сегодня, 11 декабря 2020 года, Федеральный совет принял решение, что в Швейцарии целесообразно ввести общую обязанность сообщать о кибератаках. Если данную идею поддержит также парламент (и при созыве референдума – также швейцарский народ), то на операторов критически важных

инфраструктурных объектов станет распространяться обязанность сообщать о кибератаках и обнаружении брешей в системах безопасности.

Соответствующий законопроект должен быть подготовлен до конца 2021 года. В рамках парламентских дебатов будет определено, какие из критически важных инфраструктурных секторов (например, здравоохранение, водоснабжение, питание, энергетика, телекоммуникации и транспорт) должны сообщать о происшествиях и в течение какого срока.

Для сбора и анализа отчётов правительство Швейцарии намерено создать центральный офис. Следует указать, что для некоторых критически важных инфраструктурных объектов Швейцарии уже на настоящий момент существует обязанность по отчетности.

Обязанность сообщать о кибератаках – при всей своей благовидности – является, как минимум, противоречивой.

Во-первых, введение названной обязанность для госпредприятий Швейцарии (Федеральные железные дороги, Гостелевидение и радио, ПостФинанс и т.п.) в силу их принадлежности государству и контролю со его стороны видится допустимым. Напротив, проблематичным будет регулирование, при котором обязанность сообщать о кибератаках будет распространяться также на частные компании. В таком случае компаниям придётся создавать специальные отделы для работы с федеральным офисом; если в обязанность по отчётности попадёт также малый и средний бизнес, то именно он наиболее сильно почувствует бремя дополнительных затрат.

Во-вторых, часто крайне сложно отделить информацию о кибератаке от сведений, которые позволят сделать предположение, на кого именно была совершена атака. В таких случаях, сообщающие об инцидентах компании рискуют потерять репутацию.

В-третьих, следует опасаться бюрократизации всей сферы защиты от кибератак. Федеральные чиновники и чиновники госпредприятий – мягко выражаясь – далеко не всегда являются самыми эффективными. В данной связи, стоит лишь напомнить, что Почта Швейцарии провалила создание системы электронного голосования. В итоге – после потери времени и денег налогоплательщиков – провал пришлось признать. Тем не менее, Почта Швейцарии попросила денег на второй заход». ***(Марад Видмер. В Швейцарии введут обязанность сообщать о кибератаках? // Швейцария Деловая (https://business-swiss.ch/2020/12/v-shvejcarii-vvedut-objazannost-soobshhat-o-kiberatakah/). 11.12.2020).***

***

Протидія зовнішній кібернетичній агресії

«Служба безпеки Норвегії заявила про можливу причетність хакерів із Росії до кібератаки на систему електронної пошти норвезького парламенту в серпні цього року.

…розслідування показало, що, ймовірно, операцію проводило угруповання хакерів APT28, також відоме як Fancy Bear, яку спецслужби пов'язують із російською розвідувальною службою ГРУ.

У відомстві зазначають, що інформація в поштовій системі «становить великий інтерес для розвідувальних служб декількох іноземних держав», а кібератака 24 серпня є частиною «більшої кампанії національного і міжнародного масштабу» і триває щонайменше від 2019 року.

Представники спецслужби, відомої за скороченою назвою PST, повідомили, що вирішили зупинити розслідування, оскільки воно не надало «достатньої інформації» для обвинувачення.

Російське посольство в Норвегії заявило, що PST не вдалося зібрати докази про причетність Росії, і назвало заяви норвезької сторони «неприйнятними».

Міністр закордонних справ Норвегії Іне Марі Еріксен Серейде заявила, що це серйозна подія, яка торкнулася найважливішого інституту демократії. За її словами, згідно з наявною інформацією, «за цією діяльністю стоїть Росія»…». ***(У Норвегії хакерів із Росії запідозрили в атаці на парламент // Радіо Свобода (https://www.radiosvoboda.org/a/news-norvehia-khakerska-ataka-rosia/30990602.html). 08.12.2020).***

***

«Избирательное возмездие — новая стратегия киберзащиты

В то время, когда конфликты между странами все чаще происходят в сети, требуется новое стратегическое видение, говорится в статье, размещённой в последнем выпуске American Political Science Review.

В обычных войнах агрессия сдерживается ответными военными ударами по противнику. Но если у ракеты есть обратный адрес, то у компьютерного вируса, как правило, нет. Ответные действия на основании ограниченной информации, например о местонахождении определенных IP-адресов, могут быть контрпродуктивными.

«Концентрация внимания на наиболее вероятных виновниках может быть большой ошибкой», — говорит Александр Волицки (Alexander Wolitzky) из Массачусетского технологического института (MIT), специализирующийся на теории игр. Вместе с коллегами из Северо-Западного и Чикагского университетов он считает, что существует жизнеспособный новый подход, основанный на более оправданном и хорошо информированном применении выборочного возмездия.

В своей статье ученые подробно изучили сценарии, в которых страны знают о кибератаках против них, но не обладают достоверной информацией о злоумышленниках. Они показали, что, что многосторонний характер кибербезопасности повышает риск того, что ошибочно адресованная контратака может возыметь обратный эффект, став причиной серии дополнительных атак из нескольких источников.

«Оптимальной доктриной в такой ситуации будет принимать ответные меры главным образом в отношении самых ясных и однозначных сигналов», — говорит Волицки.

Авторы надеются, что их документ вызовет обсуждение во внешнеполитических кругах, поскольку кибератаки по-прежнему являются серьезным источником угроз для национальной безопасности.

Как отмечает Волицки, описанная в статье модель применима и к вопросам, выходящим за рамки кибербезопасности, например, к защите окружающей среды, имеющей ту же специфику. Если множество фирм загрязняют реку, то оштрафовав одну из них, можно лишь уверить другие в их безнаказанности». ***(Избирательное возмездие — новая стратегия киберзащиты // Компьютерное Обозрение (https://ko.com.ua/izbiratelnoe_vozmezdie_novaya_strategiya_kiberzashhity_135620). 11.12.2020).***

***

«Ранее в этом году Белферский центр Гарвардского университета опубликовал свой Национальный индекс кибернетической мощи (NCPI), который оценивает 30 стран в соответствии с их цифровыми возможностями. Центральное место в рейтинге занимает способность нации как защищаться от кибератак, так и вести кибервойну.

«Кибервласть состоит из нескольких компонентов и должна рассматриваться в контексте национальных целей страны», - объясняют авторы. «В рамках NCPI мы измеряем государственные стратегии, возможности защиты и нападения, распределение ресурсов, частный сектор, рабочую силу и инновации. Наша оценка является одновременно мерой доказанной силы и потенциала, где окончательная оценка предполагает, что правительство этой страны может эффективно использовать эти возможности».

В отчете показано, что кибербезопасность играет все более важную стратегическую роль в судьбах стран, будь то вмешательство в выборы или кража результатов исследований вакцины COVID. Это особенно верно, когда власть для разрушения принадлежит не только государственным субъектам, но и все более мощному числу негосударственных сил, у которых есть средства и мотивация для разрушения.

Национальные стратегии кибербезопасности

Учитывая такое положение дел, возможно, неудивительно, что более 100 правительств, как считается, разработали национальные стратегии защиты от кибербезопасности для борьбы с внутренними угрозами, которые кибератаки представляют для национальной инфраструктуры, бизнеса и самих граждан. Среди этих разнообразных и разрозненных стратегий выделяются пять общих черт.

1. Специальное агентство по кибербезопасности

Для обеспечения надежной и надежной защиты кибербезопасности на национальном уровне жизненно важно, чтобы одно агентство несло общую ответственность за планы и защиту. Такое агентство может продвигать повестку дня в области кибербезопасности в стране и, вероятно, будет контролировать портфель инициатив по защите ключевой инфраструктуры, быстрому реагированию на атаки и определению стандартов кибербезопасности. Очевидно, что для того, чтобы такое агентство было эффективным, потребуются

соответствующие навыки как внутри организации, так и через партнерство с внешними агентствами как в правительстве, так и в частном секторе.

2. Программа защиты критически важной инфраструктуры.

Неизбежные ограничения ресурсов будут означать, что любое национальное агентство по кибербезопасности должно будет сосредоточить свои усилия на определенных областях. Безусловно, наиболее важной из этих областей является критическая инфраструктура, которая остается наиболее привлекательной целью для враждебных государственных субъектов. Нарушение этой инфраструктуры может иметь разрушительные последствия для общества, экономики и национальной безопасности в целом. Критическая инфраструктура обычно включает в себя сочетание операционных и информационных технологий, что усложняет ее успешную защиту. Лучшие умеют расставлять приоритеты в важнейших секторах и активах; надежный механизм управления; стандарты кибербезопасности для защиты критически важных активов, признанные во всем мире.

3. Четко определенный план реагирования на инциденты и восстановления.

В сообществе кибербезопасности преобладает мнение, что дело не в том, произойдет ли кибератака, а когда. Только если вы признаете, что кибератаки неизбежны, вы сможете начать адекватно планировать надежную защиту от атак и ответы на них. На национальном уровне ситуация ничем не отличается, поэтому правительства должны разработать план реагирования на инциденты и восстановления, чтобы ограничить эффект атак и ускорить восстановление. Лучшие из этих планов обычно имеют ряд общих функций, включая активный мониторинг ландшафта угроз; четкий путь для бизнеса и граждан для сообщения об угрозах и нападениях; проактивные меры по борьбе с угрозами; многовариантные источники информации об угрозах; надежный план мобилизации для ответа на нападения; и инструменты оценки серьезности, стандартизированные для всей экономики.

4. Четко определенные законы для всех форм киберпреступности.

Сфера киберугроз быстро развивается, поэтому жизненно важно, чтобы законы адаптировались и развивались с учетом этой ситуации. Успех во многом зависит от способности решать, какие аспекты кибербезопасности они хотят законодательно закрепить, а по каким аспектам они просто хотят дать рекомендации. Будапештская конвенция обеспечивает хорошую основу для подражания правительствам, и в настоящее время ее придерживаются более 60 стран. В нем подчеркивается, что странам было бы хорошо принять как процессуальные, так и материальные законы, чтобы не только определить полномочия и обязанности каждой страны, но и способы их применения. Глобальный характер киберпреступности означает, что страны также должны стремиться участвовать в глобальных усилиях по обмену разведданными и угрозами, а также сотрудничать в расследовании киберпреступлений.

5. Надежная и динамичная экосистема кибербезопасности.

И последнее, но не менее важное: кибербезопасность - это то, что затрагивает все общество, поэтому правительствам потребуется помощь со стороны частного сектора, сообщества кибербезопасности и граждан для разработки наиболее

надежной национальной стратегии. Наиболее успешные страны смогли создать экосистему стартапов и предпринимателей, связанных с кибербезопасностью, а также сформировать рабочую силу с надежными навыками кибербезопасности и кибер-осведомленное население, которое знакомо с рисками, с которыми сталкивается в Интернете, и имеет соответствующие привычки к цифровой гигиене.

Общество бесконечно лучше, когда оно защищено от действий киберпреступников. Сделать это отнюдь не просто, но все лучшие страны хорошо охватывают вышеуказанные элементы своей национальной стратегии. Их указания служат руководством для тех, кто не настолько продвинут, и показывают им, что нужно сделать, чтобы наверстать упущенное. Учитывая постоянную угрозу кибератак, ни одна страна не может позволить себе игнорировать этот процесс». ***(Adi Gaskell. The National Cyber Power Index: Does your country have a cybersecurity strategy? // CyberNews Investigation (https://cybernews.com/security/the-national-cyber-power-index-does-your-country-have-a-cybersecurity-strategy/). 14.12.2020).***

***

«Важность надежной кибербезопасности на национальном уровне редко подчеркивалась так, как в 2020 году.

В прошлом году реагированию на COVID препятствовали кибератаки, в то время как президентские выборы были пронизаны опасениями по поводу иностранного вмешательства и фальсификации результатов голосования. Поэтому неудивительно, что Гарвард начал публиковать рейтинговую таблицу по цифровым возможностям страны.

Национальный индекс Cyber Сила стремится сравнить способность каждой страны, чтобы успешно защитить себя от кибератак. Это инструмент, который, безусловно, интересен с академической точки зрения, но его статический характер не обязательно помогает командам по кибербезопасности здесь и сейчас. Именно здесь намеревается вмешаться новая база данных, разработанная исследователями из Университета Джона Хопкинса.

Индекс прогнозирования кибератак (CAPI) обеспечивает определенную степень предвидения возможных кибератак на национальном уровне. Например, первоначальное сканирование предполагает, что существует большая вероятность кибератаки России на Украину, при этом вторым наиболее вероятным является нападение Соединенных Штатов на Иран.

«Использование кибероперациий для деградации и нарушения критически важной инфраструктуры, для отправки политического послания, срыва экономической деятельности или для формирования враждебных целей национальной безопасности привело к новому типу конфликта между национальными государствами», - поясняет команда. «По мере того, как все больше стран развивают киберпотенциал, кибератаки, вероятно, станут более распространенным явлением в международных отношениях».

Прогнозирование угроз

Инструмент обеспечивает прогнозный анализ стран, которые с наибольшей вероятностью будут участвовать в кибервойне. Инструмент был разработан после анализа ряда крупных атак, предпринятых с 2008 года, чтобы попытаться определить, выделяются ли какие-либо конкретные характеристики, которые позволили бы предсказать будущие атаки.

«Эти атаки создают прецедент или выделяются как уникальные по своим предполагаемым эффектам», - поясняет команда. «Атрибуция атак в наших тематических исследованиях была подтверждена публичным признанием правительства США, убедительными аргументами исследователей или, в некоторых случаях, самоидентификацией самих злоумышленников».

После оценки деталей каждой атаки был выделен ряд общих факторов:

Хорошо осведомленные и организованные киберсилы - как ранее указывалось в Гарвардском индексе, ключевым компонентом кибератак любого государства являются доступные им навыки. Однако команда Джона Хопкинса идет дальше и подчеркивает важность не только сильной базы талантов, но и способности применять передовые технологии против врага.

Жалобы на национальном уровне - кибератаки становятся все более распространенной международной реакцией, когда более традиционные дипломатические меры считаются слишком мягкими, а военная реакция - слишком суровыми.

Отсутствие страха перед последствиями. Очевидно, что немногие страны хотят открытой войны, поэтому ощущение, что они могут провести свою атаку без репрессалий, будь то экономические, юридические, военные или кибернетические, является явным мотивирующим фактором. Перед тем, как продолжить, государства взвесят потенциальные риски и последствия своих действий.

Согласованность атаки с политикой национальной безопасности. Несколько более сложный фактор, который следует учитывать, - это общее соответствие стратегии национальной безопасности страны. Часто это не те вещи, которые являются общественным достоянием, поэтому исследователи признают, что требуется определенная степень догадок, чтобы объединить то, что является общественным достоянием, с тем, что не является общественным достоянием.

Технологические уязвимости, выявленные в атакованной стране. И последнее, но не менее важное, это уязвимости инфраструктуры целевой страны. Очевидно, что каждая сетевая архитектура имеет уязвимости, но у одних их будет больше, чем у других. Исследователи называют такие страны, как Россия и Китай, трудными целями именно из-за ограничительной политики в отношении доступа в Интернет и их относительно передовых технологий.

Каждый из этих факторов оценивается по шкале от 1 до 5, причем более высокие баллы означают более высокую вероятность возникновения атаки. На веб-сайте представлены 12 сценариев, иллюстрирующих действие инструмента, с маловероятными событиями, такими как нападение Индии на Китай, с одной стороны, и событиями с высокой вероятностью, такими как нападение Израиля на Иран, с другой.

Инструмент был разработан в 2019 году по мере роста угрозы, исходящей от вредоносных программ. Исследователи, за плечами которых несколько

десятилетий опыта работы в таких организациях, как Агентство национальной безопасности, стремятся помочь политикам и другим должностным лицам понять, где риски наиболее высоки.

Они создали Консультативный совет CAPI, в который входят различные заинтересованные стороны. Группа регулярно встречается для обсуждения некоторых горячих точек, выявленных проектом, и изучения некоторых последствий любых кибератак, которые могут разворачиваться.

Поскольку кибервойна становится все более распространенным явлением, подобные инструменты, вероятно, станут частью растущего арсенала, используемого для понимания, прогнозирования и последующей защиты от возможных атак». ***(Adi Gaskell. Predicting where cyberattacks will take place // CyberNews Investigation (https://cybernews.com/security/predicting-where-cyberattacks-will-take-place/). 10.12.2020).***

***

«Федеральные органы видели продолжающиеся кибератаки на аналитические центры (занимающиеся шпионажем, доставкой вредоносных программ и т.д.), с использованием фишинга и эксплойтов VPN в качестве основных векторов атак.

Агентство по кибербезопасности и безопасности инфраструктуры (CISA) и ФБР выступили с предупреждением о том, что они называют постоянными, продолжающимися кибератаками со стороны субъектов повышенной постоянной угрозы (APT), нацеленных на аналитические центры США.

По данным федеральных органов, злоумышленники стремятся украсть конфиденциальную информацию, получить учетные данные пользователей и получить постоянный доступ к сетям жертв.

Кибернетические вторжения в первую очередь направлены на тех, кто сосредоточен на международных делах или политике национальной безопасности, говорится в предупреждении, выпущенном на этой неделе, что, возможно, неудивительно, учитывая геополитический характер APT, которые, как правило, поддерживаются национальными государствами.

«Учитывая важность, которую аналитические центры могут иметь в формировании политики США, CISA и ФБР призывают отдельных лиц и организации, занимающиеся международными делами и национальной безопасностью, немедленно повысить уровень осведомленности», - говорится в предупреждении.

Что касается воздействия, APT-атаки в первую очередь ориентированы на шпионаж и стремятся похитить данные. По данным CISA и ФБР, наблюдаемая шпионская деятельность включает сброс учетных данных, ведение кейлоггеров, сбор аудио, кражу электронных писем, загрузку файлов и многое другое.

«Киберпреступники работают над тем, чтобы получить доступ к организациям, в которых работают самые умные и лучшие люди, для сбора определенной информации, данных о «новейших» технологиях или стратегических проектах, чтобы улучшить свои собственные усилия», - сказал Джеймс Маккуигган, специалист по безопасности в KnowBe4 по электронной почте.

«Мы по-прежнему видим, что киберпреступники нацелены на организации, которые разрабатывают или управляют интеллектуальной собственностью, поэтому логично, что аналитические центры являются главной целью», - добавил Стивен Банда, старший менеджер по решениям безопасности в Lookout, по электронной почте.

Однако этот доступ может быть использован и в более гнусных целях.

«Если бы человек неосознанно поделился своими учетными данными с киберпреступником, хакер мог бы не только получить доступ к сети жертвы, но и отправить электронные письма из учетной записи этого человека, создавая впечатление, что отправляемые им сообщения были на 100 процентов законными и, потенциально может повлиять на политику США», - сказал Эд Бишоп, технический директор и соучредитель Tessian.

Помимо кражи информации, в предупреждении содержалось предупреждение о том, что некоторые атаки связаны с доставкой программ-вымогателей, захватом ресурсов для майнинга криптовалют, организацией распределенных атак типа «отказ в обслуживании» (DDoS) или даже стиранием дисков при разрушительных атаках.

Векторы атаки

CISA и ФБР пришли к выводу, что субъекты APT до сих пор полагались на несколько способов первоначального доступа к атакам, включая умные методы социальной инженерии и выдачу себя за доверенных третьих лиц, чтобы обманом заставить жертв обмениваться информацией или учетными данными с помощью целевого фишинга.

«Люди больше полагаются на электронную почту, чтобы оставаться на связи с коллегами, клиентами и поставщиками, и наше недавнее исследование показало, что половина сотрудников с меньшей вероятностью будет придерживаться правил защиты данных при работе из дома», - сказал Бишоп.

Однако CISA и ФБР также отметили, что APT предпринимают более изощренные попытки проникновения в сети, такие как использование уязвимостей в удаленных сетях и других устройствах, подключенных к Интернету.

«Активизация удаленной работы во время пандемии COVID-19 привела к тому, что рабочая сила стала больше полагаться на удаленное подключение, предоставляя злоумышленникам больше возможностей для использования этих подключений и слияния с возросшим трафиком», - заявили федералы.

В результате некоторые злоумышленники используют ошибки в виртуальных частных сетях (VPN) и других инструментах удаленной работы, чтобы получить начальный доступ или постоянство в сети жертвы. Исследователи заявили, что расширение использования персональных устройств и сетей для удаленной работы упрощает этот процесс.

«К сожалению, несмотря на некоторые удобства и эффективность, которые может обеспечить удаленная работа, она значительно расширила поверхность атаки для всех предприятий, включая аналитические центры», - сказал Банда. «Например, группа экспертов из 10 исследователей, которые обычно собираются в одном центральном офисе, теперь сотрудничает из 10 отдельных удаленных

офисов. У каждого «личного офиса» есть свои требования к безопасности и множество подключенных мобильных и стационарных оконечных устройств».

И, наконец, в предупреждении говорится, что некоторые атаки начинаются с компрометации цепочки поставок, подбора паролей или использования украденных действительных учетных данных.

Атаки аналитических центров

Известные атаки на аналитические центры продолжаются. Например, в феврале 2019 года Microsoft предупредила, что российский APT Fancy Bear атакует демократические аналитические центры в Европе.

Совсем недавно Accenture сообщила, что Turla, еще один российский APT, атакует аналитические центры и другие организации, используя удобные для предприятий платформы, в первую очередь Microsoft Exchange, Outlook Web Access (OWA) и Outlook в Интернете, с целью кражи бизнес-учетных данных и другие конфиденциальные данные.

А в конце октября CISA предупредила, что северокорейская APT-группа, известная как Kimsuky, активно атакует аналитические центры, предприятия коммерческого сектора и других, часто выдавая себя за южнокорейских репортеров. Как отмечает CISA, его миссия - глобальный сбор разведывательной информации, который обычно начинается с целевых фишинговых писем, атак с промыванием, совместного использования торрент-файлов и вредоносных расширений для браузеров с целью закрепиться в целевых сетях.

Защита и смягчение последствий

CISA и ФБР рекомендовали аналитическим организациям применять ряд важнейших (но базовых) передовых методов защиты, в том числе проводить обучение по социальной инженерии и фишингу.

«Все организации, в том числе аналитические центры, являются мишенями для национальных государств и киберпреступников, и, фишируя людей, они рассматривают его как более доступный способ проникнуть в системы и инфраструктуру», - сказал Маккуигган. «Организациям необходимо поддерживать сильную программу обучения вопросам безопасности и часто обновлять ее, чтобы держать сотрудников в курсе последних моделей атак и фишинговых писем. Сотрудники могут принимать правильные решения для выявления потенциальных фишинговых писем и сообщать о них. Это действие создает более прочную культуру безопасности и позволяет организации работать над тем, чтобы стать более важным активом для отдела безопасности».

В предупреждении также говорилось о сегментации сети, хорошей гигиене паролей и многофакторной аутентификации, своевременной установке исправлений, использовании антивирусного программного обеспечения и надежном шифровании данных.

Банда также подчеркнул, что аналитические центры должны осознавать, что мобильные устройства могут быть особенно слабым звеном.

«Учитывая, что 85% мобильных фишинговых атак происходят вне электронной почты, времена, когда уделялось внимание только фишинговым атакам по электронной почте, давно прошли», - сказал он. «Фишинговые атаки нацелены на мобильных пользователей, использующих текстовые сообщения,

платформы для обмена сообщениями в социальных сетях и мобильные приложения». ***(Tara Seals. Think-Tanks Under Attack by Foreign APTs, CISA Warns // Threatpost (https://threatpost.com/think-tanks-attack-apts-cisa/161807/). 02.12.2020).***

***

«Австралийское национальное разведывательное сообщество (NIC) надеется создать высокозащищенную частную облачную службу сообщества, способную защищать данные, которые полностью засекречены до уровня совершенно секретности.

Управление национальной разведки (ONI), ведущее разведывательное агентство Австралии, возглавляет проект и в пятницу объявило о выражении заинтересованности.

«Сетевая карта стремится повысить свою способность переносить и извлекать релевантные данные из сложных источников данных. Она видит общие наборы инструментов для фильтрации и обработки данных для извлечения релевантной полезной информации как множителя силы», - пишет ONI.

«Сетевая карта стремится к большей функциональной совместимости за счет общих общих служб, общей инфраструктуры и стандартов, централизации служб и способности создавать среды для совместной работы».

Все 10 агентств NIC в конечном итоге будут использовать облако: ONI, Австралийское управление сигналов (ASD), Австралийская организация геопространственной разведки, Австралийская секретная разведывательная служба, Австралийская служба безопасности и разведки (ASIO), Организация военной разведки, Австралийская комиссия по уголовной разведке и разведка функции Австралийской федеральной полиции, Австралийского центра отчетов и анализа транзакций (Austrac) и Министерства внутренних дел.

Платформа также позволит «доверенным третьим сторонам» использовать сервисы «программное обеспечение как услуга» (SaaS) в частном облаке сообщества.

Руководство ONI этим проектом, да и сам проект, основано на рекомендациях Independent Intelligence Review 2017 года.

«Мы рекомендуем, чтобы аналитика данных и подключение к ИКТ, включая создание вычислительной среды разведывательного сообщества, в которой технические барьеры для сотрудничества сведены к минимуму, были одними из высших приоритетов более структурированного подхода к технологическим изменениям и финансированию совместных возможностей», в обзоре сказано.

В проекте не участвуют агентства, собирающие новые данные. И при этом не расширяет их круг ведения. Все существующие нормативные положения по-прежнему применяются.

Напротив, NIC надеется, что облако сообщества улучшит его способность анализировать данные и обнаруживать угрозы, а также улучшит совместную работу и совместное использование данных.

«Совершенно секретно» - это самый высокий уровень в Австралийской политике безопасности. Он представляет собой материал, который в случае

публикации может иметь «катастрофические последствия для бизнеса» или нанести «исключительно серьезный ущерб национальным интересам, организациям или отдельным лицам».

До недавнего времени единственным крупным поставщиком облачных услуг, который обрабатывал сверхсекретные данные, по крайней мере, в соответствии со стандартами правительства США, были Amazon Web Services (AWS). В 2017 году AWS запустил работу с секретным регионом AWS, нацеленным на разведывательное сообщество США, включая ЦРУ, и другие правительственные учреждения, работающие с наборами данных секретного уровня.

В Австралии AWS был сертифицирован как защищенный уровень, на два уровня классификации ниже совершенно секретного. «Защищенная» сертификация поступила через список сертифицированных облачных сервисов ASD (CCSL), который был закрыт в июне, в результате чего сертификаты, полученные в процессе CCSL, стали недействительными.

В рамках ISM 92 сервиса AWS были оценены как защищенные. В 2019 году он также заключил сделку с правительственным сектором Австралии.

Хотя CCSL больше не существует, ожидается, что Программа зарегистрированных оценщиков информационной безопасности (IRAP) будет поддерживать правительство в поддержании их деятельности по обеспечению гарантий и управлению рисками.

На этой неделе Microsoft запустила облако совершенно секретно для государственных учреждений Azure для обработки секретных данных на всех уровнях, включая совершенно секретные, для клиентов из правительства США. Однако Microsoft все еще работает с правительством для получения аккредитации.

В соответствии с CCSL Microsoft также могла хранить правительственную информацию на защищенном уровне. В отличие от всех предыдущих подобных сертификатов, сертификаты Microsoft были предварительными и сопровождались тем, что ASD называет «руководствами для потребителей».

В 2019 году ASIO выразила заинтересованность в использовании Microsoft Azure для внутренних целей для защищенных, секретных и совершенно секретных данных.

В Великобритании частная компания UKCloud запустила свой потенциально совершенно секретный сервис UKCloudX в 2018 году. UKCloud уже является поставщиком облачных сервисов для G-Cloud правительства Великобритании по контракту с государственным закупочным агентством Crown Commercial Services.

Однако ONI стремится исследовать рынок, и поставщики, имеющие опыт предоставления безопасных облачных сред, могут подавать заявки, даже если у них еще нет совершенно секретной сертификации.

Однако облако должно размещаться в инфраструктуре, физически расположенной в Австралии и географически рассредоточенной.

«[Это] первый этап многоэтапного процесса закупок, с помощью которого ONI определит, какие респонденты будут приглашены для участия в следующем этапе процесса закупок», - пишет ONI.

Выражение заинтересованности закрывается 8 февраля 2021 года». ***(Stilgherrian. Australian intelligence community seeking to build a top-secret cloud //***

ZDNet (https://www.zdnet.com/article/australian-intelligence-community-seeking-to-build-a-top-secret-cloud/). 11.12.2020).

***

«Министерство внутренней безопасности США опубликовало сегодня «бизнес-совет», в котором американские компании предупреждают о недопустимости использования аппаратного оборудования и цифровых сервисов, созданных или связанных с китайскими компаниями.

В DHS заявили, что китайские продукты могут содержать бэкдоры, лазейки или скрытые механизмы сбора данных, которые могут использоваться китайскими властями для сбора данных от западных компаний и передачи информации местным конкурентам для достижения экономических целей Китая в ущерб другим странам.

Агентство заявило, что все оборудование и услуги, удаленно связанные с китайскими компаниями, следует рассматривать как риск для кибербезопасности и бизнеса.

DHS утверждает, что законы о национальной безопасности Китая позволяют правительству принуждать любую местную компанию и гражданина изменять продукты и заниматься шпионажем или кражей интеллектуальной собственности.

DHS охарактеризовало эту практику как «кражу данных, спонсируемую правительством КНР».

«Слишком долго американские сети и данные подвергались киберугрозам из Китая, которые используют эти данные, чтобы дать китайским компаниям несправедливое конкурентное преимущество на мировом рынке», - сказал исполняющий обязанности министра внутренней безопасности Чад Ф. Вольф.

«Практика, которая дает правительству КНР несанкционированный доступ к конфиденциальным данным - как личным, так и частным - подвергает экономику и бизнес США прямому риску эксплуатации. Мы призываем предприятия проявлять осторожность перед заключением любого соглашения с фирмой, связанной с КНР».

В отдельном выступлении в понедельник Вольф также охарактеризовал Китай как «явную и реальную опасность» для демократии США.

DHS опубликовало свои рекомендации менее чем за месяц до смены администрации, и президент Байден, как ожидается, назначит своего начальника DHS в следующем месяце.

При администрации Трампа официальные лица США сосредоточили свое внимание на борьбе с китайскими кражами у американских компаний.

В интервью Fox News в июле 2020 года директор ФБР Кристофер Рэй сказал, что половина из почти 5000 контрразведывательных дел ФБР связана с кражей китайских технологий в США…». ***(Catalin Cimpanu. DHS warns against using Chinese hardware and digital services // ZDNet (https://www.zdnet.com/article/dhs-warns-against-using-chinese-hardware-and-digital-services/). 23.12.2020).***

***

«Команда обраного президента США Джо Байдена розглядає варіант введення нових санкцій проти Росії. Після вступу на посаду глава Білого дому

розгляне кілька варіантів покарання РФ за злом урядових агентств і компаній США…

…відповідь США має бути достатньо сильною, щоб створити великі економічні, фінансові та технологічні втрати для злочинців.

Однак санкційні заходи водночас мають дозволити уникнути ескалації конфлікту між двома ядерними державами. Як відповідь США Байден може розглянути: економічні заходи та відповідні кібератаки проти Росії.

"Для створення ефективного стримування і зниження ймовірності кібершпіонажу в майбутньому", - цитує джерело агентство.

Раніше повідомлялося, що хакери, які працюють, ймовірно, на російський уряд, зламали Міністерство внутрішньої безпеки США, а також управління з комунікацій та інформації. Згідно з інформацією, хакерам доступний трафік електронної пошти у цих відомствах. Зокрема, хакерам вдалося обійти засоби захисту та аутентифікації від Microsoft.

РБК-Україна писало, що в США неодноразово заявляли про хакерські атаки. Зокрема, у жовтні Агентство з кібербезпеки та інфраструктурної безпеки в США (CISA) виявило хакерську атаку на урядові мережі. За матеріалами РБК-Україна». ***(Команда Байдена розглядає санкції проти РФ за кібератаки, - Reuters // Информационное агентство ЦК (http://expert.org.ua/v-mire/2020/komanda-baydena-rozglyadaie-sankciyi-proti-rf-za-kiberataki-reuters). 2012.2020).***

***

«Державний секретар США Майк Помпео звинуватив Росію у причетності до масштабної хакерської атаки на американські відомства та компанії…

Кібератака почалася ще навесні цього року, а 14 грудня Вашингтон підтвердив, що цілями стали американське Міністерство фінансів і Національне управління з телекомунікацій та інформації.

«Ми можемо гранично сказати напевне, що в цю атаку була залучена Росія», — заявив Помпео.

За його словами, для вбудовування шкідливого коду в урядові системи США було витрачено багато зусиль.

За даними корпорації Microsoft, що також зазнала нападу, метою хакерів стали понад 40 урядових агентств, аналітичних центрів, неурядових організацій та IT-компаній.

Цілі розташовувалися не лише в США, але і в Канаді, Великій Британії, Іспанії, Бельгії, Ізраїлі, Мексиці та Об'єднаних Арабських Еміратах…». ***(Помпео звинувачує Росію у кібератаках на відомства США // Високий Замок Online. (https://wz.lviv.ua/news/426402-kiberataky-na-vidomstva-ssha-pompeo-zvynuvachuie-rosiiu). 19.12.2020).***

***

«ФБР й інші агенції, які розслідують масштабну кібератаку на урядові мережі США повідомлять членам Конгресу про втручання, за яким, як вважають, стоять російські хакери.

Влада США висловила занепокоєння щодо втручання, від якого, зокрема, постраждали Microsoft і Міністерство енергетики США.

Агентство з кібербезпеки і безпеки інфраструктури (CISA)17 грудня оприлюднило нагальне попередження про кібератаку, заявивши, що вона створює «серйозний ризик» для комп'ютерних мереж урядових установ, комунальних служб і приватного сектору.

У CISA заявили, що видалення шкідливого програмного забезпечення зі скомпрометованих систем «буде дуже складним».

Представники агенцій, що відповідають за кібербезпеку, офіційно не звинувачували Росію в кібератаці, але це зробили деякі члени Конгресу.

Вперше про кібератаку повідомили 13 грудня ЗМІ, які цитували неназваних американських чиновників. За цими даними, від атаки постраждали Департамент національної безпеки, Міністерство фінансів і Міністерство торгівлі США.

У попередженні CISA зазначається, що атака здійснена «терплячим, забезпеченим ресурсами і зосередженим противником».

Посольство Росії в США заперечило причетність Москви…». ***(ФБР доповість Конгресу США про розслідування кібератак, в яких підозрюють російських хакерів // Радіо Свобода (https://www.radiosvoboda.org/a/news-ssha-kiberataka/31007134.html). 18.12.2020).***

***

«Глава Білого дому Дональд Трамп висловив сумнів у причетності Росії до кібератак, в яких Москву звинуватив держсекретар США Майк Помпео

Про це Трам написав у twitter.

Він назвав переоціненим вплив кібератаки на американські урядові відомства та заперечив причетність до неї Росії.

"Кібератака набагато більша у фейкових медіа, ніж у реальності. Росія, Росія, Росія – це головна мелодія, коли щось трапляється, тому що жалюгідний мейнстрім, переважно з фінансових міркувань, смертельно бояться обговорити ймовірність, що це може бути Китай, а може бути!" – написав Трамп.

Президент США позначив у твіті державного секретаря Майка Помпео та главу національної розвідки Джона Ретклiффа». ***(Трамп кинувся захищати Росію після звинувачень Помпео у кібератаках // Espreso.tv (https://espreso.tv/news/2020/12/19/tramp_kynuvsya_zakhyschaty_rosiyu_pislya_zvynuvachen_pompeo_u_kiberatakakh). 19.12.2020).***

***

«Лондон не обладает данными о том, что компьютерные атаки, которые, по утверждениям американских властей, российские хакеры якобы осуществили в отношении Министерства торговли и Министерства финансов США, каким-то образом затронули британские учреждения. Об этом заявил в понедельник представитель премьер-министра Соединенного Королевства Бориса Джонсона.

«Расследования продолжаются. Национальный центр кибербезопасности работает над оценкой последствий для Великобритании, но нам неизвестны на

данный момент какие-либо связанные с Великобританией последствия», - приводит заявление представителя главы правительства агентство Рейтер.

Ранее пресс-служба Министерства торговли США подтвердила корр. ТАСС информацию о взломе компьютерной сети находящегося в его структуре Национального управления по телекоммуникациям и информации. Расследованием занимается ФБР. Как сообщило агентство Рейтер, в американском разведсообществе существует обеспокоенность, что совершившие атаки на управление, а также на Минфин хакеры могли воспользоваться аналогичными методами для взлома других структур правительства США. Ситуация настолько серьезная, что, по данным агентства, было созвано экстренное совещание Совета национальной безопасности (СНБ) при Белом доме. При этом, по версии источников газеты «Вашингтон пост», за этими кибератаками стоят работающие на российское правительство хакеры. Издание не приводит доказательств данных утверждений…». ***(У Лондона нет данных о влиянии на Британию приписываемых хакерам РФ атак на Минторг США // finanzen.net GmbH (https://www.finanz.ru/novosti/aktsii/u-londona-net-dannykh-o-vliyanii-na-britaniyu-pripisyvaemykh-khakeram-rf-atak-na-mintorg-ssha-1029889959). 14.12.2020).***

***

«В среду Европейская комиссия предложила пересмотреть свой закон о сетевой безопасности, а также разработать новую стратегию, направленную на усиление защиты ЕС от нападений и хакерских операций, поддерживаемых государством.

Планы появляются в связи с тем, что Европейский Союз сталкивается с массой кибератак на учреждения, агентства и ключевые отрасли по всему блоку, включая недавний взлом Европейского агентства по лекарственным средствам, которое отвечает за утверждение вакцин против коронавируса.

Рост числа атак во время пандемии коронавируса придал планам срочность, сказал Маргаритис Схинас, вице-президент Комиссии, отвечающий за безопасность.

«Все это указывает на то, что совершенно очевидно: Европа является главной целью», - сказал Шинас репортерам.

Два новых предложенных закона направлены на усиление кибербезопасности для компаний, предоставляющих критически важную инфраструктуру и ключевые секторы, включая энергетику, транспорт, финансовые услуги, облачные технологии, телекоммуникации, аэрокосмическую промышленность, здравоохранение, производство и ИТ-услуги центрального правительства. Поставщики облачных услуг, производители вакцин и услуги видеоконференцсвязи, такие как Zoom, также были добавлены в сферу действия закона.

Во-первых, обновление Директивы блока по сетевой и информационной безопасности (Директива NIS, теперь NIS2) будет налагать новые требования к «основным» и «важным» поставщикам услуг в критических секторах, включая отчетность о кибератаках, реализацию политик безопасности, тщательный анализ безопасности поставщиков и использование технологии шифрования.

Обновление также предоставит национальным властям больше полномочий по обеспечению соблюдения закона. Странам предлагается установить потенциальные штрафы в размере до 2 процентов или 10 миллионов евро, но они могут быть и выше. Власти также смогут временно приостановить деятельность фирмы, не выполняющей требования, и даже вынудить генерального директора временно уйти от исполнения своих обязанностей.

«Важно то, что у директивы есть зубы», - сказал Схинас.

Важные компании также столкнутся с новыми требованиями к безопасности для защиты своей физической инфраструктуры в соответствии с обновленным законом ЕС о критической инфраструктуре - Директивой об устойчивости критических организаций.

Две новые директивы нуждаются в одобрении национальных правительств в Совете ЕС и Европейского парламента.

Эти предложения могут вызвать ожесточенное лоббирование правоприменения, а также отпор со стороны столиц, опасающихся, что это может подорвать их компетенцию в вопросах безопасности. На согласование предыдущей версии Директивы ЕС по ННГ ушло три года.

Национальные органы власти «должны быть усилены и получить надлежащее финансирование и персонал для выполнения своих жизненно важных задач. Наивно вкладывать миллиарды в наши основные предприятия и инфраструктуру, а затем не защищать эти инвестиции от атак», - сказала Дита Чаранзова, Вице-президент Европейского парламента, отвечающий за кибербезопасность.

Киберщит для отражения атак

Комиссия и ее дипломатическая служба также выпустили новую Стратегию кибербезопасности, в которой излагаются новые механизмы для участников отрасли, а также государственных органов и органов безопасности для обмена данными об угрозах и реагировании на инциденты.

Этот так называемый «киберщит» предназначен для более быстрого обнаружения атак и помощи европейским организациям в реагировании и обмене информацией между секторами.

Чтобы оказать влияние, ЕС «должен определить, когда предоставлять нужную информацию, чтобы вовремя изменить ситуацию», - сказала Юлия Шуэце, исследователь из Stiftung Neue Verantwortung в Берлине.

ЕС также предложит новые правила для своих институтов и агентств в следующем году, заявили в нем, чтобы безопасно обмениваться конфиденциальными документами и усилить политику кибербезопасности среди персонала.

В стратегии также излагается план противодействия «ограничениям авторитарных режимов в Интернете» путем упрощения введения санкций в отношении поддерживаемых государством хакерских групп и разработки более строгих международных правил в рамках Организации Объединенных Наций и других международных форумов. Это включает в себя создание «рабочей группы ЕС по кибербразведке» в рамках собственной службы внешней разведки ЕС INTCEN, которая ускорит дипломатический ответ на атаки.

Но некоторые эксперты говорят, что правил может быть недостаточно. «Мы до сих пор не знаем, действительно ли сдерживание является действенной стратегией в киберпространстве и может ли оно быть достигнуто с помощью мер и инструментов, имеющихся в распоряжении ЕС», - сказал Стефан Соэсанто, старший исследователь кибербезопасности в ETH Zurich University.

Прошлым летом блок ввел первый в истории раунд санкций против российских, китайских и северокорейских хакерских групп из-за серьезных инцидентов, связанных с кибербезопасностью. В октябре он ввел санкции в отношении двух российских лиц и разведывательного подразделения за их роль во взломе парламента Германии в 2015 году.

Дипломатическая служба ЕС теперь хочет, чтобы национальные правительства рассмотрели возможность введения санкций в отношении иностранных хакеров квалифицированным большинством голосов, а не единогласным решением, что значительно повысило бы способность блока использовать этот инструмент для сдерживания.

«Сложно найти единодушие в таком деликатном вопросе. Голосование большинством сделает систему санкций ЕС более гибкой», - сказал Лукаш Олейник, исследователь кибербезопасности». ***(LAURENS CERULUS. Europe's gambit to fight off cyberattacks // POLITICO (https://www.politico.eu/article/europe-gambit-fight-off-cyberattacks/). 16.12.2020).***

***

«Система внутренней коммуникации Пентагона SIPRNET была срочно отключена для обновления программного обеспечения утром во вторник после массированной хакерской атакой на правительственные ресурсы.

Издание Washington Post обвинило российскую разведку в причастности к происшествию. В свою очередь МИД РФ данную информацию категорически отрицает.

Сколько еще сервисов подверглось хакерской атаке, пока не уточняется. По мнению издания, целью атаки на правительственную систему была возможность получить доступ к переписке о внешней политики США. Однако журналисты издания не исключают также поиск информации о вакцине против коронавируса.

«SIPRNET» - система взаимосвязанных компьютерных сетей, используемых Министерством обороны США и Госдепартаментом для передачи информации ограниченного распространения, включая ту, что с грифами секретности». ***(Система внутренней коммуникации Пентагона «SIPRNET» взломана хакерами // SecurityLab.ru (https://www.securitylab.ru/news/514894.php). 17.12.2020).***

***

«На прошлой неделе на Литовскую Республику совершили кибератаку.

В ночь на 9 декабря киберпреступники взломали несколько систем управления контентом, чтобы получить доступ к 22 веб-сайтам государственного сектора Литвы. Злоумышленники опубликовали на этих сайтах статьи с ложной информацией.

Среди них была история о польском дипломате, который якобы перевозил наркотики, оружие и деньги. Его будто бы задержали на литовской границе. Эта история также появилась на сайте Государственной пограничной службы.

Другая статья сообщала, что в аэропорту Шяуляй якобы раскрыли случаи коррупции.

Расследование, проведенное Национальным Центром Кибербезопасности, выяснило, что злоумышленники атаковали сайты, которые принадлежали региональным муниципалитетам.

Министр обороны описал ее как «самую сложную» кибератаку на страну за последние годы.

Хакеры запустили спуфинг-кампанию после того, как закончили выкладывать статьи. Это было сделано для того, чтобы распространить информацию.

«Это показывает огромные пробелы в кибербезопасности государственного сектора», - заключил министр обороны». ***(Хакеры взломали государственные сайты Литовской Республики // SecureNews (https://securenews.ru/hackers-broke-into-the-state-websites-of-the-republic-of-lithuania/). 17.12.2020).***

***

«Доля кибератак из Соединенных Штатов на чувствительные объекты России составляет 48-52% от общего числа. Об этом сообщил во вторник, 15 декабря, глава комиссии Совета Федерации по защите госсуверенитета Андрей Климов.

«По нашим оценкам, доля кибератак, осуществляемых из США, по чувствительным объектам РФ достигает как минимум 48–52%», — заявил Климов во время круглого стола в СФ.

Он добавил, что эксперты оценили эту цифру, как две трети от общего числа кибератак. По словам сенатора, в США разработаны механизмы по реализации таких программ.

В конце ноября секретарь Совета безопасности РФ Николай Патрушев рассказал, что спецслужбы США, Украины и других стран пытаются найти уязвимости информационной инфраструктуре на территории Крыма.

Кроме того, он отметил, что иностранные разведки повысили активность в информационной сфере на фоне международной обстановки». ***(В Совфеде назвали долю кибератак из США на чувствительные объекты России // Газета «Известия» (https://iz.ru/1100216/2020-12-15/v-sovfede-nazvali-doliu-kiberatak-iz-ssha-na-chuvstvitelnye-obekty-rossii). 15.12.2020).***

***

«Парламент Финляндии заявил в понедельник, что хакеры получили доступ к его внутренней ИТ-системе и получили доступ к учетным записям электронной почты некоторых членов парламента (депутатов).

Правительственные чиновники заявили, что атака произошла осенью 2020 года и была обнаружена в этом месяце ИТ-персоналом парламента. В настоящее

время это дело расследуется Центральной криминальной полицией Финляндии (KRP).

В официальном заявлении комиссар КРП Теро Муурман сказал, что атака не нанесла никакого ущерба внутренней ИТ-системе парламента, но и не была случайным вторжением.

Муурман сказал, что нарушение безопасности парламента в настоящее время расследуется как инцидент "предполагаемого шпионажа".

«На данном этапе одной из альтернатив является то, что неизвестные факторы смогли получить информацию посредством взлома либо в интересах иностранного государства, либо во вред Финляндии», - сказал Муурман.

«В результате кражи пострадало более одного человека, но, к сожалению, мы не можем назвать точное число, не ставя под угрозу текущее предварительное расследование.

«Это исключительный случай для Финляндии, серьезный из-за качества мишени и неудачный для жертв», - добавил чиновник.

КРП также заявила, что «в расследовании имело место международное сотрудничество», но не предоставила дополнительных деталей.

НОРВЕГИЯ РАСКРЫЛА ПОДОБНЫЙ ИНЦИДЕНТ ОСЕНЬЮ ЭТОГО ГОДА

Но хотя правительственные чиновники не упомянули об этом, инцидент устрашающе похож на аналогичный взлом, раскрытый в соседней скандинавской стране.

Ранее этой осенью парламент Норвегии обнаружил аналогичное нарушение своей внутренней системы электронной почты, когда хакеры получили доступ к учетным записям электронной почты некоторых официальных лиц.

В этом месяце, после многомесячного расследования, норвежская полицейская секретная служба (PST) приписала вторжение APT28, группе хакеров, связанных с российской военной разведкой ГРУ.

В недавнем отчете Microsoft подчеркивается недавняя тенденция в тактике APT28 к нацеливанию на учетные записи электронной почты с помощью набивки учетных данных и атак методом грубой силы». ***(Catalin Cimpanu. Finland says hackers accessed MPs' emails accounts // ZDNet (https://www.zdnet.com/article/finland-says-hackers-accessed-mps-emails-accounts/). 28.12.2020).***

***

«Иранские кибер-акторы, вероятно, стоят за кампанией, поощряющей смертоносное насилие против государственных чиновников США, удостоверяющих результаты выборов 2020 года.

Частью операции было создание веб-сайта, на котором будут размещены личные данные и фотографии государственных чиновников и частных лиц, участвовавших в президентских выборах.

Раскрытие личных данных

Веб-сайт под названием «Враги народа» был создан 6 декабря и к середине месяца включал личные данные (домашние адреса, электронную почту, имена и

фотографии с целью) лиц, которые не поддерживали политику нынешнего президента США. заявления о мошенничестве с избирателями.

В сегодняшнем совместном отчете Федерального бюро расследований (ФБР) и Агентства по кибербезопасности и безопасности инфраструктуры (CISA) говорится, что иранские субъекты «почти наверняка» стоят за созданием веб-сайта (в настоящее время закрытого), основываясь на утверждении «сильно достоверная информация».

Агентства добавляют, что в середине декабря 2020 года на сайте содержались угрозы убийством в адрес сотрудников избирательных комиссий США. Среди них губернаторы, государственные секретари, бывший директор CISA Кристофер Кребс, директор ФБР Кристофер Рэй и люди, работающие в компании Dominion, предоставляющей системы голосования.

Dominion стал мишенью сторонников Трампа после того, как адвокаты президента заявили, что программное обеспечение Dominion переключило голоса за Трампа на Байдена.

ФБР обнаружило несколько учетных записей электронной почты, некоторые из которых были зарегистрированы в службах конфиденциальности, которые использовались для доставки угроз смертью официальным лицам:

врагиofthepeople@tutanota.com

6e.nemiesOfThepeople.e9@protonmail.com

3e.nemiesOfThePeopl.e3@protonmail.com

3e.nemiesOfThePeopl.e3@gmail.com

Предупреждения о попытках Ирана вмешаться в президентские выборы в США в этом году начали поступать в октябре, когда ФБР и CISA опубликовали несколько предупреждений по этой теме [1, 2, 3].

Один из них относится к запугиванию избирателей посредством электронных писем, якобы от ультраправой группы Proud Boys, которые угрожали получателям, зарегистрированным как демократы, насилием, если они не проголосуют за кандидата от республиканцев: «Голосуйте за Трампа или что-то еще», - говорится в строке темы.

Даже при официально подтвержденном результате выборов внешние усилия по подрыву общественного доверия к избирательному процессу и расколу общества продолжаются.

ФБР и CISA призывают общественность проверять источники информации, прежде чем высказывать свое мнение, и искать проверенные новости из заслуживающих доверия публикаций». ***(Ionut Ilascu. FBI: Iran behind pro-Trump 'enemies of the people' doxing site // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fbi-iran-behind-pro-trump-enemies-of-the-people-doxing-site/). 23.12.2020).***

***

«Обраний президент Джо Байден заявив про необхідність модернізації збройних сил США на тлі зростаючих кіберзагроз з боку Росії та Китаю…

"Ми маємо бути здатними впроваджувати інновації та переосмислювати наш захист від зростаючих загроз у нових сферах, таких як кіберпростір", - сказав

Байден на пресконференції після брифінгу представників розвідки і оборони з питань національної безпеки.

За його словами, для вирішення проблем, які становлять для США Росія і Китай, "необхідно модернізувати наші оборонні пріоритети, щоб краще стримувати агресію в майбутньому, а не продовжувати надмірно інвестувати в успадковані системи, призначені для боротьби із загрозами минулого".

Він також зазначив, що нещодавня кібератака проти федеральних відомств становить серйозну загрозу для нацбезпеки США.

"Ми маємо скоротити розрив між тим, де наші можливості зараз, і тим, де вони мають бути, щоб краще стримувати, виявляти, руйнувати і реагувати на такі вторгнення в майбутньому", - додав він». ***(Байден закликав модернізувати оборону США через кіберзагрози з боку Росії та Китаю // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (https://day.kyiv.ua/uk/news/291220-bayden-zaklykav-modernizuvaty-oboronu-ssha-cherez-z-kiberzagrozy-z-boku-rosiyi-ta-kytayu). 29.12.2020).***

***

Кібератака на SolarWinds

«У США двоє сенаторів, республіканець і демократ, незалежно одне від одного виступили з вимогами дати належну відповідь на масовані кібератаки останнього часу на комп'ютерні мережі багатьох урядових органів США, вчинені, за даними американських фахівців із кібербезпеки, російським хакерами.

Сенатор-республіканець Мітт Ромні заявив, що той напад «вимагає відповіді», і варто б очікувати, що то буде «кібервідповідь». Але, за його словами, він не певен, що США мають здатність дати таку відповідь принаймні в такому ж чи й іще більшому масштабі, «як то Росія зробила нам».

Виступаючи на телеканалі NBC, Ромні також сказав, що розчарований реакцією на цей кібернапад чинного президента Дональда Трампа – який, всупереч наявній інформації, публічно висловив сумніви в тяжкості цього кібернападу і в тому, що його здійснила Росія.

За словами сенатора, Трамп «раптово сліпне, коли йдеться про Росію», і не хоче визнавати, що Росія – «надзвичайно поганий актор на світовій сцені».

Як сказав Ромні, американські фахівці з кібербезпеки визначили, що напад був здійснений із Росії і був дуже серйозний і шкідливий: хакери дісталися, серед іншого, до мереж органу, відповідального за ядерні можливості США і за розробки в галузі ядерної зброї.

Сенатор-демократ Марк Ворнер, зі свого боку, сказав на телеканалі ABC, що кібернапад, можливо, ще триває і що його повний масштаб іще не визначили.

Як сказав Ворнер, чільний представник демократів в комітеті Сенату у справах розвідки, Вашингтон мав би чітко дати знати противникам, «що, якщо ви йдете на такі дії, ми й інші завдамо удару у відповідь».

Обраний президент Джо Байден, як заявив майбутній голова його апарату Білого дому Рон Клайн, зараз обмірковує, яку дати відповідь на цей кібернапад.

«Ідеться не тільки про санкції, а й про інші кроки й заходи, які ми можемо здійснити, щоб знизити здатність іноземних сил здійснювати такі напади», – сказав він.

Але Клайн попередив в інтерв'ю телеканалові CBS, що наразі лишається без відповіді ще багато питань про мету, природу і обсяг цих останніх нападів.

Попереднього дня, 19 грудня, Трамп уперше відреагував на ці кібернапади, висловивши в твітері сумніви в їхній тяжкості і в тому, що їх здійснила Росія. За словами Трампа, серйозність нападів була «значно більшою в «фейкових новинах», ніж насправді», і що їх міг здійснити Китай.

Ці заяви суперечили повідомленню державного секретаря Майка Помпео, який 18 грудня сказав в інтерв'ю, що США «можуть сказати цілком чітко»: кібернапад вчинили росіяни.

Кремль заперечує свою причетність.

Про цей кібернапад уперше стало відомо 13 грудня. Уже тоді виникли серйозні підозри, що це зробили російські хакери. Посольство Росії у США вже 14 грудня заявило, що Москва «не здійснює наступальних операцій у кіберпросторі».

Як повідомляла компанія Microsoft, ця атака вразила понад 40 великих комп'ютерних мереж, із яких близько 80 відсотків перебувають у США, інші потерпілі – в Бельгії, Великій Британії, Ізраїлі, Іспанії, Канаді, Мексиці й ОАЕ. Серед потерпілих були кілька американських урядових установ. Офіційно їх не називали, але засоби інформації писали з посиланням на неназвані обізнані джерела, що йдеться, серед інших, про міністерства внутрішньої безпеки, фінансів чи торгівлі.

17 грудня Міністерство енергетики США підтвердило, що воно є серед уражених. У складі цього міністерства діє орган, відповідальний за ядерні арсенали США.

Також потерпіли й комерційні компанії.

18 грудня Федеральне бюро розслідувань та інші органи, які розслідували кібернапад, доповіли про результати в Конгресі.

Кібератака полягала в тому, що зловмисники змогли вставити шкідливий код в оновлення програмового забезпечення, які розповсюджувала в період березня – червня американська компанія SolarWinds для своєї системи управління комп'ютерними мережами, якою користуються десятки тисяч клієнтів – і державних, і комерційних. Це дало хакерам доступ і до тих комп'ютерних мереж, у яких були встановлені ці оновлення». ***(У США вимагають відповіді на кібератаку, в якій звинувачують російських хакерів // Радіо Свобода (https://www.radiosvoboda.org/a/news-ssha-kibernapad/31010477.html). 20.12.2020).***

***

«По данным Reuters, в минувшие выходные появились новости о том, что иностранные хакеры в течение нескольких месяцев тайно отслеживали учетные записи электронной почты и обмены сообщениями между Министерством финансов США и Национальным управлением по телекоммуникациям и информации. В отчете говорится, что злоумышленники проникли через вредоносный код в ИТ-продукт под названием SolarWinds, который

позволил им получить доступ к сети, которую они затем использовали для взлома почтового клиента Microsoft.

Microsoft выпустила руководство о том, как организации могут усилить безопасность, чтобы попытаться избежать этих атак, и заявила, что не выявила никаких уязвимостей продуктов Microsoft. Возможно, вы мало что сможете сделать с уязвимостью SolarWinds. Но если вы получаете свою рабочую или личную электронную почту через Outlook в Microsoft 365, есть также способы лучше защитить свою индивидуальную учетную запись, чтобы избежать взлома. (Если вы используете Windows 10, есть также несколько настроек безопасности по умолчанию, которые вы можете изменить, чтобы лучше защитить свое устройство.)

Вот пять способов защитить вашу учетную запись Microsoft.

1. Настройте многофакторную аутентификацию…
2. Защитите свой пароль…
3. Избегайте фишинговых атак…
4. Защитите свои приложения…
5. Упростите восстановление аккаунта…» ***(Alison DeNisco Rayome. 5 ways to lock down your Microsoft 365 account and keep hackers out // CNET (https://www.cnet.com/how-to/5-ways-to-lock-down-your-microsoft-365-account-and-keep-hackers-out/). 17.12.2020).***

***

«Агентство национальной безопасности США опубликовало в четверг рекомендацию по безопасности, в которой содержится предупреждение о двух методах, которые хакеры используют для расширения доступа из скомпрометированных локальных сетей в облачную инфраструктуру.

Эта рекомендация последовала за массовым взломом цепочки поставок SolarWinds, поразившим несколько правительственных агентств США, охранную фирму FireEye и совсем недавно Microsoft.

Хотя АНБ специально не упоминает о взломе SolarWinds в своих рекомендациях, оба метода, описанные в документе, также были замечены хакерами SolarWinds для расширения доступа к облачным ресурсам после первоначального получения доступа к локальным сетям через троянизированное приложение SolarWinds Orion. - согласно рекомендациям FireEye, Microsoft и CISA (Агентство по кибербезопасности и безопасности инфраструктуры США).

Чтобы не искажать сообщение АНБ, мы процитируем подробности об этих двух методах непосредственно из справки агентства:

«В первом [методе] субъекты взламывают локальные компоненты инфраструктуры федеративного единого входа и крадут учетные данные или закрытый ключ, который используется для подписи токенов языка разметки утверждений безопасности (SAML). Используя закрытые ключи, субъекты затем подделывают доверенные токены аутентификации для доступа к облачным ресурсам. [...]

В варианте первого TTP, если злоумышленники не могут получить ключ подписи вне помещения, они попытаются получить достаточные

административные привилегии в облачном клиенте, чтобы добавить злонамеренные отношения доверия с сертификатом для подделки токенов SAML.

Во втором TTP субъекты используют скомпрометированную учетную запись глобального администратора для назначения учетных данных субъектам служб облачных приложений (удостоверения для облачных приложений, которые позволяют запускать приложения для доступа к другим облачным ресурсам). Затем субъекты вызывают учетные данные приложения для автоматического доступа к облачным ресурсам (часто, в частности, к электронной почте), которые в противном случае были бы затруднены для субъектов или были бы более легко замечены как подозрительные».

АНБ отмечает, что ни один из этих методов не является новым и оба используются по крайней мере с 2017 года обеими группами национальных государств, а также другими типами субъектов угроз.

Кроме того, АНБ добавляет, что ни один из этих двух методов не использует уязвимости в продуктах федеративной аутентификации, а скорее злоупотребляет законными функциями после компрометации локальной сети или учетной записи администратора.

Агентство безопасности США заявляет, что есть контрмеры, которые компании могут принять, чтобы, по крайней мере, обнаружить, когда злоумышленник злоупотребляет этими механизмами, и быстрее отреагировать на нарушение.

Эти меры, сгруппированные по нескольким категориям, подробно описаны в рекомендации АНБ, доступной для загрузки в виде PDF-документа.

Агентство национальной безопасности также заявило, что даже если рекомендации и меры по снижению риска сосредоточены вокруг Microsoft Azure, «многие из методов можно распространить и на другие среды». ***(Catalin Cimpanu. NSA warns of federated login abuse for local-to-cloud attacks // ZDNet (https://www.zdnet.com/article/nsa-warns-of-federated-login-abuse-for-local-to-cloud-attacks/). 18.12.2020).***

***

«Размер и масштабы SolarWinds как поставщика программного обеспечения для ИТ, а также характер взлома, о котором было объявлено 13 декабря, потрясли мир ИТ и безопасности. В то время как руководители служб безопасности направляют свои компании ответные меры, для мира поставщиков есть несколько общих советов по этому поводу.

Злоумышленники продолжают использовать недостатки безопасности продукта

На протяжении 2020 года сбои в безопасности продуктов происходили месяц за месяцем, но большинство из них касалось продуктов и услуг, ориентированных на потребителя. Вендоры корпоративного B2B не получили такого внимания, но масштаб уравновешивался прорывом SolarWinds.

Компании, конкурирующие с SolarWinds за предоставление важных продуктов для инфраструктуры, мониторинга и безопасности, а также поставщиков средств обеспечения безопасности, должны сосредоточиться на следующем:

Плохие меры по обеспечению безопасности продукта создают риск для компаний B2B доли рынка. Forrester проводит множество исследований в области безопасности продуктов, в которых содержатся подробные рекомендации по реализации или совершенствованию инициатив по обеспечению безопасности продуктов. Ожидайте, что это станет основным направлением деятельности отделов закупок и юристов в результате этого нарушения.

Продавцы НЕ должны использовать взлом SolarWinds как маркетинговую возможность. Попытки использовать чужие неудачи никогда не помогают компании хорошо выглядеть, и в индустрии кибербезопасности все знают, что сегодня это могут быть они, а завтра - вы. Преследование, окунуться в воду или пристыдить жертву - это не просто дурной вкус. Это прискорбно и клиентов не привлечет. FireEye продемонстрировал потрясающую прозрачность в результате своего нарушения и смог также предоставить одну из первых подробных технических описаний инцидента с SolarWinds.

Даже поставщик программного обеспечения с развитой системой безопасности мог этого не заметить. Для выявления недостатков безопасности в своей цепочке поставок ведущие компании-разработчики программного обеспечения регулярно проводят анализ состава программного обеспечения для выявления уязвимостей в компонентах с открытым исходным кодом и используют сертификаты для подписи кода, чтобы гарантировать целостность поставляемого кода. Ни один из подходов не обнаружил бы эту атаку - вредоносного кода не было в библиотеке с открытым исходным кодом, а скомпрометированная DLL (библиотека динамической компоновки) была подписана действующим (хотя и скомпрометированным) сертификатом. Не приравнивайте восприимчивость к отсутствию зрелости в плане безопасности.

Возможно, необходимо изменить степень прозрачности SolarWinds в отношении списка клиентов. SolarWinds был достаточно большим и достаточно заметным, чтобы быть привлекательной целью для злоумышленников, даже не упоминая имена клиентов. Но на странице клиента на его веб-сайте были перечислены все пять подразделений вооруженных сил США, все 10 крупных американских телекоммуникационных компаний и пять ведущих бухгалтерских фирм в качестве клиентов. Это не означает, что какая-либо из этих организаций попала в ловушку взлома, но это означает, что злоумышленники имеют некоторое представление о ценности SolarWinds как цели в случае успеха. Управление рисками третьих сторон, юридические вопросы и закупки, вероятно, вынудят руководителей по информационной безопасности провести переоценку, если они захотят попасть в листинг в будущем». ***(Jeff Pollard. The SolarWinds and US government breach is not a marketing opportunity // ZDNet (https://www.zdnet.com/article/the-solarwinds-and-us-government-breach-is-not-a-marketing-opportunity/). 16.12.2020).***

***

«Несколько исследователей безопасности и исследовательские группы опубликовали на выходных списки от 100 до 280 организаций, которые

установили троянизированную версию платформы SolarWinds Orion и заразили свои внутренние системы вредоносным ПО Sunburst.

В список включены названия технологических компаний, местных органов власти, университетов, больниц, банков и операторов связи.

Самые известные имена в этом списке включают Cisco, SAP, Intel, Cox Communications, Deloitte, Nvidia, Fujitsu, Belkin, Amerisafe, Lukoil, Rakuten, Check Point, Optimizely, Digital Reach и Digital Sense.

Предполагается, что пострадала и MediaTek, одна из крупнейших в мире компаний, производящих полупроводники; хотя исследователи безопасности еще не на 100% включили его в свои списки.

РАСКРЫТИЕ ТАЙН ПОДОБЛАСТИ SUNBURST

Эти списки составляли исследователи безопасности путем обратного проектирования вредоносного ПО Sunburst (также известного как Solorigate).

…это вредоносное ПО было внедрено в обновления для приложения SolarWinds Orion, выпущенных в период с марта по июнь 2020 года.

В результате заминированных обновлений вредоносное ПО Sunburst было внедрено глубоко во внутренние сети многих компаний и государственных организаций, которые использовали приложение Orion для мониторинга и инвентаризации внутренних ИТ-систем.

Согласно подробным отчетам, опубликованным на прошлой неделе Microsoft, FireEye, McAfee, Symantec, Kaspersky и US Cybersecurity and Infrastructure Security Agency (CISA), на зараженных системах вредоносная программа собирала информацию о сети компании-жертвы, подождите 12-14. дней, а затем отправьте данные на удаленный сервер управления и контроля (C&C).

Затем хакеры, которые, как считается, были спонсируемой российским государством группой, анализировали полученные данные и наращивали атаки только на те сети, которые представляли интерес для их целей сбора разведданных.

На прошлой неделе компания SolarWinds признала факт взлома и сообщила, что на основании внутренней телеметрии почти 18 000 из 300 000 ее клиентов загрузили версии платформы Orion, содержащие вредоносное ПО Sunburst.

Первоначально предполагалось, что только SolarWinds сможет идентифицировать и уведомить все затронутые организации. Однако по мере того, как исследователи безопасности продолжали анализировать внутреннюю работу Sunburst, они также обнаружили некоторые причуды в работе вредоносной программы, а именно в том, как вредоносная программа пингует свой командный сервер.

Согласно исследованию, опубликованному на прошлой неделе, Sunburst отправлял собранные данные из зараженной сети на URL-адрес C&C сервера, уникальный для каждой жертвы.

Этот уникальный URL-адрес был поддоменом для avsvmcloud [.] Com и состоял из четырех частей, первая из которых представляла собой строку произвольного вида. Но исследователи безопасности заявили, что эта строка на самом деле не была уникальной, а содержала закодированное имя домена локальной сети жертвы.

С прошлой недели несколько фирм по безопасности и независимых исследователей проанализировали исторический веб-трафик и данные пассивного DNS, чтобы собрать информацию о трафике, идущем в домен avsvmcloud [.] Com, взломать поддомены, а затем отследить компании, которые установили троянизированный SolarWinds Orion app - и вредоносная программа Sunburst отправлялась из их сетей обратно на сервер злоумышленников (теперь он затонул благодаря Microsoft и FireEye).

РАСТУЩИЙ СПИСОК ЖЕРТВ ПЕРВОГО И ВТОРОГО ЭТАПОВ

Фирмы по кибербезопасности TrueSec и Prevasio, исследователь безопасности Деван Чоудхури и китайская фирма по безопасности QiAnXin - одни из немногих, кто опубликовал списки зараженных Sunburst организаций или инструментов для декодирования поддоменов avsvmcloud [.] Com.

Такие компании, как Cisco и Intel, официально подтвердили, что заразились, в интервью журналистам в минувшие выходные. Обе компании заявили, что не нашли доказательств того, что хакеры расширили доступ для доставки полезной нагрузки второго уровня в свои системы.

VMWare и Microsoft, чьи имена не фигурировали в этих общедоступных списках, также подтвердили, что они установили троянизированные обновления Orion во внутренних сетях, но также указали, что они также не обнаружили никаких доказательств эскалации атак со стороны злоумышленников.

Однако хакеры активизировали атаки на сети некоторых из своих целей. В интервью в пятницу генеральный директор FireEye Кевин Мандиа, чья компания обнаружила взлом SolarWinds при расследовании взлома своих внутренних систем, сказал, что хакеры, несмотря на заражение почти 18000 сетей, увеличили доступ только к примерно 50 целям, основываясь на видимости FireEye.

В отдельном отчете, также опубликованном в пятницу, Microsoft также сообщила, что выявила 40 своих клиентов, которые установили зараженные приложения Orion и к которым злоумышленники расширили доступ.

«Эскалация» обычно происходила, когда командный сервер avsvmcloud [.] Com отвечал зараженной компании очень специфическим ответом DNS, который содержал специальное поле CNAME.

Это специальное поле DNS CNAME содержало расположение второго C&C сервера, с которого вредоносная программа Sunburst могла бы получать дополнительные команды и иногда загружать другие вредоносные программы.

В настоящее время единственной публично известной компанией, к которой хакеры расширили доступ, является FireEye, чья реакция на взлом помогла раскрыть весь взлом SolarWinds.

Различие между ними (простое заражение Sunburst и эскалация) имеет решающее значение для реагирующих на инциденты. В первом случае им может потребоваться только удалить вредоносное ПО Sunburst, а во втором им может потребоваться просмотреть журналы, чтобы определить, к каким внутренним системам хакеры расширили доступ и какие данные были украдены из их сетей.

…большая часть сообщества кибербезопасности в настоящее время работает с сетями доставки контента, поставщиками интернет-услуг и другими интернет-компаниями для сбора пассивных данных DNS и отслеживания трафика в домен

avsvmcloud [.] Com и из него. для выявления других жертв, к которым злоумышленники увеличили доступ…» ***(Catalin Cimpanu. Partial lists of organizations infected with Sunburst malware released online // ZDNet (https://www.zdnet.com/article/partial-lists-of-organizations-infected-with-sunburst-malware-released-online/). 21.12.2020).***

***

«По мере того, как после атаки на цепочку поставок SolarWinds постепенно выявляются свидетельства криминалистики, исследователи в области безопасности обнаружили второго злоумышленника, который использовал программное обеспечение SolarWinds для размещения вредоносного ПО в корпоративных и государственных сетях.

Подробностей об этом втором субъекте угрозы по-прежнему мало, но исследователи безопасности не верят, что эта вторая сущность связана с предполагаемыми хакерами, поддерживаемыми российским правительством, которые взломали SolarWinds для внедрения вредоносного ПО в его официальное приложение Orion.

Вредоносная программа, использованная в исходной атаке, под кодовым названием Sunburst (или Solorigate), была доставлена клиентам SolarWinds в качестве заминированного обновления для приложения Orion.

В зараженных сетях вредоносная программа пингует своих создателей, а затем загружает троян-бэкдор второго этапа под названием Teardrop, который позволяет злоумышленникам запускать сеанс с использованием клавиатуры, также известный как атака, управляемая человеком.

Но в первые несколько дней после публичного раскрытия информации о взломе SolarWinds в первоначальных отчетах упоминались две полезные нагрузки второго уровня.

В отчетах Guidepoint, Symantec и Palo Alto Networks подробно описано, как злоумышленники внедряли веб-оболочку .NET под названием Supernova.

Исследователи безопасности полагали, что злоумышленники использовали веб-оболочку Supernova для загрузки, компиляции и выполнения вредоносного сценария Powershell (который некоторые назвали CosmicGale).

Однако в ходе последующего анализа, проведенного группами безопасности Microsoft, теперь выяснилось, что веб-оболочка Supernova не была частью исходной цепочки атак.

Компании, обнаружившие Supernova на своих установках SolarWinds, должны рассматривать этот инцидент как отдельную атаку.

Согласно сообщению на GitHub аналитика безопасности Microsoft Ника Каппа, веб-оболочка Supernova, по-видимому, установлена на установках SolarWinds Orion, которые остались открытыми в сети и были скомпрометированы с помощью эксплойтов, аналогичных уязвимости, отслеживаемой как CVE-2019-8917.

Путаница в том, что Supernova была связана с цепочкой атак Sunburst + Teardrop, возникла из-за того, что, как и Sunburst, Supernova была замаскирована под DLL для приложения Orion - Sunburst был скрыт внутри файла

SolarWinds.Orion.Core.BusinessLayer.dll и Supernova внутри App_Web_logoimagehandler.ashx.b6031896.dll.

Но в анализе, опубликованном поздно вечером в пятницу, 18 декабря, Microsoft заявила, что в отличие от Sunburst DLL, Supernova DLL не была подписана легитимным цифровым сертификатом SolarWinds.

Тот факт, что Supernova не был подписан, был сочтен крайне нехарактерным для злоумышленников, которые до этого времени проявляли очень высокую степень изощренности и внимания к деталям в своей работе.

Сюда входило проведение месяцев незамеченными во внутренней сети SolarWinds, добавление фиктивного буферного кода в приложение Orion, заранее замаскированное добавлением вредоносного кода позже, и маскировка своего вредоносного кода, чтобы он выглядел так, как будто разработчики SolarWinds написали его сами.

Все это выглядело слишком вопиющей ошибкой, которую бы не совершили первоначальные злоумышленники, и, как следствие, Microsoft считает, что это вредоносное ПО не имеет отношения к исходной атаке цепочки поставок SolarWinds». ***(Catalin Cimpanu. A second hacking group has targeted SolarWinds systems // ZDNet (https://www.zdnet.com/article/a-second-hacking-group-has-targeted-solarwinds-systems/). 21.12.2020).***

***

«По мере того как последствия недавней кибератаки SolarWinds продолжают проявляться, метод атаки становится все более ясным: согласно нескольким сообщениям, злоумышленники использовали обновления вредоносного троянского программного обеспечения для решения мониторинга ИТ SolarWinds Orion, подписанного действительными цифровыми подписями, для получения доступа к сети. Этот доступ позволил им повысить свои привилегии. Точка доступа могла быть результатом человеческой ошибки, когда учетные данные с паролем предоставляли доступ к FTP-сайту SolarWinds, размещенному на GitHub. Это дало бы хакерам все необходимое для загрузки вредоносного EXE-файла в экосистему SolarWinds.

Вероятно, единственной самой большой превентивной мерой в этой конкретной атаке была бы защита криптографического ключа, используемого для подписи кода, для обеспечения безопасности на протяжении всего процесса подписания. Это защитило бы целостность программного обеспечения - гарантируя, что будет подписан только код, который должен был быть подписан - и не допустил бы злоумышленников. Если процесс подписания был нарушен, тогда приоритетом стало бы выявление нарушения как можно быстрее, чтобы ограничить ущерб.

Давайте рассмотрим некоторые другие передовые методы безопасности, чтобы снизить риск атаки типа SolarWinds.

Принять подход «нулевого доверия» - никогда не доверять, всегда проверять, что кто-то - или что-то - это то, кем они являются, с высокой степенью уверенности, многофакторной аутентификацией, которая использует интеллектуальные аутентификаторы, такие как поведенческая биометрия,

мобильные интеллектуальные учетные данные и программные токены. Кроме того, применяйте принципы доступа с наименьшими привилегиями, чтобы любой пользователь, программа или процесс имел только абсолютный минимум привилегий для выполнения своей конкретной функции.

Возьмите свою рабочую силу без пароля - в то время как надежные пароли с регулярным сроком действия хороши, доступ без пароля на основе учетных данных намного лучше, что эффективно устраняет взлом паролей. Цифровой сертификат, предоставленный мобильному телефону сотрудника, преобразует его в его надежную идентификационную информацию на рабочем месте, обеспечивая безопасный доступ к корпоративным ресурсам, когда устройство разблокировано с помощью биометрических данных человека.

Используйте адаптивную аутентификацию на основе рисков с механизмом политик - это ваша система раннего обнаружения и предотвращения угроз. Контекстные данные, такие как репутация устройства, поведение пользователей и скорость, предупреждают о подозрительной активности, которую вы затем можете решить с помощью дополнительных задач аутентификации или решения полностью заблокировать определенные действия.

Разработайте корпоративную стратегию сертификатов - защищайте сетевые соединения, управляйте программным обеспечением / микропрограммным обеспечением, аутентифицируйте устройства, защищайте электронную почту, шифруйте и подписывайте данные и защищайте идентификационные данные пользователей. Благодаря корпоративной PKI для выдачи и ротации учетных данных и системе управления идентификационной информацией учетные данные в случае взлома индивидуальных учетных данных сокращаются время простоя и уязвимости.

Используйте аппаратные модули безопасности (HSM) для надежного корня доверия- защищать криптографические ключи и управлять ими на протяжении всего их жизненного цикла. Криптографические ключи необходимы для подписи и проверки сертификатов устройств для идентификации и авторизации, шифрования / дешифрования и хеширования данных для обеспечения их конфиденциальности и целостности, а также для подписи кода для защиты его целостности. HSM обеспечивают безопасную среду для защиты ключей как при использовании, так и в состоянии покоя и предлагают надежные механизмы авторизации, чтобы гарантировать, что ни одно отдельное лицо или объект не сможет нарушить политику, установленную для использования ключей. HSM - это защищенные от несанкционированного доступа устройства, сертифицированные по самым высоким стандартам безопасности, включая FIPS 140-2 уровня 3 и Common Criteria EAL 4+. Большинство организаций, заботящихся о безопасности, сегодня развертывают HSM для защиты критически важной бизнес-информации и приложений.

Применяйте строгие меры контроля политик с регулярным аудитом - организациям необходимо управлять своими криптографическими ключами и учетными данными на протяжении всего жизненного цикла, ограничивая их использование и регулярно меняя их. Аудит практики управления, соблюдение политик и усиление двойного контроля там, где это возможно, помогут

распространить передовой опыт. Кроме того, регулярный аудит или проверка работоспособности вашей среды безопасности - от используемой криптографии до политик и процедур - может выявить пробелы или риски и помочь в раннем выявлении нарушений…» ***(Jenn Markey, Iain Beveridge. Protect your organization from a SolarWinds-type attack // Entrust Corporation (https://blog.entrust.com/2020/12/protect-your-organization-from-a-solarwinds-type-attack/). 17.12.2020).***

***

«Как сообщила во вторник компания, занимающаяся разработкой программного обеспечения в области ИТ, SolarWinds, никаких других продуктов, содержащих вредоносный код, подобный тому, который был обнаружен в платформе Orion, не обнаружено.

Утверждение компании появилось после того, как она провела внутренний аудит всех своих приложений после того, как в воскресенье появилась новость о том, что российские хакеры, спонсируемые государством, взломали ее внутреннюю сеть и внедрили вредоносное ПО в Orion, платформу мониторинга и инвентаризации сети.

Вредоносная программа под названием SUNBURST (или Solorigate) была вставлена в приложения Orion версий с 2019.4 по 2020.2.1, выпущенные в период с марта 2020 года по июнь 2020 года.

«Мы просканировали код всех наших программных продуктов на наличие маркеров, подобных тем, которые использовались при атаке на наши продукты платформы Orion, указанные выше, и мы не обнаружили никаких доказательств того, что другие версии наших продуктов платформы Orion или другие наши продукты содержат эти маркеры, "заявила сегодня компания.

«Мы также не нашли доказательств того, что наши продукты SolarWinds MSP, включая RMM и N-central, а также любые из наших бесплатных инструментов или агентов содержат упомянутые выше маркеры», - добавлено в обновлении к рекомендации по безопасности, первоначально опубликованной в воскресенье.

Но хотя компания SolarWinds была довольна тем, что вредоносная программа не попала в другие продукты, того факта, что она попала в Orion, одно из самых популярных предложений, было более чем достаточно.

В документах SEC в понедельник SolarWinds сообщила, что из 300 000 ее клиентов более 33 000 использовали платформу Orion и около 18 000 загрузили версии с вредоносным ПО.

Однако хакеры не потрудились получить доступ к сетям всех этих компаний; вместо этого ограничиваются только взломом нескольких выбранных целей. На момент написания список известных жертв, взломанных с использованием платформы Orion в качестве точки входа, включает:

Американская компания по кибербезопасности FireEye

Министерство финансов США

Национальное управление по телекоммуникациям и информации Министерства торговли США (NTIA)

Национальные институты здоровья Министерства здравоохранения (NIH)
Агентство кибербезопасности и инфраструктуры (CISA)
Министерство внутренней безопасности (DHS)
Государственный департамент США
СЕГОДНЯ ВЫПУЩЕНО НОВОЕ ОБНОВЛЕНИЕ ORION ДЛЯ УДАЛЕНИЯ ВРЕДОНОСНЫХ КОМПОНЕНТОВ

В настоящее время SolarWinds находится в режиме контроля повреждений и пытается ограничить масштабы взлома. С прошлой недели компания работала над созданием нового обновления приложения Orion, которое удаляет любые следы вредоносного ПО из зараженных систем.

Хотя хакеры перестали вставлять свое вредоносное ПО в двоичные файлы Orion с июня, и последующие обновления Orion были чистыми, части вредоносного ПО SUNBURST оставались в зараженных системах и могли быть использованы для будущих атак.

Этот риск также был снижен сегодня, когда Microsoft и коалиция технических и государственных партнеров вмешались, чтобы захватить сервер управления и контроля вредоносного ПО.

SolarWinds теперь просит клиентов выполнить обновление до версий 2019.4 HF 6 и 2020.2.1 HF 2, чтобы заменить вредоносные компоненты Orion на чистые версии и устранить любую угрозу.

Этот шаг был сделан как раз вовремя, поскольку Microsoft также объявила о планах поместить известные вредоносные двоичные файлы приложений Orion в карантин, начиная с завтрашнего дня, в среду, 16 декабря, что, скорее всего, привело бы к неожиданным сбоям для пользователей приложения Orion». ***(Catalin Cimpanu. SolarWinds said no other products were compromised in recent hack // ZDNet (https://www.zdnet.com/article/solarwinds-said-no-other-products-were-compromised-in-recent-hack/). 16.12.2020).***

***

«Российская спецслужба проводит изощренную кампанию по вредоносному ПО, поражая несколько федеральных агентств США и частные компании, включая Microsoft, согласно сообщениям Государственного департамента, новостным сообщениям и анализу охранных компаний. Массовое нарушение, которое, как сообщается, включало систему электронной почты, используемую высшим руководством Казначейства, началось в начале этого года, когда хакеры взломали программное обеспечение, созданное фирмой SolarWinds, занимающейся программным обеспечением для ИТ.

Взломанная компания продает программное обеспечение, которое позволяет организации видеть, что происходит в ее компьютерных сетях. Хакеры вставили вредоносный код в обновленную версию программного обеспечения под названием Orion. По данным компании, около 18 000 клиентов SolarWinds установили испорченные обновления в свои системы. Скомпрометированный процесс обновления имел широкий эффект, масштабы которого продолжают расти по мере появления новой информации.

На выходных президент Дональд Трамп высказал в Твиттере идею о том, что за атакой может стоять Китай. Трамп, который не представил доказательств в поддержку предположения о причастности Китая, отметил госсекретаря Майка Помпео, который ранее сказал в радиоинтервью, что «мы можем довольно четко сказать, что именно русские участвовали в этой деятельности».

В совместном заявлении агентства национальной безопасности США назвали нарушение «значительным и продолжающимся». До сих пор неясно, сколько агентств затронуто или какую информацию могли украсть хакеры, но, судя по всему, вредоносное ПО чрезвычайно мощно. Согласно анализу Microsoft и компании FireEye, которые были заражены, вредоносная программа дает хакерам широкий доступ к уязвимым системам.

Microsoft заявила, что выявила более 40 клиентов, ставших целью взлома. Вероятно, появится больше информации о взломе и его последствиях. Вот что вам нужно знать о взломе SolarWinds:

Как хакеры внедрили вредоносное ПО в обновление программного обеспечения?

Хакерам удалось получить доступ к системе, которую SolarWinds использует для сбора обновлений своего продукта Orion, пояснила компания в заявлении в SEC. Оттуда они вставляли вредоносный код в легитимные обновления программного обеспечения. Это известно, как атака цепочки поставок, потому что она заражает программное обеспечение во время его сборки.

Для хакеров это большая удача, чтобы осуществить атаку на цепочку поставок, потому что она помещает их вредоносное ПО в надежную часть программного обеспечения. Вместо того, чтобы обманывать отдельные цели для загрузки вредоносного ПО с помощью фишинговой кампании, хакеры могли полагаться на несколько правительственных агентств и компаний для установки обновления Orion по запросу SolarWinds.

Этот подход особенно эффективен в данном случае, поскольку, как сообщается, тысячи компаний и государственных учреждений по всему миру используют программное обеспечение Orion. С выпуском испорченного обновления программного обеспечения обширный список клиентов SolarWinds стал потенциальной целью взлома.

Какие госструктуры были заражены вредоносным ПО?

Согласно сообщениям Reuters, The Washington Post и The Wall Street Journal, вредоносная программа затронула министерства внутренней безопасности, штата, торговли и казначейства США, а также Национальные институты здравоохранения. В четверг Politico сообщило, что ядерные программы Министерства энергетики США и Национального управления ядерной безопасности также стали мишенью.

До сих пор неясно, какая информация была украдена у федеральных агентств, если таковая была, но объем доступа, похоже, широк.

Хотя Министерство энергетики и Министерство торговли признали факт взлома источников новостей, нет официального подтверждения того, что другие конкретные федеральные агентства были взломаны. Тем не менее, Агентство по кибербезопасности и безопасности инфраструктуры США выпустило рекомендацию, призывающую федеральные агентства смягчить воздействие

вредоносного ПО, отметив, что оно «в настоящее время используется злоумышленниками».

В своем заявлении в четверг избранный президент Джо Байден заявил, что его администрация «сделает устранение этого нарушения главным приоритетом с момента нашего вступления в должность».

Почему взлом так важен?

Помимо получения доступа к нескольким правительственным системам, хакеры превратили обычное обновление программного обеспечения в оружие. Это оружие было нацелено на тысячи групп, а не только на агентства и компании, на которых сосредоточились хакеры после установки испорченного обновления Orion.

Президент Microsoft Брэд Смит назвал это « актом безрассудства » в обширном сообщении в блоге, в котором исследуются последствия взлома. Он не приписал взлом напрямую России, но назвал предыдущие предполагаемые хакерские кампании доказательством обострения кибер-конфликта.

«Это не просто атака на конкретные цели, - сказал Смит, - но на доверие и надежность критически важной мировой инфраструктуры с целью продвижения разведывательной службы одной страны». Далее он призвал к международным соглашениям, ограничивающим создание хакерских инструментов, которые подрывают глобальную кибербезопасность.

Бывший руководитель службы кибербезопасности Facebook Алекс Стамос сказал в Twitter, что взлом может привести к тому, что атаки на цепочки поставок станут более распространенными. Однако он сомневается, что взлом был чем-то необычным для хорошо обеспеченной спецслужбой.

«До сих пор вся деятельность, которая публично обсуждалась, не выходила за рамки того, что США делают регулярно», - сказал Стамос.

Были ли заражены вредоносным ПО частные компании или другие правительства?

Да. В четверг Microsoft подтвердила, что обнаружила индикаторы вредоносного ПО в своих системах, после того, как несколько дней назад подтвердила, что нарушение затрагивает ее клиентов. В сообщении Reuters также говорится, что собственные системы Microsoft использовались для поддержки хакерской кампании, но Microsoft опровергла это утверждение информационным агентствам. В среду компания начала помещать в карантин версии Orion, которые, как известно, содержат вредоносное ПО, чтобы отрезать хакерам доступ к системам своих клиентов.

FireEye также подтвердил на прошлой неделе, что он был заражен вредоносным ПО и обнаружил заражение в клиентских системах.

В понедельник The Wall Street Journal сообщила, что обнаружила по крайней мере 24 компании, которые установили вредоносное ПО. По данным журнала, в их число входят технологические компании Cisco, Intel, Nvidia, VMware и Belkin. Сообщается, что у хакеров также был доступ к Департаменту государственных больниц Калифорнии и Государственному университету Кента.

Неясно, кто из других клиентов SolarWinds из частного сектора был заражен вредоносным ПО. В список клиентов компании входят крупные корпорации, такие как AT&T, Procter & Gamble и McDonald's. Компания также считает в качестве

клиентов правительства и частные компании по всему миру. FireEye сообщает, что многие из этих клиентов были заражены.

Что мы знаем о причастности России к взлому?

Помпео в пятницу приписал взлом России. Это произошло после того, как в течение недели новостные агентства сообщили, что правительственные чиновники заявили, что за кампанию по вредоносному ПО несет ответственность хакерская группа, предположительно российская спецслужба. SolarWinds и фирмы, занимающиеся кибербезопасностью, приписывают взлом "субъектов национального государства", но не назвали страну напрямую.

В заявлении на Facebook посольство России в США отрицает ответственность за хакерскую кампанию SolarWinds. «Злонамеренная деятельность в информационном пространстве противоречит принципам российской внешней политики, национальным интересам и нашему пониманию межгосударственных отношений», - заявили в посольстве, добавив, что «Россия не ведет наступательных операций в киберпространстве».

Хакерскую группу, получившую прозвище APT29 или CozyBear, ранее обвиняли в атаке на системы электронной почты в Государственном департаменте и Белом доме во время правления президента Барака Обамы. Он также был назван американскими спецслужбами в качестве одной из групп, проникших системы электронной почты в Национальный комитет Демократической партии в 2015 году, но утечка из этих писем не связано с CozyBear. (В этом обвиняли другое российское агентство.)

Совсем недавно США, Великобритания и Канада определили эту группу как ответственную за взломы, пытавшиеся получить доступ к информации об исследованиях вакцины COVID-19». ***(Laura Hautala. SolarWinds hack continues to spread: What you need to know // CNET (https://www.cnet.com/news/solarwinds-hack-hits-major-tech-companies-and-hospital-system-what-you-need-to-know/?ftag=CAD090e536&bhid=20102274281679224800074149012732&mid=13206853&cid=534816904). 22.12.2020).***

***

«Microsoft заявила, что выявила более 40 своих клиентов, которые установили троянизированные версии платформы SolarWinds Orion и в которые хакеры наращивали вторжения, добавляя дополнительные полезные нагрузки второго уровня.

Производитель ОС заявил, что смог обнаружить эти вторжения, используя данные, собранные антивирусным продуктом Microsoft Defender, бесплатным антивирусным продуктом, встроенным во все установки Windows.

Президент Microsoft Брэд Смит сказал, что его компания сейчас находится в процессе уведомления всех затронутых организаций, 80% из которых расположены в Соединенных Штатах, а остальные распределены по семи другим странам, а именно Канаде, Мексике, Бельгии, Испании, Великобритания, Израиль и ОАЭ.

В то время как текущий список известных жертв взлома SolarWinds в основном включает правительственные агентства США, Смит сказал, что государственный сектор составляет лишь небольшую часть списка жертв, при этом

44% составляют ИТ-компании, такие как фирмы-разработчики программного обеспечения и поставщики оборудования.

Президент Microsoft также заявил, что атака продолжается, и хакеры все еще пытаются взломать новые компании, несмотря на то, что инцидент стал публичным и активно расследуется.

«Несомненно, число и местонахождение жертв будут продолжать расти, - сказал Смит.

Последней жертвой в этом списке является сама Microsoft, которая за несколько часов до анализа Смита признала, что установила троянизированную версию приложения SolarWinds внутри своей собственной инфраструктуры.

Reuters сообщило, что хакеры получили доступ к внутренней сети Microsoft, но Microsoft отрицала, что они могли достичь производственных систем и повлиять на ее бизнес-клиентов и конечных пользователей.

КРАТКОЕ ОПИСАНИЕ ВЗЛОМА SOLARWINDS И ПОСЛЕДСТВИЯ

Пять дней спустя масштабы взлома SolarWinds продолжают расти.

Весь этот инцидент начался на прошлой неделе, когда охранная фирма FireEye заявила, что спонсируемая государством хакерская группа получила доступ к ее внутренней сети, украла инструменты для проверки на проникновение и попыталась получить доступ к документам по ее государственным контрактам.

Во время расследования взлома FireEye отследила вторжение в версию SolarWinds Orion, зашифрованную вредоносным ПО, - инструмент сетевого мониторинга, используемый в крупных корпоративных сетях.

Получив уведомление от FireEye, компания SolarWinds в воскресенье призналась в взломе, сообщив, что несколько обновлений приложения Orion, выпущенных в период с марта по июнь, содержали троян-бэкдор.

Днем позже SolarWinds признала в документах SEC, что около 18000 клиентов установили троянизированные обновления, что вызвало массовый поиск внутри корпоративных сетей, при этом ИТ-персонал пытался узнать, установили ли они версию приложения Orion, зараженную вредоносными программами, и нет ли вредоносных программ второго уровня полезные нагрузки использовались для эскалации атак.

Это оказалось громоздкой и сложной задачей, поскольку вредоносная программа, названная SUNBURST или Solorigate, содержала несвязанный дизайн между полезными нагрузками первого и второго этапов, что затрудняло определение того, на каких и скольких системах хакеры увеличили свой доступ.

Тем не менее, в среду Microsoft предприняла шаги по защите пользователей и захватила веб-домен, который вредоносная программа SUNBURST первой стадии использовала для сообщения злоумышленникам. Вместе с GoDaddy и FireEye Microsoft превратила домен в аварийный выключатель, чтобы предотвратить отправку вредоносного ПО SUNBURST своим создателям и загрузку полезных данных второго уровня.

Тем не менее, компании, которые уже были заражены до того, как был установлен этот аварийный выключатель, теперь должны быть обнаружены.

По словам Смита, в настоящее время это число составляет около 40, но это число, скорее всего, будет расти по мере того, как исследователи узнают больше об

этих полезных нагрузках второго уровня, некоторые из которых были идентифицированы Symantec под названием Teardrop.

Ниже приведена карта, показывающая текущее распределение систем, зараженных вредоносным ПО SUNBURST первой стадии, по данным телеметрии Microsoft Defender.

Смит, который часто призывал правительства прекратить атаки на частный сектор в рамках своих операций по кибершпионажу, не приписывал атаку какой-либо конкретной стране, но критиковал злоумышленников.

«Это не «обычный шпионаж» даже в эпоху цифровых технологий», - сказал Смит. «Вместо этого он представляет собой акт безрассудства, который создал серьезную технологическую уязвимость для Соединенных Штатов и всего мира».

«По сути, это не просто атака на конкретные цели, но и на доверие и надежность критически важной инфраструктуры мира с целью продвижения разведки одной страны».

Смит призвал к более жестким международным правилам поведения в отношении стран, совершающих такие безрассудные атаки.

Репортаж из Washington Post утверждает, что российская группа взломщиков APT29 ответственна за взлом SolarWinds, но ни одно правительство или фирма безопасности не подкрепил претензии газеты. APT29 ранее был назван спецслужбами США и Эстонии, как связанный с Службой внешней разведки России (СВР)». ***(Catalin Cimpanu. Microsoft says it identified 40+ victims of the SolarWinds hack // ZDNet (https://www.zdnet.com/article/microsoft-says-it-identified-40-victims-of-the-solarwinds-hack/). 18.12.2020).***

***

«Кевин Мандиа, генеральный директор FireEye, сказал, что, хотя около 18 000 организаций имели вредоносный код в своих сетях, именно 50 пострадали от серьезных нарушений.

Как известно, нападениями стали казначейство США и министерства внутренней безопасности, государства и обороны.

Госсекретарь США Майк Помпео обвинил во взломе Россию.

То же самое и с председателями комитетов по разведке Сената и Палаты представителей.

Однако президент Трамп подверг сомнению роль России в двух твитах в субботу, намекая вместо этого на участие Китая.

Г-н Мандиа сказал CBS News, что кибератака "очень соответствовала" тому, что официальные лица США знают о работе российской службы внешней разведки, СВР.

«Я думаю, что это люди, которым мы отреагировали в 90-х, в начале 2000-х. Это продолжающаяся игра в киберпространстве», - сказал он.

Он сказал, что атака на базирующийся в Texace SolarWinds Orion, инструмент компьютерной сети, лежащий в основе взлома, имеет «самые ранние свидетельства того, что она была разработана».

Все началось с «пробного запуска» в октябре 2019 года, когда был изменен «безобидный код». «Затем, где-то в марте, операторы, стоящие за этой атакой,

действительно внедрили вредоносный код в цепочку поставок, - сказал он, - и внедрили его туда, и это бэкдор, который затронул всех».

Что говорят об участии России?

Несмотря на отрицание Россией "безосновательных" утверждений, многие в разведывательном сообществе США подозревают, что ответственность за это несет российское правительство.

Г-н Помпео сказал в пятницу: «Мы можем довольно четко сказать, что именно русские участвовали в этой деятельности».

Он сказал, что Россия пытается «подорвать наш образ жизни», и что президент России Владимир Путин «остается реальным риском».

Помпео и раньше занимал жесткую позицию в отношении России. Когда он был госсекретарем, США вышли из ключевого ядерного договора и Договора по открытому небу о полетах с воздушным наблюдением.

Республиканский председатель сенатского комитета по разведке Марко Рубио написал в Твиттере, что «становится все более очевидным, что российская разведка осуществила самое серьезное кибернетическое вторжение в нашей истории». По его словам, ответ «должен быть пропорциональным, но значительным».

Адам Шифф, председатель комитета по разведке Палаты представителей от демократов, поддержал эти взгляды, заявив в воскресенье: «Я не думаю, что есть какие-либо сомнения в том, что это была Россия».

И он нанес удар по президенту Трампу за его комментарии по этому поводу, в которых говорилось, что они были «одинаково разрушительными, лживыми и вредными ... для нашей национальной безопасности».

Президент долгое время относился к Москве неоднозначно, преуменьшая значение таких инцидентов, как обвинения в том, что Россия предлагала талибам награду за убийство американских войск.

В своих твитах в субботу Трамп снова включил то, что он называет «фальшивыми новостными СМИ», за преувеличение этого вопроса.

Он написал: «Кибер-хакерство в фейковых новостях гораздо больше, чем на самом деле.

«Я был полностью проинформирован, и все хорошо под контролем. Россия, Россия, Россия - это приоритетное пение, когда что-либо происходит, потому что Lamestream, в основном по финансовым причинам, боится обсуждать возможность того, что это может быть Китай (это может быть!)."

Избранный президент Джо Байден, который должен привести к присяге 20 января, пообещал сделать кибербезопасность «главным приоритетом» своей администрации.

«В первую очередь нам необходимо помешать и удержать наших противников от проведения серьезных кибератак», - сказал он в четверг.

«Мы сделаем это, среди прочего, путем возложения существенных затрат на тех, кто несет ответственность за такие злонамеренные атаки, в том числе в координации с нашими союзниками и партнерами».

Что мы знаем о хакерской кампании?

Хакерам удалось получить доступ к крупным организациям, взломав программное обеспечение для управления сетью, разработанное ИТ-компанией SolarWinds из Техаса.

Доступ мог позволить хакерам получить высокую степень контроля над сетями организаций, использующих это программное обеспечение, но, похоже, использовался для кражи данных, а не для какого-либо разрушительного или разрушительного воздействия.

Считается, что они напали на ограниченное количество организаций в попытке украсть информацию о национальной безопасности, обороне и другую связанную информацию.

Однако, хотя программное обеспечение могло быть загружено, это не обязательно означает, что данные были взяты.

Компания SolarWinds Orion ранее заявляла, что 18 000 из ее 300 000 клиентов могли быть затронуты, но нет никаких свидетельств того, что целью кибератаки была значительная кража данных клиентов или граждан.

Исследователи, назвавшие этот взлом Sunburst, говорят, что на полное осмысление его могут потребоваться годы.

Считается, что более трех десятилетий хакеры, связанные с Москвой, пытались украсть секреты США в Интернете .

Считается, что несколько других организаций по всему миру, в том числе в Великобритании, стали жертвами хакеров, использующих то же программное обеспечение для управления сетью». ***(US cyber-attack: Around 50 firms 'genuinely impacted' by massive breach // BBC (https://www.bbc.com/news/world-us-canada-55386947). 20.12.2020).***

***

«Считается, что более трех десятилетий хакеры, связанные с Москвой, пытались украсть секреты США в Интернете.

Эти нарушения систем США во многом определили, как Америка видит киберпространство и как она защищает себя.

И они узнали, что не всегда можно предсказать или остановить усилия Москвы.

1) Яйцо кукушки

Первым, кто выследил иностранных хакеров, собирающих конфиденциальные данные из США, был не шпион, а астроном, которого беспокоили неоплаченные 0,75 доллара.

Клифф Столл следил за компьютерными сетями в своей лаборатории. В 1986 году он заметил, что кто-то вошел в систему, чтобы использовать компьютер, не заплатив. В ближайшие месяцы он пойдет по их следу и будет наблюдать, как неизвестная сторона ищет военную информацию.

В своей книге «Яйцо кукушки» Столл рассказывает, как он в конечном итоге проследил логин до группы хакеров в Германии, которые продали свой доступ КГБ, московской спецслужбе.

Это побудило Столла привлечь американское разведывательное сообщество.

Открытие Столла, первой страны, переместившей информацию в Интернет, стало первым признаком того, что США станут прибыльной целью для иностранных хакеров.

2) Лунный лабиринт

Десять лет спустя, в середине 1990-х годов, была раскрыта первая крупная кампания кибершпионажа, проведенная государственной разведкой.

Под кодовым названием Moonlight Maze некоторые детали остаются засекреченными. Но это была группа высококлассных хакеров, работавших "медленно и медленно", чтобы украсть военные секреты США через черный ход.

Хакеры взяли огромное количество информации. И впервые представители министерства обороны опасались, что могут что-то оставить, чтобы саботировать свои системы.

Американские следователи были уверены, что знают, кто за этим стоит. Злоумышленники работали с 08:00 до 17:00 по московскому времени (но ни разу в российский праздник), в коде был обнаружен русский язык.

Москва все отрицала и приостановила расследование.

Среди тех, кто работал над расследованием, был Кевин Мандиа - в настоящее время генеральный директор охранной фирмы FireEye. Причастные к этому сообщают, что впервые они поняли изощренность своего противника, который, как полагают, был организацией-преемником КГБ.

3) картечь янки

Кто-то взял то, чего не следовало делать, и вставил это в компьютер.

Возможно, в наши дни это знакомая история, но в 2008 году мошенническая USB-флешка с вредоносным ПО - возможно, обнаруженная на автостоянке на военной базе за границей - потрясла Вашингтон.

Это позволило хакерам проникнуть в секретные военные системы США, которые должны были оставаться в автономном режиме.

Аналитику потребовалось четыре месяца, чтобы обнаружить брешь в Центральном командовании США, а выяснение обстоятельств под кодовым названием Buckshot Yankee заняло еще больше времени.

Он был связан с той же группой, что стояла за Moonlight Maze.

Шок привел непосредственно к созданию Киберкомандования США в Пентагоне - группы, созданной для защиты конфиденциальных сетей, а также для охоты на противников в Интернете.

4) Демократы

В последующие годы Китай стал уделять больше внимания, особенно в отношении кражи коммерческих секретов.

Но Россия никуда не делась.

Во время президентских выборов в США в 2016 году выяснилось, что внутри Демократической партии находилась не одна, а две хакерские группы российских спецслужб.

Команда из агентства внешней разведки, СВР, оставалась под прикрытием, но группа военной разведки из ГРУ - Fancy Bear - имела в виду другой план.

Она утекла украденный материал, что вызвало сбои и, возможно, сыграло роль в изменении хода выборов.

Проблема заключалась в том, что никто не был подготовлен к такой «информационной операции».

На этот раз на президентских выборах 2020 года компании и чиновники насторожились, чтобы не допустить вмешательства в выборы со стороны России.

Но чего они не осознавали, так это того, что старомодный шпионаж продолжался незамеченным - виновником снова была российская разведка. В очередной раз Москва отрицает свою роль.

5) Санберст

Точные последствия взлома Sunburst через компанию SolarWinds пока не ясны. Тем не менее, федеральные чиновники говорят о «серьезном риске» из-за огромных масштабов возможного компрометации ведомств, компаний и организаций.

Президент Microsoft Брэд Смит утверждает, что это не «обычный шпионаж».

Но другие не согласны, называя это обычным шпионажем. Они добавляют, что США не только жертва, но и исполнитель подобных взломов. Разоблачения Сноудена в 2013 году показали, что США (и Великобритания) были более чем способны раскрыть секреты других стран путем компрометации аппаратного и программного обеспечения уважаемых фирм - способом, который не сильно отличается от этой последней утечки.

Однако тревожный вопрос, который может вызвать этот взлом, заключается в том, что - после более чем 30-летнего опыта и огромных инвестиций - почему все еще потребовалось так много времени, чтобы обнаружить и остановить нарушение?

Ответ? В киберпространстве злоумышленник обычно имеет преимущество найти новый путь, прежде чем защитник сможет закрыть этот пробел.

И пока в сети есть секреты, самые способные шпионы - особенно в России - будут стремиться их украсть». ***(Gordon Corera. Five Russian hacks that transformed US cyber-security // BBC (https://www.bbc.com/news/technology-55368211). 17.12.2020).***

***

«Избранный президент США Джо Байден раскритиковал администрацию Трампа за отсутствие реакции на ответ SolarWinds и за неспособность официально объяснить атаки.

По словам Байдена, взлом SolarWinds является «серьезным нарушением кибербезопасности американских компаний, многие из них, а также федеральных агентств».

«И мы до сих пор так многого не знаем, включая полный масштаб нарушения или размер причиненного ущерба. Но мы знаем, что это нападение представляет собой серьезную опасность для нашей национальной безопасности».

Он также сказал, что нет никаких доказательств того, что ситуация находится «под контролем», добавив, что министерство обороны даже не будет информировать его как избранного президента США «по многим вопросам».

«Министерство обороны даже не будет информировать нас по многим вещам, - сказал Байден. «Я не знаю ничего, что говорило бы о том, что это находится под контролем».

Мы не можем оставить это без ответа. Это означает, что необходимо четко и публично указать, кто несет ответственность за нападение, и предпринять важные шаги по привлечению их к ответственности. - Джо Байден.

Трамп преуменьшил значение атаки

Байден заявил, что хакеры, стоящие за этой продолжающейся компромиссной кампанией, смогли застать федеральное правительство врасплох и неподготовленными.

«Иностранные игроки работали над этим нарушением с конца прошлого года, по крайней мере, в прошлом году, создавая условия для компрометации наших систем, собирая конфиденциальную информацию из нашего технологического сектора мирового уровня и от частных предприятий, а также от правительственных агентств США», - сказал Байден.

Он подчеркнул, что администрация Трампа не уделяет первоочередного внимания кибербезопасности, «устраняя или понижая уровень киберкоординаторов как в White Hosue, так и в Государственном департаменте до увольнения директора CISA».

«Иррациональное преуменьшение президентом Трампом серьезности этой атаки» также упоминалось во время пресс-конференции.

Байден призвал администратора Трампа ускорить атрибуцию атаки, поскольку «нападение произошло на вахте Дональда Трампа, когда он не смотрел».

Хотя первоначальные указания генерального прокурора Уильяма Барра и госсекретаря Майка Помпео предполагают, что за взломом стоит Россия, безусловно, как объяснил Байден, долгая история безрассудной киберразрушительной деятельности России.

«Как президент он по-прежнему несет ответственность за защиту американских интересов в течение следующих четырех недель», - сказал Байден. «Но будьте уверены, что даже если он не примет это всерьез, я буду!»

Избранный президент США добавил, что киберугрозы являются одними из самых больших угроз глобальной безопасности в 21 веке.

Байден сказал, что после прихода к власти его команда будет уделять приоритетное внимание кибербезопасности по всем направлениям, консультируясь с экспертами, чтобы спланировать следующие шаги, необходимые для защиты американских систем, для улучшения киберзащиты, чтобы лучше противостоять будущим атакам, которые, "мы знаем, придут" и возложить издержки на тех, кто совершает эти нападения.

«Я считаю, что мы должны относиться к ним с такой же серьезностью, как и к угрозам, связанным с другим нетрадиционным оружием», - добавил он.

«Мы должны работать с нашими союзниками, чтобы установить четкие международные правила и механизмы для обеспечения их соблюдения и последствий для тех стран, которые их нарушают».

Взломаны десятки почтовых ящиков Казначейства

Сенатор США Рон Виден также сообщил в понедельник, что десятки учетных записей электронной почты Министерства финансов США были скомпрометированы злоумышленниками, стоящими за взломом SolarWinds.

«По словам сотрудников казначейства, в начале июля в агентстве произошла серьезная брешь, глубина которой неизвестна», - сказал Уайден, высокопоставленный член сенатского комитета по финансам. «Microsoft уведомила агентство о взломе десятков учетных записей электронной почты».

Уайден добавил, что хакеры SolarWinds также проникли в системы департамента департаментов Министерства финансов США, «где проживают высокопоставленные чиновники министерства».

«Министерство финансов до сих пор не знает всех действий, предпринятых хакерами, и не знает, какая именно информация была украдена», - сказал Уайден». ***(Sergiu Gatlan. Biden blasts Trump administration over SolarWinds attack response // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/biden-blasts-trump-administration-over-solarwinds-attack-response/). 22.12.2020).***

***

«Согласно новому уведомлению Координационного центра US-CERT, для развертывания бэкдора SUPERNOVA в платформе SolarWinds Orion хакеры воспользовались уязвимостью нулевого дня. Уязвимость CVE-2020-10148 затрагивает SolarWinds Orion API и позволяет злоумышленникам выполнять неавторизованные команды API и тем самым скомпрометировать установки SolarWinds.

«Процесс аутентификации API можно обойти путем включения особых параметров в часть Request.PathInfo URI-запроса к API, что позволит атакующему выполнять неавторизованные команды API. В частности, если атакующий добавит в запрос серверу SolarWinds Orion параметр PathInfo 'WebResource.adx', 'ScriptResource.adx', 'i18n.ashx' или 'Skipi18n', SolarWinds может установить флаг SkipAuthorization, благодаря которому запросы API могут обрабатываться без обязательной аутентификации», - говорится в уведомлении.

Компания SolarWinds также обновила свое уведомление безопасности, сообщив, что через неизвестную уязвимость злоумышленники внедрили в платформу Orion бэкдор SUPERNOVA. Тем не менее, подробности об уязвимости компания не представила.

Как ранее сообщал SecurityLab, помимо нашумевшего бэкдора SUNBURST в платформе Orion был обнаружен еще один бэкдор SUPERNOVA, внедренный другой киберпреступной группировкой. Вредонос представляет собой web-оболочку .NET, внедренную путем модифицирования модуля app_web_logoimagehandler.ashx.b6031896.dll в приложении Orion». ***(Бэкдор SUPERNOVA был внедрен в SolarWinds Orion через уязвимость нулевого дня // SecurityLab.ru (https://www.securitylab.ru/news/515121.php). 28.12.2020).***

***

«Министр внутренних дел Питер Даттон внес на рассмотрение парламента законопроект 2020 года о внесении поправок в законодательство о безопасности (критическая инфраструктура) в четверг, назвав его важным шагом в защите критически важной инфраструктуры и основных услуг, на которые полагаются австралийцы.

«Критическая инфраструктура лежит в основе доставки товаров и услуг, которые необходимы для австралийского образа жизни, богатства и процветания нашей страны, а также национальной безопасности», - сказал Даттон.

«Хотя Австралия не пострадала от катастрофических атак на нашу критически важную инфраструктуру, мы не защищены. Австралия сталкивается с растущими угрозами кибербезопасности для основных служб, предприятий и всех уровней правительства».

Хотя Даттон сказал, что владельцы и операторы критически важной инфраструктуры лучше всего могут справиться с такими угрозами, он сказал, что для достижения положительных изменений необходимы командные усилия.

Законопроект направлен на внесение поправок в Закон о безопасности критической инфраструктуры 2018 года с целью внедрения «усовершенствованной основы для повышения безопасности и устойчивости критической инфраструктуры Австралии».

Он распространяет действие Закона на связь, транспорт, данные и облако, продукты питания и бакалею, оборону, высшее образование, исследования и здравоохранение.

Законопроект вводит позитивное обязательство по обеспечению безопасности для критически важных объектов инфраструктуры, поддерживаемое отраслевыми требованиями и обязательными требованиями к отчетности Австралийскому управлению сигналов (ASD); повышенные обязательства по кибербезопасности для тех организаций, которые наиболее важны для страны; и государственная помощь организациям в ответ на серьезные кибератаки на австралийские системы.

В четверг Даттон заявил, что обязательство по принятию и соблюдению программы управления рисками призвано улучшить основные методы обеспечения безопасности критически важных объектов инфраструктуры путем «обеспечения того, чтобы организации применяли целостный и проактивный подход к выявлению, предотвращению и снижению рисков».

По его словам, цель структуры, требующей отчетности ASD, - обеспечить «всестороннее понимание рисков кибербезопасности для критически важных объектов инфраструктуры».

"За счет большей осведомленности правительство может лучше видеть злонамеренные тенденции и кампании, которые не будут очевидны для отдельной жертвы атаки. Это гарантирует, что правительство сможет надлежащим образом консультировать и помогать организациям во всей экономике, чтобы лучше защитить свои активы от кибер-атак. атаки ", - продолжил он.

В законопроекте также содержатся полномочия последней инстанции, которые позволяют правительству вмешиваться для защиты активов во время или после серьезной кибератаки.

Даттон сказал, что законопроект был разработан на основе обширных консультаций с представителями отрасли.

Читайте также: Технологические гиганты не убеждены, что австралийский законопроект о критической инфраструктуре в настоящее время соответствует назначению

«Окончательный законопроект отражает результаты процесса консультаций и гарантирует, что у нас есть правильный баланс между принятием эффективных мер по управлению безопасностью нашей критически важной инфраструктуры и соответствующими сдержками и противовесами», - заявил он.

«На этом консультации не заканчиваются, правительство намерено продолжить обсуждение, чтобы гарантировать, что реформы будут реализованы наиболее подходящим и эффективным образом».

Это включает участие отрасли в разработке отраслевых требований и руководящих указаний для законов.

В другом месте в четверг генерал-губернатор одобрил законопроект 2020 года о реформе иностранных инвестиций (защита национальной безопасности Австралии), который обновляет структуру обзора иностранных инвестиций Австралии с общей целью устранения рисков национальной безопасности, усиления соблюдения и оптимизации инвестиций в неконфиденциальные предприятия.

Хотя законопроект направлен на защиту Австралии, сектор квантовых технологий страны, а также федеральная оппозиция отметили, что обеспокоены проблемами, которые законопроект может создать для зарождающейся отрасли, в основном вокруг инвестиционных возможностей.

Q-CTRL, первая австралийская компания по квантовым технологиям, финансируемая венчурным капиталом, ранее заявляла, что широкие определения «предприятий национальной безопасности» в законодательстве охватывают «фактически все развивающиеся компании квантовых технологий и ставят наш сектор в чрезвычайно невыгодное положение по сравнению с конкурентами, сформированными в регионах. с более крупной и зрелой базой инвесторов, включая США и ЕС».

«Проще говоря, австралийский венчурный капитал недостаточно зрел, чтобы поддерживать рост нашей отрасли на данном этапе, а это означает, что полная реализация потенциала квантовых технологий в Австралии требует привлечения иностранных инвесторов», - сказал генеральный директор, основатель и профессор Q-CTRL Майкл Бирчук. Сказал». ***(Asha Barbaschow. Tech industry concerns put aside as Critical Infrastructure Bill enters Parliament // ZDNet (https://www.zdnet.com/article/tech-industry-concerns-put-aside-as-critical-infrastructure-bill-enters-parliament/). 10.12.2020).***

***

«В ноябре федеральное правительство опубликовало проект закона о внесении поправок в закон о безопасности (критическая инфраструктура) 2020 года, который направлен на внесение поправок в Закон о безопасности критически важной инфраструктуры 2018 года (SOCI) для реализации «расширенных рамок для повышения безопасности и устойчивости критически важных объектов инфраструктуры Австралии.».

В случае принятия SOCI создаст новый класс регулируемых организаций, известных как «системы национального значения», которые министр внутренних дел Майк Пецзулло назвал наиболее важными сегментами национальной инфраструктуры: газ, вода, электроэнергия и банковское дело.

Это создаст обязательные циклы отчетности между сектором и Австралийским центром кибербезопасности, что позволит ответственному министру обозначить сектор как настолько уязвимый, что Австралийское управление сигналов (ASD) будет в сети и осуществлять мониторинг.

Но не все, как отметил Пецзулло, получат такую защиту на уровне ASD при SOCI, поскольку экономика слишком велика.

Столкнувшись в пятницу с комитетом по правовым и конституционным вопросам законодательства, Пецзулло спросили, не приведет ли забота о «высшем уровне» к игнорированию потребностей «среднего уровня». Его также попросили подробнее рассказать о том, как правительство видит свою ответственность.

«Здесь есть два направления. Это похоже на преступление в целом. Правительства создают рынки страхования - люди берут страховку - но они также борются с преступностью», - сказал он.

«Вплоть до уровня домашнего хозяйства от вас ожидается, что в рамках вашей семейной страховки вы будете защищать свою собственность с помощью сигнализации, замков и т. Д. - и это влияет на размер премии, но это не мешает полиции - фактически, полиция активно преследует преступников, которые могут совершать взлом и проникновение. Кибернетическая ситуация не исключение".

Он сказал, что, продолжая метафору страхования, недостающий элемент - это затраты, которые в актуарном смысле готовы нести как домохозяйства, так и фирмы, чтобы обеспечить определенный уровень защиты.

«Затем правительство наносит удар по злоумышленнику или по преступной группе, дополняя его», - сказал Пецзулло. «Это очень похоже на модель страхования и борьбы с преступностью. Кибернетика очень слабо развита. Нет страховых продуктов. Невозможно оценить риск так же, как, например, кража со взломом, материальный ущерб или автомобильные аварии. Мы». re в самые первые дни».

Он сказал, что департамент изучает, как оценить риск и какие схемы регулирования следует ввести в действие, чтобы покрыть уровень ниже уровня национальной безопасности.

"Я уверен, что мы с вами согласимся с тем, что атака на энергосистему, атака на нашу систему управления воздушным движением или атака, лишающая нас способности вести банковские операции, вызовет хаос, поэтому правительство сосредотачивает свое самое мощное оружие, его самые мощные ресурсы, на этот

риск», - продолжил он. "Это должно быть целостное общество и общеэкономический ответ.

«Другими словами, это будет многоуровневый подход во всей экономике».

Пецзулло ожидает, что в ближайшее время в Парламент будет внесен закон о расширенной системе регулирования. До Рождества осталось два сидячих дня.

ЗАКОН О ДАРКВЕБЕ, КОТОРЫЙ ПОМОЖЕТ ПРОТИВОДЕЙСТВОВАТЬ БАНДАМ ВЫМОГАТЕЛЕЙ

Пецзулло спросили, какие действия предпринимает правительство, чтобы помешать группам вымогателей, чтобы они могли атаковать их у источника. Его также спросили, является ли программа-вымогатель главной киберугрозой Австралии.

«Это, безусловно, наиболее распространенное явление. Это похоже на преступление в целом. С точки зрения объема преступности это так. Что касается стратегических рисков для нашей страны, правительство неоднократно заявляло ... что с точки зрения последствий нападения, наши банковская система или платежная система, которая находится в банковской системе или электросети, и прекращение распределения электроэнергии, что будет более серьезным риском для экономики Австралии и нашего общества - это менее вероятно», - сказал он.

«Так что это похоже на преступление - есть объем преступлений, а есть очень серьезные, серьезные преступления».

В четверг австралийское правительство выдвинуло законопроект 2020 года о поправках к законодательству о надзоре (выявление и нарушение), который предоставит Федеральной полиции Австралии (AFP) и Австралийской комиссии по уголовной разведке (ACIC) три новых ордера на борьбу с онлайн-преступлениями.

«Мы хотим, чтобы полномочия, содержащиеся в законопроекте… [чтобы мы] могли утихнуть, чтобы мы могли точно увидеть, где находятся эти киберпреступные узлы. Они часто находятся вне юрисдикции. К тому времени, как вы получите ордер и продолжат сотрудничество с правоохранительными органами, они прекратят свою деятельность и двинутся дальше», - сказал Пецзулло.

«Мы хотим атаковать их на месте, атаковать их серверы, захватить их системы, идентифицировать их IP-адреса и определять географическое положение, где они находятся на поверхности планеты. Проблема в том, что технологии все чаще опережают закон с темной сетью - это очень похоже на шифрование.

«Проблема в том, что та же самая технология анонимности позволяет вам оставаться невидимым, поэтому мы хотим, чтобы законодательство о темной сети ... могло убрать эту маску-невидимку. Вот куда идет объем, и если мы не будем охотиться на них в темноте сети они станут невосприимчивыми».

Говоря о технической помощи, которую ASD может предоставить в рамках имеющихся полномочий, в соответствии с соответствующим разделом Закона о разведывательных службах, Пецзулло сказал, что в настоящее время департамент не ищет дополнительных полномочий для ASD, а скорее использует свои полномочия в наступательных целях.

«Нет необходимости расширять эти полномочия. Когда вы говорите «с использованием возможностей военной разведки», ASD имеет высший уровень ... как сбора разведывательной информации в киберпространстве, так и кибер-

разрушения», - сказал он. «Сейчас мы начали применять эти орудия нападения ... против преступников. Таким образом, полиция будет выбирать цели. У них будут полномочия собирать разведданные, но вместо того, чтобы создавать совершенно новый дублированный ASD введите "- если я могу использовать эту фразу - система в AFP, они будут импортировать полномочия ASD через положения о технической помощи в рамках ISA, чтобы нам не пришлось дублировать это». ***(Asha Barbaschow. Home Affairs likens critical infrastructure protections to insurance and crime-fighting // ZDNet (https://www.zdnet.com/article/home-affairs-likens-critical-infrastructure-protections-to-insurance-and-crime-fighting/). 08.12.2020).***

***

Захист персональних даних

«В свободном доступе были обнаружены ссылки на рабочие чаты московских больниц и станций скорой помощи, где можно было найти подробные персональные данные пациентов, включая ФИО и адрес проживания

Издание Readovka сообщило в своём Telegram-канале об обнаружении ссылок на рабочие чаты московских больниц и станций скорой помощи, а вместе с ними и списков переболевших коронавирусом москвичей:

«В онлайн-документах доступны ФИО больных, адрес проживания и регистрации, а также вся информация о течении болезни и заборах анализов.

В мэрии об утечке уже знают: чаты оперативно удаляются — несколько из них исчезли на глазах наших журналистов. Чего не скажешь о документах с персональными данными больных — хранившиеся в гугл-таблицах списки уже скачаны всеми желающими».

…в Сеть также попали данные о серверах 1С и ключи для подключения к системе учета коронавирусных больных.

«Если вы переболели ковидом в Москве, у нас для вас плохие новости, — в свою очередь, пишет Baza, также ссылаясь на таблицы с данными. — Скорее всего ваши персональные данные попали в сеть — сейчас столичные власти расследуют крупнейшую утечку с начала пандемии. По разным данным, в сеть могла попасть персональная информация 300 тысяч переболевших ковидом москвичей»…

Председатель общества защиты пациентов Андрей Хромов рассказал The Insider, что это прямое нарушение закона, который защищает любую информацию о пациентах и перенесенных ими заболеваниях. По словам Хромова, в его организацию пока не было обращений от людей, чьи данные утекли в сеть, но как только они поступят, Общество защиты пациентов будет отстаивать их права.

В то, что собираемые государством данные защищены, верят только 30% россиян, говорится в октябрьском исследовании Российской венчурной компании и Института национальных проектов на основе опроса, в котором участвовали более 3 тыс. человек. В то же время большинство россиян считают допустимым сбор государством информации о контактах граждан для выявления потенциально

зараженных COVID-19, а также использование правоохранительными органами алгоритма распознавания лиц для обеспечения безопасности. Так ответили соответственно 66 и 76% опрошенных.

UPD. Руководитель столичного департамента информационных технологий Эдуард Лысенко заявил, что утечка произошла не в результате взлома, а из-за человеческого фактора. По его словам, сотрудники, которые занимались обработкой служебных документов, допустили передачу этих файлов третьим лицам.

«Проверка продолжается, по ее результатам будут приняты меры», — подытожил Лысенко.

UPD 2. Портал Readovka, изучив слитую базу, пришёл к выводу, что московская мэрия осознанно занижала статистику заболевших COVID-19 как минимум в 1,5 раза, а сама утечка персональных данных 300 тыс. заболевших людей — только верхушка айсберга. Согласно сводным таблицам московского Депздрава из попавшей Сеть базы, к 24 апреля в Москве коронавирусом болели 52 596 человек. Однако по официальным сводкам, опубликованным Оперштабом 24 апреля, к этому дню заражённых в столице было якобы только 36 897 человек.

UPD 3. Директор «Информационной культуры» Иван Бегтин отреагировал на утечку данных и заявление ДИТ о роли человеческого фактора. У себя на странице в Facebook он написал, что ведение баз заболевших в таблицах в Google называется халатностью, а не человеческим фактором. По его словам, «это ситуация не про дисциплинарные проверки и не про увольнения, а про уголовные дела».

«Это данные составляющие врачебную тайну и их вообще не имели право использовать за пределами медицинских информационных систем или иных регламентированных ГИС. А когда утекут данные по слежке Правительства Москвы за горожанами через городскую сеть Wi-Fi, приложение «Активный гражданин» и др. — это тоже будет «человеческий фактор»? А неспособность властей Москвы сформировать четкие этические и технические регламенты работать с персональными данными — это тоже человеческий фактор?» — написал Бегтин…». ***(Столичные власти проверяют информацию об утечке данных больных коронавирусом // РосКомСвобода (https://roskomsvoboda.org/67292/). 09.12.2020).***

***

«Неизвестный хакер выставил на продажу аккаунты Microsoft и Office 365 сотен руководителей компаний со всего мира. Сообщается, что хакер взломал аккаунты генеральных директоров, президентов, вице-президентов, финансовых директоров, технических директоров компаний из Великобритании, США и других стран мира.

Достоверность продаваемых данных уже подтверждена специалистами по кибербезопасности. Каким образом хакер получил доступ к этим аккаунтам, он не сообщает.

Специалисты уже признали, что продаваемые данные можно использовать для вымогательства денег или доступа к корпоративным документам и

информации». ***(На продажу выставлены аккаунты руководителей компаний со всего мира // ProPro (http://propro.com.ua/archives/20973). 01.12.2020).***

***

«Более трети (36.4%) людей уверены, что обезопасить данные на ноутбуке от киберзлоумышленников можно, просто заклеив веб-камеру персонального компьютера. На это указал опрос, произведенный специалистами компании "Мегаплан" (разработчик программного обеспечения для бизнеса).

Другой востребованный среди украинцев способ защиты от киберзлоумышленников — сокрытие персональных данных в соцсетях. Сюда же — создание фейковых страниц на социальных ресурсах. Такая практика распространена у более тридцати процентов опрошенных.

Более трети респондентов сталкивались со взломом аккаунтов в социальных сетях. Для защиты от взлома и утечек личных данных 27% опрошенных производят смену паролей раз в год.

Почти половина опрошенных (45%) не меняют пароли ежегодно, так как боятся их забыть. Такая же картина характерна для мобильного банкинга — 46% людей не меняют пароли, чтобы не забыть их.

Половина опрошенных пользуются одинаковыми паролями в разных сервисах — это, как подчеркивают эксперты по кибербезопасности, очень плохая практика». ***(Ольга Калинина. Как обезопасить данные на ноутбуке от киберзлоумышленников - заклеить веб-камеру не достаточно // Зоряный (https://zoryanyy.tv/articles/technology/kak_obezopasit_dannye_na_noutbuke_ot_kiberzloumyshlennikov_zakleit_veb_kameru_ne_dostatochno/). 02.12.2020).***

***

«В истории со взломом компьютерных систем "Манчестер Юнайтед" была поставлена точка. Все закончилось благополучно для клуба с "Олд Траффорд".

Напомним, две недели назад "Юнайтед" объявил, что клуб стал жертвой атаки со стороны "изощренных киберпреступников".

Затем стало известно, что "красные дьяволы" подверглись шантажу — хакеры требовали несколько миллионов фунтов, угрожая опубликовать деликатную для клуба информацию. Существовали опасения, что речь идет о трансферных планах "Юнайтед", контрактах игроков и коммерческих соглашениях.

Официально "Юнайтед" не распространяется, был ли заплачен выкуп, однако Daily Mail утверждает, что требования хакеров не были удовлетворены.

На время клубу пришлось отключить отдельные компьютерные системы, а некоторые сотрудники даже получили указание не пользоваться электронной почтой, но в пятницу все вернулось в норму.

Предполагается, что вирус проник во внутренние системы клуба с помощью фишинга — поддельного письма по электронной почве.

Однако благодаря тому, что компьютерные системы "Юнайтед" были сегментированы, ущерб оказался минимален. Инсайдеры клуба уверяют, что утечки секретной информации не произошло.

Тем не менее, Офис Уполномоченного по информации все еще проводит проверку в отношении "дьяволов", которым грозит многомиллионный штраф, если утечка персональной информации все же будет обнаружена». ***(Юнайтед разобрался с кибератакой // ALLSPORT-NEWS.NET (http://allsport-news.net/404055_yunayted_razobralsya_s_kiberatakoy.html). 05.12.2020).***

***

«Французский регулятор защиты данных, Национальная комиссия по информатике и свободе (CNIL), в четверг наложила на Google и Amazon крупные штрафы за нарушение правил в отношении трекеров онлайн-рекламы, известных как файлы cookie.

Регулятор приказал Google выплатить 100 миллионов евро, а Amazon - 35.

CNIL заявил, что обе компании нарушили статью 82 Закона о защите данных Франции: Google совершил три правонарушения, а Amazon - два.

Компании были оштрафованы за размещение отслеживающих файлов cookie на компьютерах своих пользователей во Франции «без получения предварительного согласия и без предоставления соответствующей информации».

Файлы cookie позволяют технологическим гигантам «следить» за своими пользователями в Интернете, чтобы компании могли показывать им персонализированную рекламу.

Google также был оштрафован за отслеживание пользователей, которые специально отключили персонализацию рекламы.

CNIL сообщил, что у Amazon и Google было 90 дней, чтобы изменить информационные баннеры, которые он показывает пользователям в файлах cookie. Если они не внесут необходимые изменения, им будет грозить дополнительный штраф в размере 100 000 евро в день до внесения изменений.

Представитель Google сказал: «Люди, использующие Google, ожидают, что мы будем уважать их конфиденциальность, независимо от того, есть у них учетная запись Google или нет. Мы придерживаемся нашего опыта предоставления предварительной информации и четких средств контроля, надежного внутреннего управления данными, безопасной инфраструктуры и, прежде всего, полезных продуктов».

Представитель Google добавил: «Сегодняшнее решение, принятое в соответствии с французскими законами об электронной конфиденциальности, не учитывает эти усилия и не учитывает тот факт, что французские правила и нормативные требования являются неопределенными и постоянно меняются. Мы продолжим взаимодействовать с CNIL по мере того, как будем вносить улучшения, чтобы лучше понимать его проблемы».

Представитель Amazon заявил: «Мы постоянно обновляем наши методы обеспечения конфиденциальности, чтобы гарантировать соответствие меняющимся потребностям и ожиданиям клиентов и регулирующих органов, а также полное соблюдение всех применимых законов в каждой стране, в которой мы работаем».

Штрафы, наложенные на технологических гигантов США, - последнее из ряда наказаний, наложенных европейскими регулирующими органами…». ***(Романов Роман. Французский регулятор оштрафовал Google и Amazon на 100 и***

35 млн. евро за нарушение конфиденциальности пользователей // Internetua (https://internetua.com/francuzskii-regulyator-oshtrafoval-google-i-amazon-na-100-i-35-mln-evro-za-narushenie-konfidencialnosti-polzovatelei). 10.12.2020).

***

«Безопасность ваших учетных записей в Интернете в значительной степени зависит от того, насколько надежны ваши пароли, и если они слишком просты, злоумышленники могут взломать вашу учетную запись, подбирая ваш пароль.

Чтобы убедиться, что пользователи Chrome не используют слабые пароли, функция проверки безопасности Google Chrome предупредит вас, если ваши пароли были обнаружены при утечке данных.

Когда пользователь сохраняет учетные данные для входа в браузер, единственный способ обнаружить слабые учетные данные - открыть диспетчер паролей в Chrome.

Google сейчас работает над новой функцией, которая будет автоматически обнаруживать и выделять слабые пароли при выполнении проверки безопасности, как показано ниже.

Как включить новую проверку ненадежного пароля в Chrome

Новая функция проверки безопасности Chrome пока недоступна в стабильных каналах, но вы можете включить ее в Chrome Canary, выполнив следующие действия:

Загрузите и установите Chrome Canary.

Ener Chrome: // отметьте в адресной строке и нажмите Enter.

Найдите «слабые» и включите флажки «Проверка безопасности для слабых паролей» и «Проверка надежности паролей».

Когда будет предложено перезапустить браузер, сделайте это.

Чтобы проверить свои ненадежные пароли с помощью проверки безопасности, просто перейдите в «Настройки» > «Проверка безопасности»> «Проверить сейчас», чтобы выполнить проверку безопасности ваших паролей.

После нажатия Google автоматически просканирует ваши сохраненные пароли и выделит более слабые. Вы можете нажать на кнопку «Обзор», чтобы внести изменения в сохраненный пароль». ***(Mayank Parmar. Google Chrome will soon warn you when using weak passwords // Bleeping Computer® (https://www.bleepingcomputer.com/news/google/google-chrome-will-soon-warn-you-when-using-weak-passwords/). 02.12.2020).***

***

«Когда в октябре голландскому исследователю удалось взломать аккаунт президента США Дональда Трампа в Твиттере, в сообществе кибербезопасности не было никакого шока. В конце концов, Трамп не известен особо надежными паролями - Виктор Геверс, голландский исследователь кибербезопасности, вместе с двумя другими впервые смогли угадать пароль Трампа в 2016 году. Тогда пароль был «вы уволены», а в этом году он было «maga2020!» - простые фразы, легко связанные с личностью Трампа.

С этой разработкой команда CyberNews Investigation заинтересовалась, какие шаблоны используют обычные люди для создания своих паролей. Мы собрали данные о публичных утечках данных, включая Сборник нарушений, Сборник № 1-5 и другие базы данных. Затем мы анонимизировали данные и отключили пароли, чтобы мы могли рассматривать эти данные изолированно.

Всего мы смогли проанализировать 15 212 645 925 паролей, из которых 2 217 015 490 были уникальными. Мы обнаружили кое-что интересное в том, как люди создают пароли: свои любимые спортивные команды, города, еда и даже ругательства. Мы могли бы даже определить вероятный возраст человека, посмотрев, какой год он использует в своем пароле.

Поскольку данные поступали в различных формах, мы отфильтровали результаты, чтобы включить в них только те термины, которые мы могли понять и из которых мы могли собрать некоторые идеи.

Статистика паролей 2020

Мы проанализировали 15,2 миллиарда паролей по различным категориям используемых терминов. Мы рассмотрим наиболее интересные аспекты каждой категории, которую мы рассматривали.

Самые популярные годы, используемые в паролях

Один из самых интересных моментов - это когда мы посмотрели, какие годы с 1900 по 2020 годы наиболее часто использовались людьми при создании паролей.

Делая грубое предположение, люди обычно могут использовать годы в своих паролях, чтобы отметить:

- их год рождения
- год создания пароля
- особый год

Из нашего анализа мы видим, что самым популярным годом был 2010 год, когда в паролях использовалось почти 10 миллионов версий этого года. Вторым по популярности был 1987 год - 8,4 миллиона, а третьим - 1991 год - почти 8,3 миллиона.

Если посмотреть на график в целом, то можно увидеть, что с 1940 по 1990 год наблюдается устойчивый рост использования. После этого тенденция снижается, а с 2004 по 2010 год снова резко возрастает.

Основываясь на трех основных возможностях того, почему люди используют годы в паролях, мы можем сделать некоторые предположения:

Рост с 1940-х до 1990-х годов коррелирует с годами рождения создателей паролей, так что создателей паролей, родившихся в 1980–1990 годах, было больше, чем тех, кто родился в 1940–1980 годах.

Всплеск использования паролей «2010», скорее всего, указывает не на годы рождения (это означает, что этим пользователям меньше 10 лет), а скорее на комбинацию создания пароля и особого года.

Пик в 2000 году может быть годом рождения, но также может быть особенным, поскольку это был рубеж тысячелетия.

Конечно, это лишь некоторые предположения, которые мы делаем на основе этого набора данных.

Любимое имя в Интернете

Нам также было очень интересно узнать, какое имя в Интернете больше всего нравится - по крайней мере, какое имя чаще всего использовалось в этих просочившихся паролях. Как правило, из 15 миллиардов паролей, которые мы проанализировали, менее 1% использовали имя при создании пароля.

Так какое же имя? Победитель: Ева, но с трудом. Имя №2 - Алекс, что примерно на 50 000 раз меньше, чем Ева. После этого идет Анна, и она постепенно сокращается до 10-го места в списке самых распространенных паролей - Даниэль.

Оба наименее популярных имени - я говорю о двух последних - это Дарси и Дарси. Как бы то ни было, это не кажется популярным.

Любимая спортивная команда мира - и спорт

Глядя на данные по спортивным командам, мы получаем представление не только о том, какие спортивные команды являются лучшими в мире, но и о том, какие виды спорта наиболее популярны:

Спортивная команда номер один, по крайней мере, для англоязычного мира, кажется, это Phoenix Suns из НБА, за которой следует превосходящая команда Miami Heat (полное раскрытие: я из Майами). Третий - Цинциннати Редс из MLB. Конечно, поскольку это общие термины, есть вероятность, что некоторые из этих терминов не связаны со спортом, но это, по сути, риск, связанный со всеми терминами в этой статистике.

Европейский футбол (футбольные клубы) трижды входил в первую десятку, а Ливерпуль, Челси и Арсенал занимали 5, 6 и 8 места соответственно.

Всего мы видим, что есть пять команд НБА, две из MLB и три европейских футбольных клуба. Исходя из этого, мы можем предположить, что НБА, безусловно, является самым популярным видом спорта в мире, за ним следует европейский футбол / футбол (хотя некоторые статистические данные показывают, что футбол - номер один, а баскетбол - номер 3).

Когда мы смещаем наше понимание в сторону англоязычного мира с большим количеством данных, поступающих из США и Запада, результаты нашего анализа паролей, кажется, коррелируют.

Просто для удовольствия, наименее популярная спортивная команда для использования в паролях - это «wolverhamptonwanderers», использованная всего 3 раза, что, как мне сказали, довольно точно, исходя из их общей производительности.

Занимайтесь спортом!

Любимое ругательство в Интернете

Другой аспект, который нас интересовал, заключался в том, чтобы увидеть, сколько паролей содержит ругательства и какие ругательные слова наиболее предпочтительны.

Согласно нашему анализу, всего 152 933 335 паролей содержали ругательства. Из 2,2 млрд уникальных паролей это около 7%.

Результаты показывают, что любимым проклятым словом в Интернете является слово «задница», которое встречается почти 27 миллионов раз, за которым следует слово «секс» с немногим более 5 миллионов. Самое гибкое в мире слово «F» занимает третье место, его используют менее чем в 5 миллионах паролей…

Город №1 в мире

Просматривая данные, мы видим, что многие пользователи добавляли к своим паролям некоторые варианты названия своего города. Теперь, прежде чем переходить к нашему анализу, мы можем угадать причину, по которой люди поступают так: гордость или любовь к своему городу.

Даже если это просто признание их родного города, добавление этого к их паролям, скорее всего, будет означать некоторую признательность за город, если только это не что-то вроде «ihatephiladelphia2020!»

Итак, какие города чаще всего используются в паролях?

Под номером один идет слово «абу», которое, скорее всего, представляет столицу ОАЭ Абу-Даби. Город номер два - Рим, модная столица Италии.

Третье место занимает Лима в Перу, за ней следует гонконг - гонконг, и этот список продолжает тенденцию международных, неамериканских городов. Фактически, только два американских города, похоже, попали в этот список: Остин и «Антонио» от Сан-Антонии, и что интересно, они оба находятся в Техасе.

Лучшие месяцы, дни и сезоны

Если бы люди были похожи на меня, лучшим месяцем был бы июль или август, лучшим днем - пятница или суббота, а лучшим сезоном - явно лето. К счастью или к сожалению, мир не состоит из моих копий, поэтому давайте посмотрим, какие месяцы, дни и сезоны люди предпочитают чаще всего использовать в своих паролях.

Что ж, я рад знать, что у людей в этом мире есть здравый смысл. «Лето» наиболее популярно, а «осень» - наименее. Верхний будний день - «пятница», но нет никаких причин, чтобы «суббота» была внизу - здравый смысл подсказывает, что «понедельник» наименее популярным.

И, наконец, «май» является самым популярным месяцем, более чем в два раза популярнее, чем второй по популярности «июнь». Да, конечно, «может» - тоже обычное слово, так что есть шанс, что данные немного искажены в этом смысле. В любом случае, самые теплые месяцы находятся наверху, а абсолютно ужасный февраль в два раза непопулярен, чем предпоследний «январь».

Лучшая еда для паролей

Наконец, мы посмотрим, какие блюда люди любили включать в свои пароли. Удивительно, но это всего 1,9% при примерно 42 миллионах использований.

Кажется, что самое популярное слово о еде - это либо вкусная еда, либо вкусный напиток. Здесь «лед» может относиться к «мороженому» или «чаю со льдом», но поскольку «сливки» не входят в первую десятку, скорее всего, это напиток. Тот факт, что «чай» - номер 2, только подтверждает мою теорию. За ними следуют «пирог» и «орех».

В наименее популярных пищевых словах «майонез», «маргарин» и «приправа».

Важная вещь об этой статистике паролей

Особенно сложно судить о том, являются ли эти элементы пароля - год, ругательство, спортивная команда, город или что-то еще - обязательно хорошим или плохим.

Однако мы смотрели на длину используемых паролей с точки зрения количества используемых символов. К сожалению, большинство используемых паролей состояло из 8 или менее символов.

Это, в сочетании с вероятностью того, что пароли не были слишком сложными - вместо этого состояли из легко угадываемых комбинаций - заставляет нас думать, что пароли из этих баз данных не соответствуют стандартам. Есть гораздо лучшие способы создать надежный пароль.

Например, при использовании слова «heat» в качестве элемента пароля легко угадывается «Letsgoheat» (10 символов), а что-то более сложное - «heatromearsenalhjamesp» (парольная фраза из 22 символов). Люди также создают надежные парольные фразы, используя мнемонические устройства, что лучше, поскольку они обычно длинные и содержат случайные слова, не имеющие логического значения между собой, поэтому их легче запомнить, но сложнее для алгоритма взлома.

Конечно, сейчас этот разговор уже стал спорным: лучшие пароли - это те, которые вам совсем не нужно запоминать. По этой причине мы обычно настоятельно рекомендуем использовать менеджеры паролей. Эти простые в использовании инструменты создают для вас очень сложные пароли, которые вам даже не нужно запоминать.

В основном они представлены в виде расширений браузера, которые будут создавать или вводить ваши имена пользователей и пароли за вас. Единственное, что вам нужно запомнить, - это один мастер-пароль для использования менеджеров паролей…». ***(Bernard Meyer. After analyzing 15 billion passwords, these are the most common phrases people use // CyberNews Investigation (https://cybernews.com/best-password-managers/most-common-passwords/). 07.12.2020).***

***

«Федеральное правительство надеется «модернизировать» и «оптимизировать» использование имеющихся у него данных, а также установить правила обмена этими данными между агентствами, а также с частным и исследовательским секторами.

Реформы данных, представленные в законопроекте о доступности и прозрачности данных 2020 года, преподносятся министром государственных услуг Стюартом Робертом как возможность создать новую основу, которая может проактивно помочь в разработке более качественных услуг и политик.

Законопроект, а также законопроект о доступности и прозрачности данных (последующие поправки) были внесены в парламент в среду после двухлетних консультаций.

Правительство первоначально объявило о своем намерении ввести Закон о доступности и прозрачности данных (DATA) в мае 2018 года, когда оно поручило Управлению национального уполномоченного по данным (NDC) разработать закон в ответ на отчет Комиссии по производительности о доступности и использовании данных за 2016 год. Правительство Австралии надеялось ввести закон к 3 июня, но из-за того, что пандемия COVID-19 повлияла на его график, консультации по разоблачительному проекту законопроекта не состоялись.

В 2018 году правительство также пообещало 65 миллионов австралийских долларов на «реформу» австралийской системы данных, а в следующем году был создан Национальный консультативный совет по данным, который будет консультировать NDC по вопросам этического использования данных, ожиданий сообщества, передовой технической практики и отрасли. и международные события.

В двух словах, новый законопроект создает схему контролируемого доступа к данным государственного сектора.

Согласно законодательству, данные будут использоваться только для трех целей: предоставление государственных услуг, информирование о государственной политике и программах, а также исследования и разработки.

В документе для обсуждения в сентябре 2019 года федеральное правительство изменило то, что оно предлагало годом ранее, удалив фундаментальный элемент конфиденциальности - согласие.

Позиция правительства в отношении согласия с тех пор стала более тонкой: в палату был внесен законопроект, в котором говорится, что любой обмен личной информацией должен осуществляться с согласия отдельных лиц, если это не является необоснованным или невыполнимым.

Сейчас внимание сосредоточено на разработке «следующих слоев материалов в поддержку законопроекта», заявила на этой неделе национальный комиссар по данным Дебора Антон, включая правила, которые будут представлены после того, как законопроект будет принят парламентом.

Australian Security Intelligence Организация поправка Билл 2020, тем временем, прошел обе палаты в среду.

Он реализует ответ правительства на отчет PJCIS в полномочиях ASIO по допросу и задержанию, внося поправки в Закон об австралийской организации безопасности и разведки 1979 года в отношении полномочий по обязательному допросу и устройств слежения.

Он также вносит поправки в четыре закона, чтобы внести соответствующие поправки; и вносит поправки в зависимость от вступления в силу Закона 2020 года о Федеральном окружном и семейном суде Австралии (Последующие поправки и переходные положения).

В начале этого месяца PJCIS представила консультативный отчет, в котором рекомендовалось принять закон после того, как ASIO лишилась возможности использовать устройство слежения без внутренней авторизации.

В разведках надзор и другие законодательные акты Поправка (Integrity мера) Билл 2020, который реализует решение правительства о продлении Генерального инспектора разведки и (IGIS) юрисдикций Безопасности разведывательных функций ACIC и АУСТРАКЕ, а не только ASIO, а также вошла в доме в среду.

Закон об обязательном введении Кодекса ведения переговоров со СМИ Австралии также поступил в Палату представителей на этой неделе, как и закон 2020 года о внесении поправок в законодательство о безопасности (критическая инфраструктура), который был назван значительным шагом в защите критически важной инфраструктуры и основных услуг, на которые полагаются австралийцы. министр внутренних дел Питер Даттон.

3 декабря правительство Австралии также представило законопроект о внесении поправок в законодательство о слежке (выявление и нарушение) 2020 года, согласно которому федеральной полиции Австралии и Комиссии по уголовной разведке Австралии будет предоставлено три новых ордера на борьбу с онлайн-преступностью». ***(Asha Barbaschow. Bill giving government the nod to share data enters Parliament // ZDNet (https://www.zdnet.com/article/bill-giving-government-the-nod-to-share-data-enters-parliament/). 11.12.2020).***

***

«Кибербезопасность может быть далеко не у многих из нас в этом году, и в свете пандемии и катастрофических экономических потрясений забота о сохранении нашей личной конфиденциальности и безопасности в Интернете не обязательно является приоритетом.

Однако в этом году кибератаки никому не дали передохнуть. Нарушения данных, проникновение в сеть, массовые кражи и продажи данных, кражи личных данных и вспышки программ-вымогателей произошли в течение 2020 года, и подпольный рынок не показывает никаких признаков остановки.

По мере того как большая часть мирового населения перешла на работу с домашних моделей, а предприятия быстро перешли на удаленные операции, участники угроз также изменились. Исследования показывают, что удаленные сотрудники становятся источником до 20% инцидентов, связанных с кибербезопасностью, растет число программ- вымогателей, и нам еще предстоит узнать, что «123456» не является подходящим паролем.

Многие компании и организации также еще не соблюдают надлежащую гигиену безопасности, а уязвимости представляют собой постоянную угрозу для корпоративных сетей. В результате в этом году мы видели множество кибератак, худшие из которых мы описали ниже.

ЯНВАРЬ:

Travelex: службы Travelex были отключены от сети после заражения вредоносным ПО. Пострадали сама компания и предприятия, использующие платформу для предоставления услуг по обмену валюты.

Возврат налогов IRS: резидент США был заключен в тюрьму за использование информации, просочившейся в результате утечки данных, для подачи поддельных налоговых деклараций на сумму 12 миллионов долларов.

Независимый школьный округ Manor: школьный округ Техаса потерял 2,3 миллиона долларов во время фишинга.

Wawa: 30 миллионов записей, содержащих данные о клиентах, были доступны для продажи в Интернете.

Microsoft: гигант из Редмонда сообщил, что пять серверов, используемых для хранения анонимной пользовательской аналитики, были открыты и открыты в Интернете без надлежащей защиты.

Медицинская марихуана: была взломана база данных, поддерживающая системы точек продаж, используемые в диспансерах медицинской и рекреационной марихуаны, что затронуло примерно 30 000 пользователей в США.

ФЕВРАЛЬ:

Estée Lauder: Сообщается, что из-за сбоев в системе безопасности промежуточного программного обеспечения было обнаружено 440 миллионов внутренних записей.

Налоговый портал правительства Дании: идентификационные номера налогоплательщиков 1,26 миллиона датских граждан были случайно раскрыты.

DOD DISA: Агентство оборонных информационных систем (DISA), которое занимается ИТ для Белого дома, признало нарушение данных, потенциально ставящее под угрозу записи сотрудников.

Управление по финансовому регулированию и надзору Великобритании (FCA): FCA случайно раскрыло конфиденциальную информацию, принадлежащую примерно 1600 потребителям, в рамках запроса FOIA.

Clearview: весь список клиентов Clearview AI был украден из-за уязвимости программного обеспечения.

General Electric: GE предупредила сотрудников о том, что неавторизованный человек может получить доступ к принадлежащей им информации из-за сбоев в системе безопасности поставщика Canon Business Process Service.

МАРТ:

T-Mobile: хакер получил доступ к учетным записям электронной почты сотрудников, взломав данные, принадлежащие клиентам и сотрудникам.

Marriott: Сеть отелей пострадала от кибератаки, в результате которой были проникнуты учетные записи электронной почты. Пострадало 5,2 миллиона гостей отеля.

Whisper: приложение для анонимного обмена секретами показало в Интернете личные профили и наборы данных миллионов пользователей.

Министерство внутренних дел Великобритании: GDPR был нарушен 100 раз при обработке схемы урегулирования споров в ЕС.

Хакерские кольца для замены SIM-карт: Европол произвел аресты по всей Европе, уничтожив хакеров, занимающихся заменой SIM-карт, ответственных за кражу более 3 миллионов евро.

Virgin Media: компания предоставила данные 900 000 пользователей через открытую маркетинговую базу данных.

Whisper: Миллионы личных профилей и наборов данных пользователей были оставлены, открыты и доступны для всеобщего обозрения.

Мастер MCA: 425 ГБ конфиденциальных документов, принадлежащих финансовым компаниям, были общедоступны через базу данных, связанную с приложением MCA Wizard.

NutriBullet: NutriBullet стал жертвой атаки Magecart, когда код снятия скимминга платежных карт заразил магазин электронной коммерции фирмы.

Marriott: Marriott раскрыла новую утечку данных, затронувшую 5,2 миллиона гостей отеля.

АПРЕЛЬ:

Администрация малого бизнеса США (SBA): до 8000 соискателей срочных кредитов оказались втянутыми в утечку данных PII.

Nintendo: 160 000 пользователей пострадали от кампании массового взлома аккаунтов.

Email.it: итальянский провайдер электронной почты не смог защитить данные 600 000 пользователей, что привело к его продаже в Dark Web.

Nintendo: Nintendo заявила, что 160 000 пользователей пострадали от массового взлома учетных записей, вызванного устаревшей системой входа NNID.

Управление по делам малого бизнеса США (SBA): Управление по делам малого бизнеса выявило, что к утечке данных причастны до 8000 соискателей срочной ссуды.

МАЙ:

EasyJet: Бюджетная авиакомпания выявила утечку данных, раскрывающую данные, принадлежащие девяти миллионам клиентов, включая некоторые финансовые записи.

Блэкбауд: Поставщик облачных услуг был атакован операторами программ-вымогателей, которые захватили системы клиентов. Позже компания заплатила выкуп, чтобы данные клиентов не просочились в сеть.

Mitsubishi: Утечка данных, от которой пострадала компания, потенциально также привела к краже конфиденциальных данных о конструкции ракеты.

Toll Group: логистический гигант подвергся второй атаке программ-вымогателей за три месяца.

Мобильные пользователи Пакистана: данные, принадлежащие 44 миллионам пакистанских мобильных пользователей, просочились в сеть.

Иллинойс: Управление безопасности занятости штата Иллинойс (IDES) утекло записи о гражданах, претендующих на пособие по безработице.

Wishbone: хакерская группа ShinyHunters опубликовала в Интернете 40 миллионов пользовательских записей.

EasyJet: Групповой иск на сумму 18 миллиардов фунтов стерлингов был подан с целью компенсации клиентам, пострадавшим от утечки данных в том же месяце.

ИЮНЬ:

Amtrak: произошла утечка информации о клиенте, и хакеры получили доступ к некоторым учетным записям Amtrak Guest Rewards.

Калифорнийский университет, Сан-Франциско: Университет заплатил хакерам выкуп в размере 1,14 миллиона долларов, чтобы спасти исследования COVID-19.

AWS: AWS предотвратил масштабную DDoS-атаку со скоростью 2,3 Тбит / с.

Postbank: мошенник из южноафриканского банка получил мастер-ключ и украл 3,2 миллиона долларов.

НАСА: банда вымогателей DopplePaymer утверждала, что взломала сети ИТ-подрядчика НАСА.

Claire's: Компания по производству аксессуаров стала жертвой заражения картами Magecart.

ИЮЛЬ:

CouchSurfing: 17 миллионов записей, принадлежащих CouchSurfing, были обнаружены на подпольном форуме.

Йоркский университет: Британский университет раскрыл утечку данных, вызванную Blackbaud. Были украдены записи о сотрудниках и студентах.

MyCastingFile: американская платформа для кастинга актеров раскрыла PII 260 000 пользователей.

SigRed: Microsoft исправила эксплойт 17-летней давности, который можно было использовать для взлома серверов Microsoft Windows.

MGM Resorts : Хакер выставил на продажу записи о 142 миллионах гостей MGM.

V Shred: Личные данные 99 000 клиентов и инструкторов были опубликованы в Интернете, и V Shred решил проблему лишь частично.

BlueLeaks: правоохранительные органы закрыли портал, на котором размещалось 269 ГБ украденных файлов, принадлежащих полицейским управлениям США.

EDP: поставщик энергии подтвердил инцидент с вымогателем Ragnar Locker. По всей видимости, было украдено более 10 ТБ деловой документации.

MongoDB: хакер попытался выкупить 23 000 баз данных MongoDB.

АВГУСТ:

Cisco: бывший инженер признал себя виновным в нанесении огромного ущерба сетям Cisco, ремонт которого обошелся компании в 2,4 миллиона долларов.

Canon: фотограф-гигант был поражен бандой вымогателей Maze.

LG, Xerox: Maze снова нанес удар, опубликовав данные, принадлежащие этим компаниям после того, как им не удалось обеспечить платежи с помощью шантажа.

Intel: 20 ГБ конфиденциальных корпоративных данных, принадлежащих Intel, были опубликованы в Интернете.

The Ritz, London: Мошенники выдавали себя за сотрудников в хитроумной фишинговой афере против клиентов Ritz.

Freepik: Платформа бесплатных фотографий выявила утечку данных, затронувшую 8,3 миллиона пользователей.

Университет Юты: университет уступил киберпреступникам и заплатил выкуп в размере 457 000 долларов, чтобы группа не могла публиковать информацию о студентах.

Experian, Южная Африка: Южноафриканский филиал Experian обнаружил утечку данных, затронувшую 24 миллиона клиентов.

Carnival: круизный оператор сообщил об атаке программы-вымогателя и последующей утечке данных.

СЕНТЯБРЬ:

Невада: школа в Неваде, пострадавшая от атаки программ-вымогателей, отказалась платить киберпреступникам, поэтому в ответ данные об учениках были опубликованы в Интернете.

Немецкая программа-вымогатель для больниц. Пациент больницы скончался после того, как его перенаправили из больницы с активной инфекцией, связанной с вымогателем.

Правоохранительные органы Беларуси: произошла утечка частной информации о 1000 высокопоставленных полицейских.

NS8: генерального директора стартапа по кибермошенничеству обвинили в вымогательстве у инвесторов 123 миллиона долларов.

Спутники: иранским хакерам были предъявлены обвинения в компрометации спутников США.

Cerberus: Разработчики банковского трояна Cerberus опубликовали исходный код вредоносного ПО после того, как не смогли продать его частным образом.

BancoEstado: Чилийский банк был вынужден закрыть отделения из-за программ-вымогателей.

ОКТЯБРЬ:

Barnes & Noble: Книготорговец подвергся кибератаке, которая, как считается, была делом рук группы программ-вымогателей Egregor. Украденные записи просочились в сеть в качестве доказательства.

ИМО ООН: Международная морская организация ООН (ИМО ООН) выявила нарушение безопасности, затрагивающее общественные системы.

Бум! Мобильный телефон: поставщик телекоммуникационных услуг стал жертвой атаки со снятием карт Magecart.

Google: Google заявила, что предотвратила DDoS-атаку со скоростью 2,54 Тбит / с, одну из крупнейших когда-либо зарегистрированных.

Dickey's: В период с июля 2019 года по август 2020 года сеть ресторанов-барбекю в США подверглась атаке на торговые точки. Три миллиона клиентов позже разместили в Интернете данные своих карт.

Ubisoft, Crytek: секретная информация, принадлежащая игровым гигантам, была опубликована в Интернете бандой вымогателей Egregor.

Инсайдерская торговля Amazon: бывший финансовый менеджер Amazon и их семья были обвинены в мошенничестве с инсайдерской торговлей на 1,4 миллиона долларов». ***(Charlie Osborne. The biggest hacks, data breaches of 2020 // ZDNet (https://www.zdnet.com/article/the-biggest-hacks-data-breaches-of-2020/). 07.12.2020).***

***

«Комиссия по защите данных (DPC) объявила о завершении расследования GDPR, проведенного в отношении международной компании Twitter. Расследование DPC началось в январе 2019 г. после получения уведомления о нарушении от Twitter, и DPC обнаружил, что Twitter нарушил статьи 33 (1) и 33 (5) GDPR в части несвоевременного уведомления о нарушении DPC и неспособность надлежащим образом задокументировать нарушение. DPC наложил на Twitter административный штраф в размере 450 000 евро в качестве эффективной, соразмерной и сдерживающей меры.

Проект решения по этому запросу, представленный другим заинтересованным надзорным органам в соответствии со статьей 60 GDPR в мае этого года, стал первым проектом, прошедшим процедуру статьи 65 («разрешение споров») с момента введения GDPR. и был первым проектом решения в деле «больших технологий», по которому все надзорные органы ЕС консультировались как заинтересованные надзорные органы.

Европейский совет по защите данных опубликовал решение по статье 65 и окончательное решение на своем веб-сайте здесь». ***(Data Protection Commission announces decision in Twitter inquiry // DATA PROTECTION COMMISSION***

(https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-twitter-inquiry). 15.12.2020).

***

«Разработчик шпионского ПО Cellebrite сумел расшифровать сообщения и вложения, хранящиеся в мессенджере Signal. Он годами считался самым защищенным в мире, а теперь Cellebrite, сотрудничающая с правоохранительными органами многих стран (Россия в их числе) намерена «на законных основаниях» предоставлять силовикам доступ к переписке в этом мессенджере.

Signal скомпрометирован

Израильская компания Cellebrite, разработчик шпионского ПО, заявила, что сумела взломать мессенджер Signal. По данным портала TechRadar и разработчика антивируса AVG, Signal – это самый защищенный мессенджер в мире.

Обойти защиту Signal специалисты Cellebrite смогли при помощи собственного программного инструмента Physical Analyzer, предназначенного для систематизации и обработки информации, полученной со смартфона.

Они постоянно работают над его усовершенствованием, и один из апдейтов позволил им, по их утверждению, взломать Signal.

В основе Signal лежит проприетарная система шифрования текста и контента Signal Protocol с открытым исходным кодом.

Эта система также используется компаниями Facebook и Microsoft в своих месседжерах, но в них она шифрует только текстовые сообщения, а не передаваемые файлы.

Как проходил процесс взлома Signal

Cellebrite опубликовала подробный отчет о процессе взлома Signal прямо на своем официальном сайте. Специалисты компании рассказали, что база данных мессенджера хранится в зашифрованном с помощью SqlScipher виде. SqlScipher – это расширение SQLite с открытым исходным кодом, которое обеспечивает прозрачное 256-битное AES-шифрование файлов базы данных. Для чтения БД хакерам был нужен специальный ключ, который, как оказалось, можно извлечь из файла с общими настройками и расшифровать его с помощью ключа под названием «AndroidSecretKey», который сохраняется «Keystore» - специальной функцией ОС Android.

«После получения расшифрованного ключа нам нужно было знать, как расшифровать базу данных. Для этого мы использовали открытый исходный код Signal и искали любые обращения к базе данных. Изучив десятки классов кода, мы, наконец, нашли то, что искали», – сообщили хакеры.

Затем они запустили SqlCipher в базе данных с расшифрованным ключом и значениями 4096 и 1 для размера страницы и итераций kdf, что позволило им расшифровать БД и обнаружить текстовые сообщения в файле «signal.db.decrypted» в таблице с названием «sms». Все отправленные и полученные файлы были найдены папке «app_parts», но они были дополнительно зашифрованы.

Специалисты Cellebrite выяснили, что для шифрования вложений Signal использует алгоритм AES в режиме CTR, после чего им осталось только провести дешифровку. Дополнительно сопоставлять найденные файлы с чатами им не

пришлось – это было сделано еще на этапе анализа сообщений, и в итоге они получили полностью читабельные чаты, доступные теперь в том же виде, в котором их видят участники беседы.

Пользователи беззащитны

Взлом Signal может повлечь за собой последствия общемирового масштаба, поскольку Cellebrite весьма активно сотрудничает с правоохранительными органами и госструктурами многих стран мира, включая Россию. Ее основной продукт – это программно-аппаратный комплекс UFED, предназначенный для быстрого взлома смартфонов на базе iOS и Android и извлечения из них информации.

В России устройства UFED закупаются на миллионы рублей. Например, в 2018 г. управление Следственного комитета по Волгоградской области закупило за 800 тыс. руб. переносной аппаратный комплекс UFED Touch2 Ultimate Ruggedized. Поставщиком выступила «ЛАН-проект». В 2017 г. управление МВД по Хабаровскому краю обновило ПО UFED Touch до версии UFED Touch2 Ultimate, закупив соответствующие услуги за 1,26 млн руб. у «ЛАН-проект». Через эту же компанию UFED Touch2 закупил Сбербанк, заплативший 4,1 млн руб. за 11 единиц.

Cellebrite уже сообщила, что намерена сотрудничать с правоохранительными органами различных стран для взлома Signal на нужных им устройствах «на законных основаниях». Таким образом, информация, хранящаяся в мессенджере и до декабря 2020 г. считавшаяся защищенной, может оказаться в руках силовых структур в полностью дешифрованном виде.

Отметим, что у Signal есть и другие проблемы с безопасностью. В сентябре 2020 г. стало известно, что он «сливает» номера телефонов своих пользователей, а это позволяет вытащить всю информацию из их профилей. Она впоследствии может использоваться злоумышленниками для создания поддельных аккаунтов с целью мошенничества, но виноваты в этом будут не только мессенджеры, но и сами пользователи.

Справедливости ради стоит добавить, что аналогичная брешь была обнаружена и в WhatsApp, а вместе с ним – и в Telegram. Последний тоже считается одним из самых безопасных мессенджеров в мире». ***(Эльяс Касми. Взломан самый защищенный мессенджер в мире. Взломщики будут продавать переписку силовикам // CNews (https://www.cnews.ru/news/top/2020-12-15_hakery_vzlomali_samyj_zashchishchennyj). 16.12.2020).***

***

«По меньшей мере у 36 журналистов, продюсеров, ведущих и руководителей Al Jazeera, а также журналиста телеканала Al Araby TV в Лондоне были взломаны iPhone с помощью уязвимости нулевого дня без взаимодействия с пользователем в приложении iMessage для iOS.

Citizen Lab, исследовательская группа по кибербезопасности и нарушениям прав человека при Университете Торонто, заявила, что нулевой день был частью цепочки эксплойтов под названием Kismet, которая была создана и продана NSO Group, известным поставщиком шпионского ПО и продуктов для наблюдения.

Исследователи утверждают, что NSO продала хакерский инструмент Kismet по крайней мере четырем организациям, которые использовали его в июле и августе 2020 года для взлома личных iPhone 36 отчетов Al Jazeera со всего мира.

Команда Citizen Lab считает, что она идентифицировала двоих из четырех покупателей в Саудовской Аравии и Объединенных Арабских Эмиратах, связывая эту деятельность с двумя группами, которые организация отслеживала, как Monarchy и Sneaky Kestrel.

Последующие расследования показали, что атаки продолжались как минимум с октября 2019 года.

На момент обнаружения атак Citizen Lab сообщила, что инструмент эксплойтов Kismet работал против новейших устройств Apple (например, iPhone 11 с iOS 13.5.1).

Нулевой день перестал работать этой осенью, когда Apple выпустила iOS 14, в которую были включены несколько улучшенных функций безопасности.

Группа академических исследований уведомила Apple об атаках и заявила, что производитель ОС в настоящее время изучает отчет.

РЕГИОНАЛЬНАЯ ПОЛИТИКА И НУЛЕВЫЕ ДНИ

Сегодня, 20 декабря, для получения комментариев представитель NSO Group назвал отчет «домыслом», в котором отсутствуют какие-либо доказательства, «подтверждающие связь с NSO».

Компания заявила, что продает инструменты наблюдения только правоохранительным органам и не может определить, что ее клиенты делают с ее инструментами.

Citizen Lab ранее публиковала несколько отчетов, в которых утверждалось, что разработанные НСО хакерские инструменты использовались вне рамок расследований правоохранительных органов для отслеживания политических соперников, диссидентов, журналистов, духовенства и активистов в таких странах, как Марокко, Мексика, Саудовская Аравия, Того, Испания, ОАЭ и другие.

Катарское информационное агентство "Аль-Джазира", как полагают, стало объектом нападения из-за натянутых политических отношений между Катаром и соседними странами…». ***(Catalin Cimpanu. Zero-click iOS zero-day found deployed against Al Jazeera employees // ZDNet (https://www.zdnet.com/article/zero-click-ios-zero-day-found-deployed-against-al-jazeera-employees/). 20.12.2020).***

***

«Поставщик электроэнергии и газа из возобновляемых источников People's Energy сообщил своим более чем 250 000 клиентов, что «брешь» в безопасности его ИТ-системы была использована цифровыми взломщиками.

Соучредители британской компании Карин Соде и Дэвид Пайк написали клиентам в четверг утром, чтобы подтвердить, что «вчера People's Energy пострадала от взлома данных кибербезопасности».

«Никакая финансовая информация, реквизиты банковского счета или пароли онлайн-счетов People's Energy не были скомпрометированы для каких-либо внутренних клиентов. Однако были получены некоторые личные данные», - говорится в электронном письме, отраженном на его веб-сайте.

Эти данные включали имена участников, домашние адреса, адреса электронной почты, номера телефонов, даты рождения, номера счетов People's Energy, сведения о тарифах и идентификационные номера счетчиков.

«Мы определили, как осуществлялся доступ к нашим системам, и брешь в нашей безопасности была устранена. Мы также работаем со специальной группой безопасности, чтобы добавить дополнительную защиту в наши системы», - продолжает электронное письмо.

К сожалению, 15 клиентов малого бизнеса получили доступ к финансовым данным при взломе базы данных. Компания сообщила BBC, что реквизиты банковских счетов и коды сортировки были украдены, но все они были предупреждены непосредственно по телефону.

О взломе были проинформированы полиция, британский регулятор данных, Управление информационного комиссара и энергетический контролер Ofgem, и соучредители заявили, что следуют данным советам…» ***(Paul Kunert. Ethical power supplier People's Energy hacked, 250,000 customers' personal info accessed // The Register (https://www.theregister.com/2020/12/17/peoples_energy_hacked/). 17.12.2020).***

***

«Две тысячи серверов, содержащих 45 миллионов изображений рентгеновских лучей и других медицинских изображений, были оставлены в сети в течение последних двенадцати месяцев, и были доступны для всех без каких-либо средств защиты.

По крайней мере, так говорится в исследовании CybelAngel, продающего платформу защиты от цифровых рисков. Компания добавила, что не только конфиденциальная личная информация была незащищенной, но злоумышленники также получили доступ к этим серверам и отравили их очевидным вредоносным ПО.

«Тот факт, что мы не использовали какие-либо хакерские инструменты в ходе нашего исследования, подчеркивает легкость, с которой мы смогли обнаружить эти файлы и получить к ним доступ», - сказал Дэвид Сигула, старший аналитик по кибербезопасности CybelAngel и автор отчета компании.

В исследовании не упоминались поставщики медицинских услуг или медицинские учреждения, у которых были обнаружены нехватки безопасных систем.

Среди данных, взятых из незащищенных сетевых устройств хранения данных, связанных с больницами и медицинскими центрами по всей планете, было 23000 изображений британских пациентов, оставленных для доступа в общедоступный Интернет на 90 отдельных серверах. Рентгеновские снимки и компьютерная томография были доступны онлайн благодаря тому, что, по словам CybelAngel, было комбинацией незащищенного хранилища NAS и протокола передачи медицинских данных DICOM 1980-х годов.

Хотя он подходит для поставленной задачи, протоколы безопасности DICOM носят рекомендательный характер. В самом стандарте сказано:

Настоящий стандарт предполагает, что прикладные объекты, участвующие в обмене DICOM, реализуют соответствующие политики безопасности, включая, помимо прочего, контроль доступа, контрольные журналы, физическую защиту, поддержание конфиденциальности и целостности данных, а также механизмы для идентификации пользователей и их прав на данные доступа. По сути, каждая прикладная сущность должна гарантировать безопасность своей локальной среды, прежде чем даже пытаться защищать связь с другими прикладными объектами.

Открытые изображения включали в некоторых случаях «до 200 строк метаданных на запись, которые включали PII (личную информацию; имя, дату рождения, адрес и т. Д.)» И личную информацию о здоровье, включая «рост, вес, диагноз пациента» и так далее.

Cybelangel обнаружила, что даже специализированная фирма, «рекламирующая платную услугу для безопасного размещения и управления изображениями DICOM», просочилась в сеть около 500 000 файлов, потому что никто не подумал защитить свою сетевую файловую систему (NFS) на порту 2049.

Несмотря на то, что Cybelangel заявила, что использовала множество инструментов для поиска в сети открытых данных DICOM, в ее отчете были представлены снимки экрана с Shodan и откровенные выводы исследователей, которые просто вводили общие порты DICOM в систему поиска небезопасных комплектов, чтобы увидеть, какие устройства откликнулись.

Помимо очевидных проблем с защитой данных, наибольшее беспокойство вызвал вывод CybelAngel о том, что он «не первый, кто взглянул на эти серверы». В отчете говорится: «Некоторые [серверы] включали вредоносные сценарии. Заражение незащищенных серверов очень распространено и обычно осуществляется с помощью сценариев автоматизации, особенно для установки биткойнских (или подобных) майнеров».

Фирма рекомендовала медицинским организациям «обеспечить надлежащую сегментацию сети подключенного медицинского оборудования для визуализации» в качестве одного из средств предотвращения доступа злоумышленников к тому, чего им не следует делать.

В прошлом году компания Greenbone Networks провела аналогичное исследование, выявив вероятные поисковые запросы и номера портов через Shodan, и обнаружила, что медицинская информация 24 миллионов человек была раскрыта в Интернете как 737 миллионов элементов данных DICOM. ®» ***(Gareth Corfield. 45 million medical scans from hospitals all over the world left exposed online for anyone to view – some servers were laced with malware // The Register(https://www.theregister.com/2020/12/15/dicom_45_million_medical_scans_unsecured/). 15.12.2020).***

***

«Поставщики торговых терминалов Verifone и Ingenico выпустили меры по снижению рисков после того, как исследователи обнаружили, что устройства используют пароли по умолчанию.

Исследователи подробно рассматривают широко распространенные проблемы безопасности в торговых точках (PoS) - в частности, три семейства терминальных устройств, производимые поставщиками Verifone и Ingenico.

Проблемы, которые были раскрыты поставщикам и с тех пор исправлены, открывают несколько популярных PoS-терминалов, используемых розничными продавцами по всему миру, для различных кибератак. Затронутые устройства включают Verifone VX520, серию Verifone MX и серию Ingenico Telium 2. Эти устройства широко используются в розничной торговле - например, было продано более 7 миллионов терминалов VeriFone VX520.

«Благодаря использованию паролей по умолчанию мы смогли выполнить произвольный код через бинарные уязвимости (например, переполнение стека и переполнение буфера)», - заявили исследователи из группы Cyber R&D Lab в новом анализе недостатков на этой неделе. «Эти недостатки PoS-терминала позволяют злоумышленнику отправлять произвольные пакеты, клонировать карты, клонировать терминалы и устанавливать устойчивые вредоносные программы».

PoS-терминалы - это устройства, которые считывают платежные карты (например, кредитные или дебетовые карты). Следует отметить, что затронутые устройства представляют собой PoS-терминалы - устройство, используемое для обработки карты - в отличие от PoS-систем, которые включают взаимодействие кассира с терминалом, а также инвентарные и бухгалтерские записи торговцев.

Проблемы с безопасностью

Исследователи выявили две проблемы безопасности в этих PoS-терминалах. Основная проблема заключается в том, что они поставляются с паролями производителя по умолчанию, которые можно легко определить с помощью поиска Google.

«Эти учетные данные обеспечивают доступ к специальным «режимам обслуживания», в которых доступна конфигурация оборудования и другие функции», - заявили исследователи. «Один производитель, Ingenico, даже не дает вам изменить эти настройки по умолчанию».

Присмотревшись к специальным «сервисным режимам», исследователи затем обнаружили, что они содержат «необъявленные функции» после разрушения терминалов и извлечения их прошивки.

«В терминалах Ingenico и Verifone эти функции позволяют выполнять произвольный код через бинарные уязвимости (например, переполнение стека и переполнение буфера)», - заявили исследователи. «На протяжении более 20 лет эти «сервисные супер режимы» позволяли необъявленный доступ. Часто функции находятся в устаревшем или устаревшем коде, который все еще развертывается с новыми установками».

Злоумышленники могут использовать эти недостатки для запуска множества атак. Например, проблема с выполнением произвольного кода может позволить злоумышленникам отправлять и изменять передачу данных между терминалом PoS и его сетью. Злоумышленники также могут считывать данные, позволяя им копировать информацию о кредитных картах людей и в конечном итоге проводить мошеннические транзакции.

«Злоумышленники могут подделывать и изменять транзакции», - заявили они. «Они могут атаковать банк-эквайер через уязвимости на стороне сервера, например, в системе управления терминалами (TMS). Это аннулирует внутреннее доверие, данное между терминалом PoS и его процессором».

Исследователи связались с Verifone и Ingenico, и с тех пор были выпущены исправления для устранения проблем.

Verifone была проинформирована в конце 2019 года, и исследователи подтвердили, что уязвимости были исправлены в конце 2020 года. «В ноябре 2020 года PCI выпустила срочное обновление терминалов Verifone по всему миру», - заявили исследователи.

Между тем исследователи заявили, что потребовалось почти два года, чтобы связаться с Ingenico и получить подтверждение этого исправления…». ***(Lindsey O'Donnell. Security Issues in PoS Terminals Open Consumers to Fraud // Threatpost (https://threatpost.com/security-issues-pos-terminals-fraud/162210/). 11.12.2020).***

***

«UiPath, старт-ап, который создает ПО для автоматизации робототехники, отправляет пользователям электронные сообщения об утечке их данных.

«1 декабря 2020 года компании стало известно о несанкционированном раскрытии данных пользователей UiPath Academy», - написала в письмах компания…

Данные включали в себя реальные имена, адреса электронных почт, логины пользователей и детали сертификации UiPath для пользователей UiPath Academy.

«Нам известно только об одном ресурсе, где информация была доступна. По причинам безопасности, UiPath не может раскрыть его имя», - сообщает компания.

Также сообщается, что были слиты данные пользователей, зарегистрированных до 17 марта 2020 года включительно. Не пострадали пароли и сведения о финансах. Утечке подверглись только данные UiPath Academic. Компания отказалась сообщить, сколько именно пользователей было затронуто инцидентом». ***(UiPath рассказал об утечке данных // SecureNews (https://securenews.ru/ui-path-told-about-the-data-leak/). 11.12.2020).***

***

«Spotify признал, что пользовательские данные «утекли» некоторым бизнес-партнерам сервиса. Поэтому сейчас он сбрасывает пароли пользователей.

Представители стриминговой платформы сообщили, что утечка была обнаружена и исправлена только через 7 месяцев.

«12 ноября Spotify обнаружил уязвимость в своей системе, с помощью которой произошла случайная утечка регистрационных данных нескольким бизнес-партнерам сервиса. Среди таких данных могли быть адрес электронной почты, отображаемое имя, пароль, пол, дата рождения», - объясняет Spotify.

По оценкам специалистов сервиса, 9 апреля 2020 года уязвимость уже существовала, обнаружили ее 12 ноября и сразу же приняли меры по устранению.

Spotify связался с бизнес-партнерами, чтобы убедиться, что они удалили пользовательские данные, и сбросил пароли пользователей, которых задела утечка.

Это уже третий инцидент в Spotify за последние месяцы. Несколько дней назад хактивист, который называет себя Daniel, угнал страницу Spotify for Artists, где опубликовал посты в поддержку Тэйлор Свифт и Дональда Трампа.

А в конце ноября исследователи также обнаружили утечку в облачной базе данных, которая содержала логины 350,000 пользователей сервиса». ***(Spotify сбрасывает пароли пользователей после утечки данных // SecureNews (https://securenews.ru/spotify-resets-user-passwords-after-data-leak/). 15.12.2020).***

***

«Новое исследование показало, что потребители в Бразилии в основном не осведомлены о правилах защиты данных в стране и не подвергают сомнению методы управления персональными данными компаний.

Опрос, проведенный бразильской кредитной аналитической компанией Boa Vista с участием более 500 потребителей в период с августа по сентябрь 2020 года, показывает, что более 70% опрошенных не знают, что такое Общие правила защиты данных.

Подавляющее большинство опрошенных потребителей (90%) считают, что их личная информация не защищена должным образом запрашивающими их компаниями, а 77% выразили озабоченность по поводу возможного неправомерного использования их данных. Из опрошенных бразильских потребителей 40% заявили, что стали жертвами мошенничества.

С другой стороны, 53% опрошенных бразильских потребителей заявили, что не всегда принимают меры для защиты своей конфиденциальности, прежде чем сообщать свои личные данные компаниям. В то время как 88% респондентов заявили, что им неудобно сообщать такие данные, как регистрационный номер налогоплательщика, 55% не оспаривают компании, когда их просят предоставить такую личную информацию.

Положение о защите данных Бразилии было санкционировано президентом Жаиром Болсонару 18 сентября после почти месяца неопределенности по поводу фактической даты вступления в силу правил. Члены правления национального органа по защите данных, ответственного за соблюдение правил, были назначены в конце октября.

Опрос, проведенный Бразильской ассоциацией компаний-разработчиков программного обеспечения (ABES) в партнерстве с EY вскоре после введения правил, показал, что большинству бразильских компаний все еще необходимо приспосабливаться к правилам. Последующее исследование, проведенное ABES и EY, показало, что в технологическом секторе дела обстоят лучше, но 56% компаний в этом секторе все еще должны соблюдать новые правила». ***(Angelica Mari. Brazilians mostly unaware of data protection regulations // ZDNet (https://www.zdnet.com/article/brazilians-mostly-unaware-of-data-protection-regulations/). 29.12.2020).***

***

«Сайт продвижения книг NetGalley пострадал от утечки данных, которая позволила злоумышленникам получить доступ к базе данных с личной информацией участников.

NetGalley - это веб-сайт, который позволяет авторам и издателям продвигать цифровые рецензии своих книг (гранки) защитникам книг, влиятельным читателям и профессионалам отрасли в надежде, что они порекомендуют книги своей аудитории.

В понедельник, 21 декабря, сайт NetGalley был взломан и поврежден. После дальнейшего расследования было установлено, что злоумышленники также получили доступ к резервной копии базы данных сайта, содержащей данные участников.

«С большим сожалением сообщаем вам, что в понедельник, 21 декабря 2020 года, NetGalley стала жертвой инцидента, связанного с безопасностью данных. То, что поначалу казалось простым искажением нашей домашней страницы, после дальнейшего расследования привело к несанкционированному и незаконному доступ к файлу резервной копии базы данных NetGalley, - сообщил NetGalley в сообщении об утечке данных.

Эта резервная база данных включала личную информацию участников NetGalley, включая их логин, пароль, имя и адрес электронной почты. Другая дополнительная информация, которая могла быть в базе данных, включает почтовый адрес пользователя, дату рождения, название компании и адрес электронной почты Kindle.

NetGalley заявляет, что в базе данных не хранилась финансовая информация. В ответ на нарушение NetGalley требует, чтобы все пользователи сбросили свой пароль при следующем входе в систему.

BleepingComputer обратился к NetGalley с вопросами о том, хешируются ли пароли в базе данных, но не получил ответа.

Что делать пользователям NetGalley?

Если вы являетесь участником NetGalley, вам следует немедленно войти на сайт и изменить свой пароль.

Если вы используете тот же пароль NetGalley на других сайтах, вам также следует изменить пароль на этих сайтах на уникальный и надежный для этого сайта.

Использование уникальных паролей на каждом сайте, на котором у вас есть учетная запись, предотвращает нарушение данных на одном сайте от воздействия на вас других веб-сайтов, которые вы используете.

Рекомендуется использовать менеджер паролей, который поможет вам отслеживать уникальные и надежные пароли на каждом сайте». ***(Lawrence Abrams. NetGalley discloses data breach after website was hacked // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/netgalley-discloses-data-breach-after-website-was-hacked/). 24.12.2020).***

***

«Японский разработчик игр Koei Tecmo раскрыл утечку данных и отключил свои европейские и американские веб-сайты после того, как украденные данные были опубликованы на хакерском форуме.

Koei Tecmo известен своими популярными играми для ПК и консолей, включая Nioh 2, Hyrule Warriors, Atelier Ryza, Dead or Alive и т. Д.

20 декабря злоумышленник заявил, что 18 декабря взломал веб-сайт koeitecmoeurope.com с помощью целевого фишинга, отправленного сотруднику. В рамках этой атаки была украдена база данных форума с 65 000 пользователей, и злоумышленник утверждает, что установил на сайт веб-оболочку для постоянного доступа.

«В оболочке, которую я нашел, есть учетные данные FTP, и я был бы рад поделиться ими с вами, если вы купили оболочку, а также несколько секретов Twitter для их учетных записей Twitter, которые у них есть», - заявил злоумышленник в рамках своей коммерческой презентации.

В сообщении на хакерском форуме злоумышленник пытался продать базу данных форума за 0,05 биткойна, или примерно 1300 долларов, и доступ к веб-оболочке за 0,25, или примерно за 6500 долларов.

23 декабря тот же злоумышленник бесплатно слил базу данных на том же хакерском форуме.

Образцы базы данных, которые видел BleepingComputer, включают адреса электронной почты участников форума, IP-адреса, хешированные пароли и соли, имена пользователей, дату рождения и страну.

Koei Tecmo переводит веб-сайты в автономный режим

Узнав об утечке данных, Koei Tecmo отключил американский (https://www.koeitecmoamerica.com/) и европейский (koeitecmoeurope.com) веб-сайты со следующим сообщением: «Из-за возможности внешней кибератаки на этот веб-сайт он временно закрыт на время расследования проблемы».

Узнав об атаке, Koei Tecmo выпустил уведомление об утечке данных, в котором говорилось, что форум на веб-сайте британской дочерней компании был скомпрометирован, а украденные данные были просочены в сеть.

«На веб-сайте, управляемом KTE, страница «Форум» и информация о зарегистрированном пользователе (приблизительно 65 000 записей) были определены как данные, которые могли быть взломаны. Данные пользователя, которые могли быть утечкой посредством взлома, считаются (необязательно) имена учетных записей и соответствующий пароль (зашифрованный) и / или зарегистрированный адрес электронной почты», - сообщил Koei Tecmo в уведомлении об утечке данных.

Koei Tecmo заявляет, что нарушение затронуло только форум, а не другие части сайта. Также говорят, что никакой финансовой информации в этой базе данных не хранилось.

Игровая компания определила, что «вероятность того, что это атака вымогателя мала» и что компания не предъявляла никаких угроз или требований.

Из соображений осторожности Koei Tecmo отключила дочернюю компанию KTE в Великобритании от своей внутренней сети на время расследования атаки…». ***(Lawrence Abrams. Koei Tecmo discloses data breach after hacker leaks stolen data //***

Bleeping Computer® (https://www.bleepingcomputer.com/news/security/koei-tecmo-discloses-data-breach-after-hacker-leaks-stolen-data/). 26.12.2020).

***

«Исполняющий обязанности министра внутренней безопасности США (DHS) Чэд Вольф (Chad Wolf) сообщил, что ведомство изучает вопрос о том, встраивал ли китайский производитель телевизоров TCL «бэкдоры» для обхода безопасности в свои устройства на базе Android.

«DHS проводит проверку таких организаций, как китайский производитель TCL. В этом году было обнаружено, что TCL встроил бэкдоры во все свои телевизоры, что делает пользователей уязвимыми к кибератакам и краже данных. TCL также получает государственную поддержку КПК (Коммунистической партии Китая), чтобы конкурировать на мировом рынке электроники, благодаря чему компания стала третьим по величине производителем телевизоров в мире», — пояснил Вольф.

В прошлом месяце TCL сообщила ресурсу Tom's Guide об исправлении двух уязвимостей (CVE-2020-27403 и CVE-2020-28055) в устройствах TCL под управлением Android, которые были обнаружены исследователем безопасности Джоном Джексоном (John Jackson) и ИБ-специалистом из Sick Codes.

Эксплуатация одной из проблем позволяет любому просматривать файловую систему телевизора TCL без ввода пароля, другая представляла собой скрытую функцию, позволяющую отправлять скриншоты и логи активности пользователей на серверы в Китае.

По словам Sick Codes, TCL исправила данные уязвимости в телевизорах по всему миру в «тихом патче», не уведомляя владельцев телевизоров и не запрашивая у них разрешения. Это означает, что TCL имеет «полный доступ» к устройствам в домах людей.

«В целом, мы обеспокоены тем, что недавние комментарии о TCL, по-видимому, происходят из-за неточных описаний наших продуктов, функций и возможностей и, к сожалению, привели к спекулятивным выводам и поспешным суждениям. Мы категорически отвергаем необоснованные комментарии и умозрительные выводы», — сообщил представитель TCL журналистам Tom's Guide». ***(США заподозрили производителя телевизоров TCL в намеренном встраивании бэкдоров // SecurityLab.ru (https://www.securitylab.ru/news/515109.php). 25.14.2020).***

***

«Киберпреступная группировка REvil похитила данные крупной сети косметических клиник и угрожает опубликовать фотографии пациентов до и после операций.

По информации издания BBC, хакеры взломали облачные хранилища крупнейшей британской сети клиник Hospital Group (также известной как Transform Hospital Group) и пообещали на своей странице в даркнете опубликовать данные, если не получат выкуп. Как утверждают киберпреступники, они похитили более 900 гигабайт фотографий пациентов.

Представители Hospital Group подтвердили факт взлома и отметили, что компания проинформировала об этом своих клиентов и Управление комиссара по информации Великобритании (Information Commissioner's Office). Клиника также обратилась в местную полицию и Национальный центр кибербезопасности.

«Мы можем подтвердить, что наши IT-системы подверглись взлому. Данные платежных карт наших пациентов не были скомпрометированы, в отличие от персональной информации некоторых пациентов», — сообщили представители Hospital Group». ***(Хакеры REvil угрожают опубликовать похищенные снимки пластических операций // SecurityLab.ru (https://www.securitylab.ru/news/515111.php). 25.12.2020).***

***

«Исследователи кибербезопасности из компании Flashpoint сообщили о росте цен на доступ к RDP-серверам, украденные данные платежных карт и бизнес-модель «DDoS-как-услуга» на подпольных форумах и торговых площадках.

«В результате пандемии и связанных с ней глобальных тенденций спрос на вредоносные и незаконные товары, услуги и похищенные данные достиг нового пика на рынках даркнета. Мы наблюдали то, что можно назвать впечатляющими, проницательными инновациями во всей экосистеме киберпреступности», — отметили специалисты.

После глубокого исследования подпольного рынка специалисты обнаружили, что цены на украденные данные платежных карт резко выросли в 2020 году — с $14,64 в 2019 году до $20,16 в 2020 году. Между тем, цена «дампов» платежных карт также выросла с $24,19 в 2019 году до $26,50 в среднем в 2020 году.

Проприетарный протокол удаленного рабочего стола Microsoft, используемый для предоставления системным администраторам возможности удаленного подключения к корпоративным устройствам, а также для обновления серверов, по-прежнему является фаворитом у киберпреступников. Популярность списков RDP среди киберпреступников продолжает расти. На подпольных торговых площадках в 2020 году цены на доступ по RDP различаются: глобальный административный доступ стоит $10, а взломанный RDP — $35.

Между тем, по словам исследователей, цены на DDoS-сервисы, растут с 2017 года. Тогда как в 2017 году стандартные предложения DDoS-наемников редко превышали $27, в 2020 году 10-минутная DDoS-атака (60 Гбит/с) стоит $45, а четырехчасовая DDoS-атака (15 Гбит/с) в среднем стоит $55. Цена на полностью управляемую DDoS-атаку составляет $165. По словам исследователей, повышение цен связано с несколькими факторами.

«Во-первых, отключение более крупных web-сайтов должно производиться по индивидуальному заказу из-за улучшений в предложениях по защите от DDoS-атак и широкого использования сетей распространения контента, что выходит за рамки возможностей всех, кроме самых продвинутых преступников. Однако все еще есть случаи, когда злоумышленники могут успешно атаковать крупные ресурсы, например, отключение Википедии с помощью DDoS-атаки в сентябре 2019 года».

По их словам, DDoS-сервисы, взимающие почасовую оплату, также становятся все более популярными.

Стоимость конфиденциальных данных для выполнения мошеннических схем и проведения автоматических кибератак снова растет. Например, стоимость записи так называемых «дампов» платежных карт, то есть полной информации о карте с 2018 года увеличилась на 225%. Высокий спрос на украденные личные данные также включает списки «Fullz», которые содержат различные комбинации идентификационных и банковских данных, таких как банковские журналы, номера маршрутизации, платежные карты, удостоверения личности государственного образца, а также личную информацию, включая записи номеров социального страхования или даты рождения». ***(В даркнете растут цены на доступ через RDP, DDoS-атаки и данные платежных карт // SecurityLab.ru (https://www.securitylab.ru/news/515059.php). 23.12.2020).***

***

«Федеральная торговая комиссия США выполняет резолюцию об усилении защиты от недостатков безопасности, возникающих при транзакциях электронной торговли. Недавние действия агентства, связанные с обвинениями в неправомерных действиях провайдера телеконференцсвязи Zoom Video Communications, являются ярким примером.

В соглашении с Zoom FTC наложила на компанию весьма специфические требования в отношении вопросов безопасности и конфиденциальности, связанных с услугами Zoom. Мировое соглашение 13 ноября 2020 года стало официальным после того, как период комментариев истек в середине декабря.

FTC заявила, что соглашение с Zoom требует, чтобы компания «внедрила надежную программу информационной безопасности, чтобы уладить обвинения в том, что провайдер видеоконференцсвязи участвовал в ряде обманных и недобросовестных действий, которые подорвали безопасность его пользователей».

Zoom не признал и не опроверг утверждения Комиссии о принятии решения.

Широкий эффект пульсации электронной коммерции

Что немаловажно в мире электронной коммерции, действия Комиссии по делу Zoom отражали больше, чем внутреннюю политику по усилению правоприменения в вопросах электронной коммерции. Согласно анализу дела Клири Готтлиб, действия FTC также отражали решение федерального суда, которое привело к тому, что Комиссия решила принять более жесткие и целенаправленные принудительные меры по сравнению с более общими требованиями соответствия .

Кроме того, влияние действий FTC выходит далеко за рамки приложений для услуг видеоконференцсвязи и влияет на широкий спектр операций электронной коммерции. «Решение Zoom абсолютно применимо в широком смысле, - сказала Кэтлин Бенуэй, партнер Alston and Bird. Решение Федеральной торговой комиссии «предлагает уроки любой компании, которая собирает личную информацию потребителей в электронном виде. Таким компаниям было бы разумно внимательно изучить жалобу Zoom и принять меры, чтобы их системы и процессы не вызывали подобных проблем», - сказала она E- Commerce Times.

Специфика утверждений FTC по делу Zoom дает некоторое представление о типах транзакций электронной торговли, которые вызывают озабоченность Комиссии и могут повлиять на исполнение.

В своей жалобе FTC сообщила, что по крайней мере с 2016 года Zoom вводила клиентов в заблуждение, утверждая, что предлагает «сквозное 256-битное шифрование» для защиты коммуникаций пользователей, «хотя на самом деле это обеспечивает более низкий уровень безопасности. Сквозное шифрование - это метод защиты связи, так что только отправитель и получатель - и никто, даже поставщик платформы - не может прочитать контент, пояснила FTC.

По заявлению FTC, Zoom сохранил криптографические ключи, которые фактически могли позволить компании получить доступ к содержимому собраний своих клиентов, и частично защищал свои телеконференции с помощью более низкого уровня шифрования, чем обещал. В апреле 2020 года Zoom признал, что его услуги, как правило, не поддерживают сквозное шифрование, согласно анализу случая, проведенному Олстоном и Берд.

Согласно жалобе FTC, Zoom также ввел в заблуждение некоторых пользователей, которые хотели хранить записанные встречи в облачном хранилище компании, ложно заявив, что эти встречи были зашифрованы сразу после окончания встречи. Вместо этого некоторые записи якобы хранились в незашифрованном виде до 60 дней на серверах Zoom, прежде чем были перенесены в его безопасное облачное хранилище.

Кроме того, Zoom развернул рабочий механизм, связанный с браузером Apple Safari, который FTC охарактеризовал как метод, позволяющий обойти меры безопасности и конфиденциальности Safari без надлежащего уведомления или согласия пользователя. Комиссия утверждала, что размещение было несправедливым действием или практикой.

Расчет требует принятия нескольких мер по обеспечению соответствия

По данным FTC, Zoom согласился разработать и внедрить комплексную программу безопасности и соблюдать другие подробные меры для защиты своей пользовательской базы, которая резко выросла с 10 миллионов пользователей в декабре 2019 года до 300 миллионов в апреле 2020 года во время пандемии COVID-19. . В рамках урегулирования Zoom будет:

ежегодно оценивать и документировать любые потенциальные внутренние и внешние риски безопасности и разрабатывать способы защиты от таких рисков;

реализовать программу управления уязвимостями; и

развернуть меры безопасности, такие как многофакторная аутентификация, для защиты от несанкционированного доступа к своей сети; установить контроль удаления данных; и принять меры для предотвращения использования известных скомпрометированных учетных данных пользователя.

Кроме того, персонал Zoom должен будет проверять любые обновления программного обеспечения на предмет недостатков безопасности и должен гарантировать, что обновления не будут мешать сторонним функциям безопасности, как это произошло с механизмом Apple Safari.

Мировое соглашение также запрещает компании искажать информацию о своей политике конфиденциальности и безопасности, в том числе о том, как она

собирает, использует, поддерживает или раскрывает личную информацию; его защитные функции; и степень, в которой пользователи могут контролировать конфиденциальность или безопасность своей личной информации.

В ответ на мировое соглашение компания заявила, что «безопасность наших пользователей является главным приоритетом для Zoom».

«Мы серьезно относимся к тому доверию, которое наши пользователи испытывают к нам каждый день, особенно потому, что они рассчитывают, что мы будем поддерживать их связь во время этого беспрецедентного глобального кризиса, и мы постоянно совершенствуем наши программы безопасности и конфиденциальности. Мы гордимся достижениями, которые мы сделали для наша платформа, и мы уже рассмотрели проблемы, выявленные FTC. Наше решение с FTC соответствует нашему стремлению к инновациям и усовершенствованию нашего продукта, поскольку мы обеспечиваем безопасную видеосвязь», - говорится в ответе компании. пресс-секретарь Келси Маркович, газета E-Commerce Times.

FTC будет сохранять бдительность в отношении безопасности и конфиденциальности

Решение Zoom явно указывает на более агрессивную позицию FTC в области правоприменения. «Я думаю, что FTC удвоит свое внимание на обеспечении конфиденциальности и безопасности данных во многих отраслях и компаниях», - сказал Алексис Коллинз, партнер Cleary Gottlieb.

«В последние годы агентство приняло меры против различных типов компаний, которые собирают или обрабатывают данные о потребителях или проводят деятельность в области электронной коммерции, за предполагаемые недостатки в соблюдении их политики конфиденциальности или реализации разумных мер кибербезопасности, независимо от того, сталкиваются ли эти компании напрямую потребителей», - сказал Коллинз E-Commerce Times.

Например, FTC достигла взаиморасчетов с рядом компаний, производящих потребительские товары или услуги, такими как Equifax и Uber, и сторонними поставщиками услуг, такими как InfoTrax, сказала она.

Еще одним сигналом того, что FTC продолжит агрессивную позицию по вопросам конфиденциальности и безопасности, стали комментарии двух нынешних членов комиссии к заключениям, которые они подали по делу. Каждый предположил, что агентство должно было занять еще более жесткую позицию принуждения к урегулированию Zoom.

Согласно сообщению Клири Готтлиб Коллинз, комиссар Рохит Чопра выразил обеспокоенность тем, что в соглашении отсутствуют положения о значимом возмещении ущерба для тех пользователей, которым нанесен ущерб из-за искажений со стороны Zoom, таких как договорные релизы, возмещения или кредиты для малых предприятий, которые приобрели услуги Zoom на основе ложных заявлений., не требовали уведомления затронутых пользователей и отсутствовали денежные штрафы.

Комиссар Ребекка Слотер предположила, что «более эффективный приказ» потребовал бы от Zoom пересмотреть риски, которые ее продукты и услуги представляют для конфиденциальности потребителей в дополнение к безопасности, согласно анализу дела Алстона и Берда». ***(John K. Higgins. FTC's***

Zoom Deal Signals Commitment to Security Enforcement // ECT News Network, Inc (https://www.technewsworld.com/story/86962.html). 29.12.2020).

***

«Google, Microsoft, Cisco Systems и другие хотят, чтобы апелляционный суд отказал израильской компании в иммунитете за предполагаемое распространение шпионского ПО и незаконную деятельность по кибер-слежке.

WhatsApp, дочерняя компания Facebook, получила новую поддержку высокого уровня в своем деле против израильской разведывательной компании NSO Group. Судебное дело направлено на привлечение NSO Group к ответственности за распространение своего шпионского ПО Pegasus в популярной службе обмена сообщениями WhatsApp с целью установки его шпионского ПО на телефоны журналистов и правозащитников.

Группа компаний, в которую входят технологические гиганты Google, Microsoft и Cisco Systems, подали юридическое заключение под названием amicus, чтобы поддержать WhatsApp против предполагаемой незаконной деятельности NSO по кибер-слежке, включая продажу «кибер-слежки как услуги» иностранным правительствам и другим лицам. компании. VMWare и GitHub также подписали бриф вместе с LinkedIn - дочерней компанией Microsoft - и Internet Association, которая представляет десятки технологических компаний, включая Amazon, Facebook и Twitter.

Между тем, Electronic Frontier Foundation (EFF) подал Amicus краткое своей собственной поддержки WhatsApp, утверждая, что дело это не просто битва технологических компаний, но есть потенциальный результат, который будет иметь «серьезные последствия для миллионов пользователей Интернета и другие граждане стран мира»

Трусы Amicus в юридическом выражении известны как amicus curiae, что в переводе с латыни означает «друг суда». Краткие сводки обычно используются в апелляционных делах, чтобы указать или предоставить новую информацию, которую основные участники судебного процесса, возможно, не рассмотрели.

В данном случае краткие сводки нацелены на оказание поддержки WhatsApp, чтобы убедить Апелляционный суд девятого округа США привлечь к ответственности NSO за свою деятельность. Текущий случай перед судом является обращением за иммунитет, что НСУ подал после того, как федеральный судья разрешил костюм WhatsApp первоначально поданный в октябре 2019 года, чтобы двигаться вперед в начале этого года.

Президент NSO Шири Долев защитила компанию, заявив, что она должна быть защищена от судебных исков, поскольку она продает свои инструменты правительствам и правоохранительным органам, которые используют их, чтобы преследовать преступников и находить жертв стихийных бедствий, среди других благотворительных мероприятий.

Технологические компании и первоначального судью по делу пока не убедили этот аргумент. «Даже если инструменты продаются правительствам, которые используют их для узконаправленных атак, существует множество

способов, которыми они могут попасть в чужие руки», - сказал в блоге Том Берт, корпоративный вице-президент Microsoft по безопасности и доверию клиентов. пост опубликован в понедельник в поддержку amicus.

«Расширение суверенного иммунитета, к которому стремится NSO, будет способствовать дальнейшему стимулированию растущей индустрии кибер-наблюдения к разработке, продаже и использованию инструментов для эксплуатации уязвимостей в нарушение законодательства США», - написал он. «Частные компании должны по-прежнему нести ответственность, когда они используют свои инструменты кибер-наблюдения для нарушения закона или сознательно разрешают их использование для таких целей, независимо от того, кто их клиенты или чего они пытаются достичь».

EFF, которая часто сталкивается с технологическими компаниями из-за проблем с конфиденциальностью, в данном случае совпадает с ними против NSO.

«Соучастие корпораций в нарушениях прав человека является широко распространенной и постоянной проблемой, и Девятый округ не должен расширять возможности технологических компаний, таких как NSO Group, избегать ответственности за содействие нарушениям прав человека иностранными правительствами», - говорят старшие юристы EFF София Коуп и Эндрю Крокер написал в блоге, также опубликованном в понедельник, относительно amicus EFF.

В первоначальном случае WhatsApp подал в суд на NSO Group за якобы создание таких инструментов, как Pegasus, чтобы ее клиенты могли шпионить и читать защищенные сообщения WhatsApp журналистов и правозащитников. Дело связано с обнаружением в мае 2019 года уязвимости нулевого дня в платформе обмена сообщениями WhatsApp, которой воспользовались злоумышленники, которые смогли внедрить шпионское ПО Pegasus на телефоны жертв в ходе целевых кампаний.

В иске утверждается, что NSO Group разработала код слежки и использовала уязвимые серверы WhatsApp для отправки вредоносного ПО примерно на 1400 мобильных устройств, в том числе на устройства более 100 правозащитников, журналистов и других представителей гражданского общества как минимум в 20 странах мира.

«Когда мы собрали информацию, которую изложили в нашей жалобе, мы узнали, что злоумышленники использовали серверы и услуги интернет-хостинга, которые ранее были связаны с NSO», - сказал Уилл Кэткарт, глава WhatsApp, в сообщении, когда был подан иск. «Кроме того, как отмечается в нашей жалобе, мы связали некоторые учетные записи WhatsApp, использованные во время атак, с NSO. Хотя их атака была очень изощренной, их попытки замести следы не увенчались успехом».

WhatsApp утверждает, что атака нарушает различные законы штата и федеральные законы США, в том числе Закон США о компьютерном мошенничестве и злоупотреблениях, и направлена в иске, чтобы запретить NSO Group использовать сервисы Facebook и WhatsApp, а также требовать возмещения другого неуказанного ущерба». ***(Elizabeth Montalbano. Tech Giants Lend WhatsApp Support in Spyware Case Against NSO Group // Threatpost***

(https://threatpost.com/tech-giants-lend-whatsapp-support-in-spyware-case-against-nso-group/162552/). 22.12.2020).

***

«18 декабря семь штатов заключили мировое соглашение с интернет-магазином Cafe-Press на 2 миллиона долларов в результате утечки данных в 2019 году, в результате которой была раскрыта информация примерно 22 миллионов потребителей. Нарушение затронуло личную информацию потребителей, включая имена пользователей и пароли, номера социального страхования и / или идентификационные номера налогоплательщиков.

Из 2 миллионов долларов 750 000 долларов будут незамедлительно разделены между штатами: Нью-Джерси, Нью-Йорк, Коннектикут, Индиана, Кентукки, Мичиган и Орегон.

Согласно мировому соглашению, если CafePress улучшит свои методы обеспечения конфиденциальности данных, штаты согласились приостановить урегулирование баланса. Эти улучшения включают реализацию комплексной программы кибербезопасности, которая регулярно обновляется и оценивается, план уведомления о взломе данных (включая подготовку, обнаружение, анализ, локализацию, искоренение и восстановление), а также другие меры безопасности, такие как шифрование, сегментация и тестирование на проникновение. CafePress также должен обновлять информацию, раскрываемую потребителям, включая информацию о закрытии учетной записи и удалении данных. Компания также должна иметь стороннюю оценку рисков на следующие пять лет». ***(KATHRYN RATTIGAN. CafePress to Pay $2 Million in Multi-State Data Breach Settlement // Robinson+Cole (https://www.dataprivacyandsecurityinsider.com/2020/12/cafepress-to-pay-2-million-in-multi-state-data-breach-settlement/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+DataPrivacyAndSecurityInsider+%28Data+Privacy+%2B+Security+Insider%29). 23.12.2020).***

***

Кібербезпека Інтернету речей

«Многие в настоящее время управляют отоплением, освещением и развлечениями своего дома с помощью смартфона или голоса. В течение следующего десятилетия почти каждое новое устройство будет иметь постоянное подключение к Интернету. Цифровое преобразование повседневной жизни можно найти во всем, от тостеров до дверных звонков.

Благодаря смарт-часам, привязанным к нашим запястьям, отслеживающим нашу частоту сердечных сокращений, и смартфону в нашей руке, отслеживающему каждое наше общение и местоположение в режиме реального времени, многие из них уже являются полностью подписанными участниками сетевого образа жизни.

По мере того как предприятия и власти стремятся не отставать от наших растущих ожиданий, они могут создавать больше проблем, чем решений в нашей жизни.

Конец быстрого движения и ломки вещей

Проблема с миссией Кремниевой долины по быстрому движению и разрушению заключается в том, что она не может определить серьезные последствия, которые она создает на своем пути. Компании, у которых до сих пор остались шрамы от борьбы с BYOD и теневой ИТ, теперь можно увидеть, как они борются с угрозами, которые устройства Интернета вещей принесли в их корпоративную сеть.

Однако существующие проблемы даже шире, чем социальные последствия, этические обязанности и защита бизнеса от заложников программ- вымогателей. Мы только начинаем понимать, как создаются опасные или смертельные ситуации, когда наша критически важная инфраструктура работает.

Приводя все в сеть, не создаем ли мы невольно уязвимости в нашей критически важной инфраструктуре и в том месте, где мы живем?

Программа-вымогатель Ryuk нацелена на больницы

Больницы все чаще борются с кибератаками, которые угрожают лечению пациентов в период увеличения количества госпитализаций из-за COVID-19. В Германии уже обвинили компьютерный вирус в смерти пациента. Недобросовестные киберпреступники могут атаковать все, начиная с аппаратов МРТ, аппаратов ИВЛ и даже подключенных микроскопов.

В мире, где еще не было ковидов, еще в 2017 году именно атака программы-вымогателя WannaCry стала глобальной эпидемией. Было заражено более 400 000 компьютеров как минимум в 150 странах на сумму около 4 миллиардов долларов. Ryuk последовал за ним и впервые появился в августе 2018 года, но он был основан на более старой программе под названием Hermes и продолжал развиваться в виртуальной игре в кошки-мышки с охранными фирмами.

Метод доставки Ryuk заключался в фишинговых письмах, содержащих ссылки на зараженные документы Google Диска. Ничего не подозревающие пользователи устанавливали на свой компьютер вредоносное ПО. Но атаки продолжают менять тактику, и неизбежный отказ от файлов, размещенных на дисках Google, затруднит предприятиям освоение новых методов проведения атак.

В октябре ФБР предупредило отрасль здравоохранения, что программы-вымогатели, такие как Ryuk, по-прежнему активно атакуют весь сектор общественного здравоохранения.

Критическая инфраструктура под атакой

Агентство по кибербезопасности и безопасности инфраструктуры (CISA) сообщило, что 16 секторов, включая государственные объекты, атомную энергетику, транспорт и водные системы, являются целями для злоумышленников. Угрозы растут параллельно с нашей растущей зависимостью от удаленной работы и устройств IoT.

Погружение городов в темноту стало реальностью, когда в 2015 году на украинскую энергосистему была совершена атака. Совсем недавно в США оператор природного газа был вынужден отключиться после заражения программой-вымогателем. И снова комбинация фишинговых писем и сбоев в

системе безопасности позволила злоумышленникам переключиться с ИТ-сети объекта на сеть ОТ объекта.

Морской транспорт США и два города во Флориде также оказались заложниками программ-вымогателей.

По мере роста глобальной напряженности кибератаки на правительства, спонсируемые государством, будут продолжать использовать уязвимости национальной инфраструктуры и рискуют стать нормой.

Очень необходимый звонок для пробуждения

Проблемы теперь намного серьезнее, чем ощущение, что ваш умный дом вас предал. По данным Microsoft, многие компании в этом году втиснули два года реализации инициатив по цифровой трансформации всего в несколько месяцев. Целые города и страны только начинают осознавать уязвимости, создаваемые быстрым движением, без учета возможных последствий для безопасности в будущем.

Как и ожидалось, рынок защиты критически важной инфраструктуры ожидает экспоненциального роста в течение следующих пяти лет. Но куда мы идем отсюда? Многие невольно создали гораздо большую поверхность угрозы, вторгаясь туда, что также привело к непредвиденным последствиям и уязвимостям.

Мы знаем, что предпочтительный метод доставки атаки обычно осуществляется через зараженные ссылки, веб-сайты и вложения электронной почты. Компаниям и тем, кто управляет критически важной инфраструктурой, нужно не только ставить галочки каждые 12 месяцев, чтобы соответствовать требованиям. Непрерывное образование имеет важное значение для защиты от нарушений безопасности и киберпреступности.

Достаточно ли признать, что спонсируемые государством кибератаки являются одной из самых серьезных угроз в 2021 году, чтобы окончательно развеять мифы, связанные с программами-вымогателями? Создавая культуру безопасности в сочетании с реактивными и проактивными мерами противодействия, руководители могут начать устранять уязвимости в цифровом мире, который постоянно подвергается атакам». ***(Neil C. Hughes. Why ransomware is the biggest threat to our critical infrastructure // CyberNews Investigation (https://cybernews.com/security/why-ransomware-is-the-biggest-threat-to-our-critical-infrastructure/). 03.12.2020).***

***

«Возможности искусственного интеллекта растут, и легко забыть, что его защита несовершенна. Однако ученые выяснили, что уязвимостью ИИ могут воспользоваться даже другие алгоритмы. В результате злоумышленник может повлиять на работу автономной системы вождения, программы интеллектуального анализа текста или компьютерного зрения. Вот как технологии помогают бизнесу обезопасить программы искусственного интеллекта.

В сентябре 2019 года Национальный институт стандартов и технологий США опубликовал свое первое в истории предупреждение об атаке на коммерческий алгоритм искусственного интеллекта.

Аналитики в сфере информационной безопасности определили, что целью стала программа Proofpoint, которая использует машинное обучение для определения спам-рассылок. Система создавала заголовки писем и присваивала им оценку вероятности того, что сообщение было спамом. Однако анализируя эти оценки и содержание писем, алгоритм смог создать клон модели машинного обучения и создавать рассылки, которые не могли быть обнаружены.

Возможно, за этим сообщением последуют и многие другие. По мере распространения ИИ появляются и новые возможности для использования его уязвимостей. Это привело к появлению компаний, которые ищут слабые места в алгоритмах, чтобы заметить вредоносные действия до того, как они нанесут ущерб.

Этим занимается и стартап Robust Intelligence. Его сооснователь и CEO Ярон Сингер — профессор Гарварда, который руководит компанией во время творческого отпуска в Сан-Франциско. Его программа использует ИИ, чтобы обойти алгоритм, считывающий чеки.

Она автоматически настраивает интенсивность пикселей, из которых состоят цифры и буквы на чеке.

Это меняет данные, которые поступают в распространенный коммерческий алгоритм проверки-сканирования.

С таким инструментом мошенник может опустошить банковский счет жертвы. Например, он меняет законный чек, добавляя в него несколько нулей.

Сингер рассказывает: «Во многих приложениях даже небольшие изменения могут привести к совершенно разным результатам. Но проблема еще глубже: суть в том, как выполняется машинное обучение».

Технология Robust Intelligence используется такими компаниями, как PayPal и NTT Data, а также крупной райдшеринговой компанией. Сингер предупреждает, что не может описать, как именно она применяется, чтобы об этом не узнали потенциальные мошенники.

Компания продает два инструмента: программу для поиска слабых мест в алгоритме и ИИ-брандмауэр, алгоритм, который автоматически выявляет потенциально уязвимые места. Поисковый инструмент может запускать алгоритм много раз, исследуя входы и выходы и ища способы обмануть его.

Такие угрозы носят не только теоретический характер. Исследователи показали, что враждебные алгоритмы могут обмануть реальные ИИ-системы, в том числе автономные системы вождения, программы интеллектуального анализа текста и коды компьютерного зрения. В одном из часто упоминаемых примеров группа студентов Массачусетского технологического института напечатала на 3D-принтере черепаху, которую программа Google распознала как винтовку из-за тонких отметин на поверхности.

«Если вы разрабатываете модели машинного обучения, то у вас нет возможности имитировать реальную кибератаку или провести тест на проникновение», — говорит Сингер.

Задача исследования Сингера — изменить входные данные системы машинного обучения таким образом, чтобы она вела себя некорректно, и разрабатывать системы, которые будут безопасны. Обман ИИ основан на том, что они учатся на примерах и улавливают тонкие изменения, на что не способны люди.

Для этого могут использоваться несколько тщательно подобранных наборов входных данных. Например, системе распознавания лиц показывают измененные лица. Исходя из ее реакции, враждебный алгоритм может определить, какие настройки вызовут ошибку или конкретный результат.

Кроме системы проверки, Сингер демонстрирует способ перехитрить систему обнаружения мошенничества в интернете в рамках поиска слабых мест. Эта мошенническая система ищет признаки того, что кто-то, совершающий транзакцию, на самом деле является ботом. Для этого используется широкий спектр характеристик, включая браузер, операционную систему, IP-адрес и время.

Сингер также показывает, как технология его компании может обмануть коммерческие системы распознавания изображений и лиц с помощью тонких настроек фотографии. Система распознавания лиц приходит к выводу, что немного измененная фотография Биньямина Нетаньяху на самом деле показывает баскетболиста Джулиуса Барнса. Сингер демонстрирует эти же функции потенциальным клиентам, которые беспокоятся, что кто-то может повлиять на работу их алгоритмов и это навредит их репутации.

Некоторые крупные компании, использующие ИИ, начинают разрабатывать свои собственные алгоритмы защиты. Например, у Facebook есть собственная команда для кибератак, которая пытается взломать внутренние системы и выявить слабые места.

Зико Колтер, главный научный сотрудник Центра искусственного интеллекта Bosch, говорит, что исследования по защите ИИ все еще находятся на ранней стадии. Немецкая компания обратилась к Колтеру, адъюнкт-профессору Университета Карнеги — Меллона, чтобы удостовериться в надежности ее алгоритмов, некоторые из которых используются в автомобилестроении. Колтер говорит, что большинство усилий по защите коммерческих систем направлены на предотвращение атак, а не на обеспечение их надежности.

В октябре 2020 года Bosch и еще 11 компаний, среди которых Microsoft, Nvidia, IBM и MITRE, выпустили программы для поиска уязвимостей в системах ИИ.

По прогнозу Gartner, к 2022 году 30% кибератак на ИИ будут использовать алгоритмы искусственного интеллекта.

Александр Мадри, адъюнкт-профессор Массачусетского технологического института, работающий над машинным обучением, говорит, что до сих пор не ясно, как гарантировать безопасность систем искусственного интеллекта. Он добавляет, что уязвимости отражают более фундаментальную слабость современного ИИ. Но повышение надежности алгоритмов может также улучшить их интеллект. Согласно статье, написанной Мадри и его коллегами, которая будет представлена на конференции в конце этого месяца, алгоритмы распознавания образов, способные противостоять атакам, также можно эффективнее применить к новым задачам, что делает их более полезными.

Необычный способ работы ИИ не только делает их уязвимыми для атак, но и означает, что они могут подвести самым неожиданным образом.

Это, скорее всего, приведет к проблемам в таких областях, как медицинская визуализация и финансы, говорит Мадри. «Модели ИИ — очень прилежные

студенты, и они сделают все возможное, чтобы решить узкую проблему. Каждая компания, использующая ИИ, должна думать об этом». ***(Елена Лиханова. Битва интеллектов: как ИИ используется для борьбы с вредоносными алгоритмами // ООО "РБ.РУ" (https://rb.ru/story/ai-vs-ai/). 07.12.2020).***

***

«4 декабря был подписан Закон о повышении кибербезопасности Интернета вещей от 2020 года, в результате чего был принят первый федеральный регламент Интернета вещей (IoT).

IoT относится к системе подключенных к Интернету устройств - «вещей», которые обмениваются данными по беспроводным сетям; Закон определяет Интернет вещей как «расширение возможности подключения к Интернету на физические устройства и повседневные предметы». Интернет вещей пронизывает все сектора и отрасли, включая коммерческие и правительственные, с акцентом на использование устройств Интернета вещей федеральными правительственными учреждениями.

Использование устройств Интернета вещей быстро растет, как и общие проблемы, связанные с конфиденциальностью и безопасностью. Решая эти проблемы, закон призван «установить минимальные стандарты безопасности для устройств Интернета вещей, принадлежащих или контролируемых федеральным правительством, а также для других целей».

Глобальная перспектива

Морган Льюис ранее сообщал об одном из предшественников закона - Калифорнийском Законе об улучшении кибербезопасности Интернета вещей от 2017 года . Закон штата Калифорния 2017 года, вступивший в силу 1 января 2020 года, стал первым законом об Интернете вещей, принятым на уровне штата и предусматривающим «разумную» и «надлежащую» кибербезопасность Интернета вещей.

По другую сторону Атлантики Агентство по кибербезопасности Европейского союза также опубликовало различные рекомендации и руководства по безопасности Интернета вещей. После успешных консультаций по вопросам безопасности IoT в феврале 2020 года правительство Соединенного Королевства приняло правила кибербезопасности IoT.

Акт

Федеральный закон предписывает действия, которые должны быть предприняты Национальным институтом стандартов и технологий (NIST) и Управлением по управлению и бюджету (OMB) в отношении использования устройств Интернета вещей федеральными правительственными учреждениями. Это требует, чтобы NIST и OMB предприняли определенные шаги для повышения кибербезопасности в отношении таких устройств IoT:

Закон требует от NIST «разрабатывать и публиковать стандарты и руководящие принципы для федерального правительства по надлежащему использованию и управлению агентствами устройств IoT, принадлежащих агентству или контролируемых им и связанных с информационными системами, принадлежащими или контролируемыми агентством, включая минимальную

информационную безопасность. требования по управлению рисками кибербезопасности, связанными с такими устройствами».

Закон также требует, чтобы OMB проверял политику и принципы информационной безопасности агентства на основе стандартов и руководств NIST и издавал такие политики и принципы, которые необходимы для обеспечения того, чтобы политика и принципы агентства соответствовали стандартам и руководствам NIST.

NIST должен будет пересматривать и при необходимости пересматривать стандарты и руководства каждые пять лет.

Закон также требует, чтобы NIST разработал и опубликовал инструкции для агентств, подрядчиков и субподрядчиков, касающиеся уязвимостей безопасности.

Наконец, закон требует, чтобы не позднее декабря 2022 года директор OMB разработал и контролировал реализацию политик, принципов, стандартов или руководств, которые могут потребоваться для устранения уязвимостей безопасности применимых устройств IoT.

На момент публикации этого поста неясно, как NIST будет вводить в действие или реализовывать соответствующие руководящие принципы.

Закон довольно узок по своему охвату. Он уполномочивает NIST устанавливать стандарты кибербезопасности для устройств IoT, но не устанавливает минимального порога для таких стандартов, и эти стандарты применимы только к федеральным правительственным учреждениям. Тем не менее, вполне вероятно, что в цепочке поставок будет эффект просачивания, и, в любом случае, этот закон создаст прецедент для частного сектора, сигнализируя о более жестком обеспечении соблюдения и регулирования IoT в будущем». ***(VITO PETRETTI, OLIVER BELL. The Internet of Things Cybersecurity Improvement Act of 2020: IoT Goes Federal // Morgan, Lewis & Bockius LLP (https://www.morganlewis.com/blogs/sourcingatmorganlewis/2020/12/the-internet-of-things-cybersecurity-improvement-act-of-2020-iot-goes-federal). 17.12.2020).***

***

Кіберзлочинність та кібертероризм

«Американська компанія з кібербезпеки FireEye заявила, що постраждала від хакерської атаки, яку підтримувала "держава, що має значні наступальні можливості"…

Хакери зламали мережу та вкрали інструменти, що використовували для тестування безпеки клієнтів. У FireEye не впевнені, що саме зловмисники збираються робити з отриманими даними: використовувати чи розкрити. Тому компанія розробила понад 300 контрзаходів, щоб захистити клієнтів.

Гендиректор компанії Кевін Мандіа зазначив, що зловмисники використовували нову комбінацію технік, з якими FireEye та її партнери раніше не стикалися.

За попередніми даними, хакери фінансувалися іноземною державою. Якою саме - не вказується. Наразі триває розслідування хакерської атаки разом із ФБР. У

бюро також підтвердили, що характер атаки свідчить про підтримку іноземної держави.

Що це за іноземна держава?

Офіційно ще не називали країну, яка може стояти за атаками, проте джерела Business Insider заявляють, що йдеться про Росію. Так, два співробітники європейської розвідки підтвердили, що хакерів підтримує Росія, цю інформацію передали американським колегам ще до того, як FireEye зробила офіційну заяву про злам.

Анонімний представник НАТО заявив, що вкрадені дані "можуть бути корисними для Головного розвідувального управління РФ, Федеральної служби безпеки РФ та для будь-кого іншого". На думку європейського розвідника, найбільшою перемогою Росії є те, що вона отримала доступ до даних своїх ворогів.

Компанія FireEye розслідувала кібератаки на енергосистему України у 2015-2016 роках. Тоді компанія визначила Росію як відповідальну за багато хакерських атак, зокрема і за атаку на Україну». ***(Компанія з кібербезпеки FireEye заявила про хакерську атаку з боку іноземної держави. Імовірно, це Росія // iPress (https://ipress.ua/news/kompaniya_z_kiberbezpeky_fireeye_zayavyla_pro_hakersku_ataku_z_boku_inozemnoi_derzhavy_imovirno_tse_rosiya_316805.html). 10.12.2020).***

***

«Кибер-исследователи из Университета Бен-Гуриона в Негеве обнаружили непрерывную кибербиологическую атаку, в ходе которой невольных биологов могут обмануть и заставить генерировать опасные токсины в своих лабораториях.

Согласно новой статье, только что опубликованной в Nature Biotechnology, в настоящее время считается, что преступнику необходимо физически контактировать с опасным веществом, чтобы произвести и доставить его. Однако вредоносное ПО может легко заменить короткую подстроку ДНК на компьютере биоинженера, так что они непреднамеренно создают последовательность, производящую токсин.

«Чтобы регулировать как преднамеренное, так и непреднамеренное производство опасных веществ, большинство поставщиков синтетических генов проверяют порядки ДНК, что в настоящее время является наиболее эффективной линией защиты от таких атак», - говорит Рами Пузис, руководитель лаборатории анализа сложных сетей BGU, член Департамент разработки программного обеспечения и информационных систем и Cyber @ BGU. Калифорния была первым штатом в 2020 году, принявшим закон о регулировании покупки генов.

«Однако за пределами штата биотеррористы могут покупать опасную ДНК у компаний, которые не проверяют заказы», - говорит Пузис. «К сожалению, рекомендации по скринингу не были адаптированы с учетом последних достижений в синтетической биологии и кибервойне».

Недостаток в руководстве Министерства здравоохранения и социальных служб США (HHS) для поставщиков ДНК позволяет обходить протоколы скрининга с помощью стандартной процедуры обфускации, что затрудняет программному обеспечению скрининга обнаружение ДНК, вырабатывающей

токсин. «Используя эту технику, наши эксперименты показали, что 16 из 50 обфускированных образцов ДНК не были обнаружены при скрининге в соответствии с рекомендациями HHS «наилучшего соответствия», - говорит Пузис.

Исследователи также обнаружили, что доступность и автоматизация рабочего процесса синтетической генной инженерии в сочетании с недостаточным контролем кибербезопасности позволяют вредоносному ПО вмешиваться в биологические процессы в лаборатории жертвы, замыкая цикл с возможностью использования эксплойта, записанного в молекулу ДНК.

Атака с использованием ДНК-инъекции демонстрирует новую значительную угрозу изменения биологических процессов вредоносным кодом. Хотя существуют более простые атаки, которые могут нанести вред биологическим экспериментам, мы решили продемонстрировать сценарий, в котором используются многочисленные слабые места на трех уровнях рабочего процесса биоинженерии: программное обеспечение, скрининг биобезопасности и биологические протоколы. Этот сценарий подчеркивает возможности применения ноу-хау в области кибербезопасности в новых контекстах, таких как биозащита и генное кодирование.

«Этот сценарий атаки подчеркивает необходимость усиления цепочки поставок синтетической ДНК с помощью защиты от кибербиологических угроз», - говорит Пузис. «Для устранения этих угроз мы предлагаем улучшенный алгоритм скрининга, который учитывает редактирование генов in vivo. Мы надеемся, что эта статья подготовит почву для надежного и устойчивого к противодействию скрининга последовательностей ДНК и услуг по производству синтетических генов с усиленной кибербезопасностью, когда скрининг биобезопасности будет осуществляться в соответствии с местными законами во всем мире». ***(Staff Writer. New Cyberattack Can Trick Scientists Into Making Dangerous Toxins or Synthetic Viruses // MITechNews.com (https://mitechnews.com/cyber-defense/new-cyberattack-can-trick-scientists-into-making-dangerous-toxins-or-synthetic-viruses/). 06.12.2020).***

***

«Компания «Elcore Украина», официальный дистрибьютор Trend Micro, сообщила результаты опроса, согласно которому за последний год 23% организаций по всему миру подверглись семи или более атакам, завершившимся проникновением в их сети или системы. Подавляющее большинство (83%) опрошенных организаций считают, что существует «некоторая» или «высокая» вероятность успешной атаки в ближайшие 12 месяцев.

Американская исследовательская организация Институт Понемона (Ponemon Institute) опубликовала последнюю версию Индекса киберрисков Trend Micro (Cyber Risk Index — CRI; www.trendmicro.com/cyberrisk), для расчёта которого измеряется разница между текущим уровнем безопасности организации и вероятностью подвергнуться атаке.

«CRI быстро становится незаменимым инструментом для руководителей подразделений по информационной безопасности, предоставляя им данные для оценки готовности организации противостоять кибератаке, — говорит Джон Клэй

(Jon Clay), директор отдела информирования о глобальных угрозах Trend Micro. — В этом году мы добавили данные по Европе и Азиатско-Тихоокеанскому региону, чтобы можно было представить поистине глобальную картину. Это поможет организациям во всем мире найти более эффективные способы упрощения работы, снижения угроз от действий инсайдеров и из-за нехватки навыков, а также повысить уровень безопасности облачных сред и в результате минимизировать киберриски и поддержать быстрое восстановление после пандемии».

Индекс CRI представляет собой числовую шкалу от –10 до 10, где –10 — наивысший уровень риска. Текущий глобальный индекс составляет –0,41, что соответствует «повышенному» риску. Наиболее высокий риск зафиксирован в США (–1,07) из-за недостаточной готовности систем защиты от кибератак по сравнению с другими регионами.

По мнению организаций, главными киберрисками в мире являются:

фишинг и социальная инженерия;

кликджекинг;

программы-вымогатели;

бесфайловые атаки;

ботнеты;

атаки типа man-in-the-middle (связанные с перехватом канала связи).

Наибольшую тревогу у организаций по всему миру вызывают:

потеря данных клиента;

доступ к финансовой информации;

потеря клиентов;

кража или повреждение оборудования.

Между некоторыми странами наблюдаются различия. США — единственная страна, где респонденты отметили возникновение расходов на оплату услуг внешних консультантов как основное негативное последствие атаки, в то время как в странах Азиатско-Тихоокеанского региона большее волнение вызывает ущерб критически важной инфраструктуре организации.

К основным глобальным рискам безопасности ИТ-инфраструктуры относятся:

несогласованность и сложность систем внутри организации;

небрежность сотрудников;

инфраструктура облачных вычислений и её поставщики;

нехватка квалифицированных кадров;

действия злоумышленников-инсайдеров».

(В 2020 г. 23% организаций по всему миру подверглись семи или более атакам // Компьютерное Обозрение (https://ko.com.ua/v_2020_g_23_organizacij_po_vsemu_miru_podverglis_semi_ili_bolee_atakam_135610). 10.12.2020).

***

«Специалисты «Лаборатории Касперского» поделились видением текущей ситуации в области информационной безопасности промышленных предприятий и представили прогноз на 2021 г.

По мнению экспертов, заражения будут становиться менее случайными или иметь неслучайные продолжения. У злоумышленников было несколько лет, чтобы провести профилирование случайно зараженных компьютеров, имеющих либо прямое отношение к технологическим сетям промышленных предприятий, либо периодический доступ к ним. Киберпреступники, занимающиеся массовыми заражениями, будут перепродавать (возможно, уже продают) доступ к таким компьютерам группировкам, сфокусированным на промышленных предприятиях.

Некоторые группировки уже несколько лет специализируются на атаках промышленных предприятий для прямой кражи денег. За эти годы они хорошо изучили особенности бизнес-процессов своих жертв, а также получили доступ к большому объему информации об объектах технологической сети и технологическом процессе. Эксперты полагают, что следует ожидать появления новых сценариев атак на АСУ ТП и полевые устройства, а также неожиданных схем их монетизации.

На уровень безопасности промышленных предприятий может негативно повлиять снятие с поддержки Windows 7 и Server 2008, популярных в АСУ ТП по всему миру, и, конечно же, утечка исходных кодов Windows XP – к сожалению, эти операционные системы до сих пор очень часто встречаются в технологических сетях. Есть высокая вероятность реализации сценария наподобие WannaCry в будущем. И промышленные предприятия могут оказаться в числе наиболее пострадавших.

Что касается атак вымогателей, они становятся все более технологичными и изощренными. Злоумышленники почувствовали вкус к нападениям на промышленные компании (ведь те платят выкуп), и, следовательно, будут продолжать такие атаки. Кроме того, эксперты ожидают рост числа гибридных атак с кражей документов и последующей угрозой их публикации в случае отказа платить выкуп или продажей украденной информации в даркнете. Также, по всей видимости, получат развитие идеи, реализованные в Snake: выраженная направленность шифровальщиков на АСУ ТП.

Злоумышленники начали понимать, что внутри периметра OT (операционные технологии) секреты охраняются хуже, чем в офисных сетях, а пробиться в технологическую сеть может быть даже проще ввиду наличия собственного периметра и уникальной поверхности атаки. «Плоская сеть» и прочие проблемы с разграничением доступа в OT-сетях могут сделать их привлекательной точкой входа в труднодоступные уголки корпоративной сети или дорожкой к инфраструктуре других организаций, а также прочим объектам холдингов и корпораций.

По мнению экспертов, продолжит расти количество APT-групп, в том числе атакующих организации, относящиеся к различным промышленным секторам. Активность злоумышленников будет коррелировать с локальными конфликтами, в том числе в «горячей фазе»: кибератаки, включая атаки на промышленные предприятия, будут использоваться как инструмент военных действий наряду с беспилотниками и информационными атаками через СМИ. Помимо задач «закрепиться на черный день» и кражи информации, кто-то рано или поздно обязательно перейдет к более активным действиям.

Переход в онлайн и цифровизация муниципальных и государственных сервисов сделают их более уязвимыми для злоумышленников, создадут больше возможностей для кросс-ведомственных атак и атак на смежные структуры. Например, атакующие смогут подбираться к финальной цели, такой как, например, транспортные системы, через каналы связи и цепочки поставок, объединяющие различные государственные, муниципальные и частные инфраструктуры, начав атаку, например, с веб-сервиса муниципальных или правительственных органов.

Ограничение возможности проведения работ «на месте» замедлило темпы укрепления защиты периметра промышленных предприятий и их технологических сетей, помешав, в частности, установке и настройке нового оборудования. Вкупе с увеличением количества и разнообразия сессий удаленных подключений это может привести к снижению уровня защиты периметров технологических сетей промышленных предприятий. Безопасность промышленных объектов в таких условиях будет в значительной степени зависеть от эффективности работы endpoint-решений и программ повышения осведомленности сотрудников. В то же время кибератаки, нацеленные на промышленные компании, становятся более зрелыми. Как следствие, даже несмотря на то, что количество атакованных компьютеров сокращается, число серьезных инцидентов уменьшаться не будет.

Количество сотрудников на местах, способных своевременно реагировать на инцидент и перевести системы и установки в режим ручного управления в случае успешной кибератаки, сократилось. Это может способствовать увеличению масштаба распространения вредоносного ПО и усугубить последствия киберинцидентов». ***(Промышленные предприятия становятся все более привлекательной целью для хакеров // Компьютерное Обозрение (https://ko.com.ua/promyshlennye_predpriyatiya_stanovyatsya_vse_bolee_privlekatelnoj_celyu_dlya_hakerov_135564). 08.12.2020).***

***

«Злоумышленники вымогают у израильской страховой компании, требуя почти 1 миллион долларов в биткойнах, чтобы прекратить утечку украденных данных компании.

В понедельник группа киберпреступников, назвавшая себя BlackShadow, написала в Твиттере, что они взломали израильскую страховую компанию Shirbit и во время атаки украли файлы.

«Команда Black Shadow осуществила масштабную кибератаку. Произошла массированная атака на сетевую инфраструктуру компании Shirbit, которая находится в экономической сфере Израиля», - написали в Твиттере злоумышленники.

С тех пор злоумышленники постоянно сливают документы и изображения жертвы в канал Telegram, который они создали для этой цели. Эти украденные данные включают документы, файлы PST электронной почты, отсканированные документы, аудиозаписи и изображения паспортов.

Прошлой ночью злоумышленники наконец опубликовали требование выкупа, в котором говорилось, что у Shirbit есть 24 часа, чтобы отправить 50 биткойнов, или примерно 1 миллион долларов, и они прекратят утечку своих данных.

Злоумышленники предупредили, что будут продолжать утечку данных каждые 24 часа, если им не заплатят.

На момент написания биткойн-адрес 13YiK3qHxTdGcD6nfCf7vWXFgWXnbpJvy2 не получал никаких платежей.

Охранные фирмы предостерегают от выплаты выкупа

Израильская компания по кибербезопасности Profero считает, что это требование выкупа - не более чем рекламный ход, и что злоумышленники не планируют прекращать утечку данных в случае оплаты.

Хотя приписывание этих атак не установлено, в последнее время участились кибератаки между Израилем и Ираном.

В октябре в отчете Profero и ClearSky Cyber Security подробно рассказывается, как иранский злоумышленник, известный как MuddyWater и связанный с КСИР (Корпус стражей Исламской Республики), планировал в сентябре разрушительные атаки на интересы Израиля.

Считается, что MuddyWater планировал использовать фишинговые электронные письма или использовать уязвимость Microsoft Exchange CVE-2020-0688 для развертывания поддельных программ обновлений Google под названием PowGoop. После установки PowGoop будет развертывать программу-вымогатель Thanos (Hakbit) на устройствах жертвы.

Программа-вымогатель Thanos продвигается на русскоязычных хакерских форумах как партнерская служба вымогателей (RaaS), где партнеры получают специальный конструктор программ-вымогателей. Взамен разработчики зарабатывают 30% всех выплат выкупа.

Израильские фирмы, занимающиеся кибербезопасностью, могут предотвратить атаки MuddyWater в сентябре, но ожидаются дальнейшие кибератаки». ***(Lawrence Abrams. BlackShadow hackers extort Israeli insurance company for $1 million // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/blackshadow-hackers-extort-israeli-insurance-company-for-1-million/). 04.12.2020).***

***

«Злоумышленники используют законную почтовую службу SendGrid для подделки фишинговых писем HMRC, которые обходят фильтры спама.

Известная проблема неоднократно использовалась мошенниками для уклонения от обнаружения продуктами защиты электронной почты, однако конкретного решения пока не найдено.

Служба доставки электронной почты использовалась для подделки электронных писем HMRC

SendGrid - это компания по доставке электронной почты, предоставляющая инфраструктуру для рассылки информационных бюллетеней, рекламных писем и оперативных деловых писем, таких как уведомления о доставке.

Хотя SendGrid сам по себе является законным сервисом, злоумышленники злоупотребляют некоторыми его функциями, чтобы обойти фильтры спама и продукты для защиты электронной почты.

Исследователь безопасности, известный как TheAnalyst, поделился с BleepingComputer информацией о продолжающейся фишинговой кампании HMRC, которая использует SendGrid для обхода спам-фильтров.

Фактические фишинговые веб-страницы, на которые есть ссылки в электронном письме, имитируют дизайн HMRC и GOV.UK.

Эти страницы содержат формы, собирающие конфиденциальную информацию о пользователях, такую как:

Уникальный справочный номер налогоплательщика (UTR)

Номер государственного страхования (NINo)

Номер паспорта и срок действия

Номер водительского удостоверения с указанием даты выдачи и истечения срока действия.

Имя, дата рождения и адресная информация

Фишинговая страница размещена на взломанном веб-сайте: https: // Technicalzia [.] Net / tax /

TheAnalyst сообщил BleepingComputer, что «устаревшие» учетные записи, предоставленные SendGrid, сделали платформу открытой для злоупотреблений со стороны злоумышленников.

«В данном конкретном случае HMRC имеет хорошую DMARC запись, что делает большинство получателей, чтобы просто барахло им, но когда [Мошенники] пародия другие домены, которые на самом деле sendgrid в SPF / DMARC это гораздо хуже,» TheAnalyst объяснил BleepingComputer.

Чтобы доставить эту фишинговую кампанию HMRC своим жертвам, злоумышленники подделали поле электронной почты От исходящего электронного адреса сборщика налогов: no_reply@advice.hmrc.gov.uk

Поскольку мошенники используют инфраструктуру доставки SendGrid, эти электронные письма «проходят через многие почтовые фильтры», - пояснил исследователь.

Текущая нерешенная проблема

SendGrid ответил на TheAnalyst «s доклада о том, что они пытаются сохранить свою платформу защищена от таких актеров фишинга.

Компания посоветовала сообщать о любых вредоносных электронных письмах в свою группу потребительского доверия, чтобы они могли быть расследованы и приняты меры

Однако исследователя и других пользователей Twitter это не убедило.

«Эта проблема продолжается как минимум полгода, и они обещали исправить ее в начале следующего года, но я не очень уверен».

«Мы компания Fortune 1000 и маркетинг использует Sendgrid, но я делаю все, что могу, чтобы эти контракты аннулируются, мы можем заблокировать их в SPF / DMARC,» TheAnalyst сказал BleepingComputer.

Основная проблема исследователя заключается в том, что, хотя SendGrid продолжает сообщать пользователям, что они решат проблему с помощью проверки права собственности на домен до того, как разрешить им отправлять электронные письма, именно «устаревшие» учетные записи скомпрометированы и подвержены злоупотреблениям со стороны мошенников.

По словам исследователя, во время Дня благодарения платформа SendGrid была использована в масштабной фишинг-кампании Zoom .

В результате атаки были украдены учетные данные тысяч пользователей.

На вопрос о дополнительной информации материнская компания SendGrid сказала BleepingComputer:

«Twilio знает об этом инциденте и предприняла шаги для расследования и решения проблемы. Twilio очень серьезно относится к злоупотреблениям своей платформой и услугами».

«Всегда прискорбно, когда человек или организация становятся жертвой фишинг-атаки. Мы рекомендуем пользователям нашей платформы воспользоваться существующими средствами управления безопасностью для защиты своих учетных записей, такими как использование 2FA и управления доступом по IP, и поощрять отправителей электронной почты в полной мере использовать технологии аутентификации электронной почты для защиты своих доменов от подделки ".

«Дополнительную информацию о передовых методах защиты учетных записей электронной почты можно найти [в блоге SendGrid]», - сказал BleepingComputer представитель Twilio.

По мере приближения конца года пользователи должны проявлять бдительность в отношении любых фишинговых и налоговых мошенничеств со стороны HMRC.

Получателям фишинговых писем с любым упоминанием SendGrid рекомендуется пересылать такие письма на адрес нарушения [at] sendgrid.com и не переходить по ссылкам внутри них». ***(Ax Sharma. HMRC phishing scam abuses mail service to bypass spam filters // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hmrc-phishing-scam-abuses-mail-service-to-bypass-spam-filters/). 02.12.2020).***

***

«ФБР предупреждает американские компании о том, что мошенники активно злоупотребляют правилами автоматической переадресации в веб-клиентах электронной почты, чтобы повысить вероятность успешных атак компрометации деловой электронной почты (BEC).

Это предупреждение было выпущено посредством совместного уведомления для частных предприятий (PIN), отправленного 25 ноября и согласованного с DHS-CISA.

Мошенники BEC известны тем, что используют социальную инженерию, фишинг или взлом для взлома корпоративной электронной почты с конечной целью перенаправления будущих или ожидающих платежей на банковские счета, находящиеся под их контролем.

Центр рассмотрения жалоб на Интернет-преступления (IC3) ФБР также выпустил Объявление о государственной службе (PSA) в сентябре 2019 года, в котором предупреждает, что мошенничество с BEC продолжает расти с каждым годом, при этом с июня 2016 года по июль 2019 года жалобы жертв составили более 26 миллиардов долларов в виде финансовых убытков. и 100% -ный рост

выявленных глобальных незащищенных убытков в период с мая 2018 г. по июль 2019 г.

IC3 также указала в отчете о преступности в Интернете за 2019 год. BEC был типом киберпреступлений с самыми высокими зарегистрированными общими потерями жертв в 2019 году, поскольку только за последний год он составил около 1,8 миллиарда долларов индивидуальных и коммерческих потерь.

Целевые медицинские и производственные организации

PIN-код, помеченный как «TLP: WHITE», содержит подробную информацию о том, как мошенники успешно скомпрометировали бизнес с помощью мошенничества BEC, и о том, как правила автоматической переадресации электронной почты используются для сбора информации и ограничения возможностей жертв по обнаружению мошеннических действий.

Мошенники BEC использовали правила электронной почты, добавленные к веб-клиентам целевой электронной почты, чтобы скрыть свою деятельность, выдавая себя за сотрудников или деловых партнеров.

«Согласно недавним отчетам ФБР, киберпреступники применяют правила автоматической переадресации в почтовых клиентах электронной почты жертв, чтобы скрыть их действия», - заявило ФБР.

«Правила пересылки веб-клиента часто не синхронизируются с настольным клиентом, что ограничивает видимость правил для администраторов кибербезопасности».

ФБР также предоставляет информацию о двух атаках с августа 2020 года, когда мошенники BEC использовали веб-правила пересылки электронной почты для нацеливания на американские производственные компании и компании по производству медицинского оборудования.

В обоих случаях злоумышленники смогли успешно скрыть свою деятельность от служб безопасности компаний, автоматически перенаправив все компрометирующие электронные письма на почтовые учетные записи злоумышленников.

Это позволяло им выдавать себя за других поставщиков и запрашивать отправку платежей за оказанные услуги на банковские счета, находящиеся под их контролем.

В августе 2020 года киберпреступники создали правила автоматической пересылки электронной почты на недавно обновленном веб-клиенте американской компании по производству медицинского оборудования. Веб-почта не синхронизировалась с настольным приложением и осталась незамеченной для компании-жертвы, которая соблюдала правила автопересылки только на настольном клиенте. RSS также не был включен в настольном приложении. После того, как участники BEC получили доступ к сети, они выдали себя за известного международного поставщика. Актеры создали домен с похожим написанием на жертву и общались с продавцом, используя IP-адрес в Великобритании, чтобы еще больше повысить вероятность оплаты. Актеры получили от жертвы 175 тысяч долларов.

Во время другого инцидента в августе 2020 года тот же субъект создал три правила пересылки в электронной почте, которая используется компанией в

производственной отрасли. Первое правило автоматически перенаправляло любые электронные письма с запросами «банк», «оплата», «счет», «перевод» или «чек» на адрес электронной почты киберпреступника. Два других правила основывались на домене отправителя и снова пересылались на тот же адрес электронной почты.

Злоупотребление электронной почтой при атаках BEC

ФБР также предупредило партнеров из частного сектора о злоумышленниках, злоупотребляющих Microsoft Office 365 и Google G Suite в атаках BEC, в двух отдельных уведомлениях [1, 2].

«Мошенничество инициируется с помощью специально разработанных наборов для фишинга, имитирующих облачные сервисы электронной почты, с целью взлома корпоративных учетных записей электронной почты и запроса или неправильного перевода денежных средств», - говорится в ПИН-коде ФБР, отправленном 3 марта.

Жертвы перенаправляются с помощью крупномасштабных фишинговых кампаний на фишинговые наборы, способные определять «службу, связанную с каждым набором скомпрометированных учетных данных» и отображать правильный пользовательский интерфейс.

Используя информацию, полученную из взломанных облачных учетных записей электронной почты, мошенники выдают себя за сотрудников скомпрометированных предприятий, чтобы подключиться к коммуникациям с другими поставщиками для перенаправления платежей на банковские счета, которые они контролируют.

Они также собирают и эксфильтруют контакты из зараженных учетных записей электронной почты, чтобы впоследствии использовать их в других фишинговых атаках и поставить под угрозу большее количество предприятий, что значительно упрощает переход к другим целям в том же или родственных отраслях.

Несмотря на то, что и Google G Suite, и Microsoft Office 365 поставляются с функциями безопасности, которые могут помочь блокировать попытки мошенничества с BEC, многие из них должны быть вручную настроены и включены ИТ-администраторами или группами безопасности организации.

По данным ФБР, из-за этого «малые и средние организации или организации с ограниченными ИТ-ресурсами наиболее уязвимы для мошенничества с BEC»…». ***(Sergiu Gatlan. FBI warns of BEC scammers using email auto-forwarding in attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fbi-warns-of-bec-scammers-using-email-auto-forwarding-in-attacks/). 01.12.2020).***

***

«Эксперты Cybereason обнаружили шпионскую кампанию, которая использует соцсети и облачные платформы, чтобы атаковать политиков.

По наблюдениям экспертов, участники кампании вели свою деятельность на территории стран Среднего Востока. Исследователи считают, что их целью были политики и региональные власти. Запуск кампании приписывают политически мотивированной APT-группировке Molerats, которая была активна в странах

Среднего Востока с 2012 года. Злоумышленники уже использовали бэкдоры Spark и Pierogi, чтобы атаковать власти Палестины.

Киберпреступники используют три вида малвари: два бэкдора, SharpStage и Dropbox, и загрузчик MoleNet. Они созданы, чтобы взламывать Facebook, Dropbox, Google Docs и Simplenote и красть пользовательские данные с их компьютеров.

Cybereason добавляет, что новые варианты малвари использовались вместе с бэкдором Spark, который ранее приписывался Molerats также, как и полезная нагрузка Quasar RAT.

Email-фишинг – еще одно средство шпионской кампании, которое фокусируется на конфиденциальной политической информации стран Среднего Востока, включая отношения Израиля и Саудовской Аравии, выборы ХАМАС и даже секретная встреча госсекретаря США с премьер-министром Израиля и кронпринцем Саудовской Аравии». ***(Исследователи обнаружили шпионскую кампанию, которая нацелена на политиков Среднего Востока // SecureNews (https://securenews.ru/the-researchers-found-the-espionage-company-which-is-aimed-at-politicians-in-the-middle-east/). 10.12.2020).***

***

«Аамир Лакхани из Fortinet обсуждает передовые методы защиты данных компании от угроз следующего поколения, таких как трояны доступа к периферии (EAT).

Киберпреступники постоянно держат руку на пульсе потенциальных новых векторов атак, ища следующую возможность. В настоящее время они перемещают значительные ресурсы для нацеливания и использования новых периферийных сетевых сред, таких как облако и удаленные сотрудники, а не просто нацелены на базовую сеть. Защита этих новых сред, включая новые технологии и конвергентные системы, является более сложной задачей, чем может показаться.

Например, переход к удаленной работе - это не просто увеличение количества конечных пользователей и устройств, удаленно подключающихся к сети. Хотя мы наблюдаем ожидаемый всплеск атак, нацеленных на начинающих удаленных сотрудников и уязвимые устройства для получения доступа к сети, мы также начинаем видеть новые атаки, нацеленные на подключенные домашние сети.

По некоторым данным, домашние офисные сети в 3,5 раза чаще заражаются вредоносным ПО, чем корпоративные. Многие атаки на домашние сети были направлены на использование старых, более уязвимых устройств, таких как домашние маршрутизаторы и развлекательные системы. Но в настоящее время также предпринимаются новые усилия, направленные на интеллектуальные системы, подключенные к домашней среде, которые объединяют несколько устройств и систем.

Зачем нужна интеллектуальная граница?

За последние несколько лет традиционный периметр сети был заменен несколькими периферийными средами - центром обработки данных, глобальной сетью, мультиоблачностью, Интернетом вещей, удаленными сотрудниками и т. д. - каждая из которых имеет свои уникальные риски. Преимущество плохих участников в том, что, хотя все эти грани взаимосвязаны, многие организации

отдают предпочтение производительности и цифровой трансформации, а не централизованной видимости и единому управлению.

Киберпреступники могут использовать домашние сети для проникновения в корпоративные сети. Злоумышленники могут поставить под угрозу конечных пользователей и их домашние ресурсы, используя подробную информацию, которую собирают и хранят подключенные устройства. Более изощренные злоумышленники используют эти устройства и эту информацию в качестве стартовой площадки для других типов атак. Атаки на корпоративные сети, запущенные из домашней сети удаленного сотрудника, особенно когда четко известны тенденции использования, можно тщательно координировать, чтобы они не подавали сигнал тревоги. Интеллектуальное вредоносное ПО, имеющее доступ к сохраненным данным о подключении, гораздо легче скрыть.

Рост EAT и продвинутых атак

Это только начало того, что сейчас возможно. Продвинутое вредоносное ПО может перехватывать данные с помощью новых троянов пограничного доступа (EAT) для выполнения таких задач, как перехват голосовых запросов из локальной сети с целью взлома систем или ввода команд. Добавление кроссплатформенных возможностей к угрозам EAT с помощью такого языка программирования, как Go, сделает EAT еще более опасными, поскольку эти атаки смогут переходить с устройства на устройство независимо от базовой ОС.

Как бороться с этими угрозами

Организации могут дать отпор, включив синие команды. Команды ИТ-безопасности могут использовать тактику, методы и процедуры (ДТС) киберпреступников, такие как учебные пособия по действующим лицам, которые исследуются командами по анализу угроз, в системы ИИ, чтобы обеспечить обнаружение шаблонов атак. Аналогичным образом, по мере того, как организации освещают тепловые карты активных в настоящее время угроз, интеллектуальные системы смогут проактивно скрывать сетевые цели и размещать привлекательные ловушки на путях атаки.

Однако организации не могут бороться со всеми этими угрозами в одиночку. Когда происходит атака, им необходимо знать, кого информировать, чтобы можно было должным образом поделиться «отпечатками пальцев» и чтобы правоохранительные органы могли выполнять свою работу. Организации по исследованию угроз, поставщики средств кибербезопасности и другие отраслевые группы должны сотрудничать для обмена информацией, но им также необходимо сотрудничать с правоохранительными органами, чтобы помочь демонтировать враждебные инфраструктуры для предотвращения будущих атак. У киберпреступников нет границ в Интернете, поэтому борьба с киберпреступностью также должна выходить за рамки границ. Только работая вместе, это партнерство переломит ситуацию в борьбе с киберпреступниками.

В конце концов, организации смогут отреагировать на любые попытки контрразведки до того, как они произойдут, что позволит синим командам сохранить превосходящий контроль. Такой вид обучения дает членам группы безопасности возможность улучшить свои навыки при блокировке сети.

Это не звучит как зашитая пластинка, но важность кибергигиены невозможно переоценить. Когда организации сосредотачиваются на обучении и осведомленности, сотрудники получают все необходимое для выполнения основных задач безопасности, таких как выявление подозрительного поведения, обновление устройств и соблюдение правил кибергигиены в командах. После этого крайне важно, чтобы организации инвестировали в правильные системы и решения - от виртуальных частных сетей до программного обеспечения для защиты от вредоносных программ и технологий шифрования, - которые обеспечивают четкую видимость и детальный контроль над всем ландшафтом угроз. Как говорится, сложность - враг безопасности. Таким образом, лучший ответ на все более сложный и динамичный цифровой мир - вернуться к основам. И это начинается с кибергигиены.

Необходимо динамическое изменение

Акцент киберпреступников сместился с базовой сети на ее наиболее удаленные участки - в основном, на домашние сети удаленных сотрудников. Продвинутое вредоносное ПО, такое как EAT, очень затрудняет обнаружение и устранение угроз. К счастью, у организаций есть множество ресурсов и доступных тактик для отражения этих новых атак. Используйте перечисленные выше передовые методы, чтобы улучшить свою стратегию кибербезопасности и защитить свои интеллектуальные преимущества». ***(Aamir Lakhani. Defending the Intelligent Edge from Evolving Attacks // Threatpost (https://threatpost.com/defending-intelligent-edge-evolving-attacks/162172/). 10.12.2020).***

***

«Убедительный фишинг с учетными данными электронной почты, бэкдоры по электронной почте и мобильные приложения - все это часть последних усилий группы по борьбе с военными и правительственными целями.

Группа усовершенствованных постоянных угроз (APT) SideWinder развернула новую инициативу по фишингу и вредоносному ПО, используя недавние территориальные споры между Китаем, Индией, Непалом и Пакистаном в качестве приманки. Цель состоит в том, чтобы собрать конфиденциальную информацию от своих целей, в основном расположенных в Непале и Афганистане.

Согласно анализу, SideWinder обычно нацелен на жертв в Южной Азии и окрестностях - и эта последняя кампания не является исключением. Целями здесь являются несколько правительственных и военных подразделений для стран региона, по словам исследователей, в том числе министерства обороны и иностранных дел Непала, непальской армии, Совета национальной безопасности Афганистана, министерства обороны Шри-Ланки, Президентского дворца в Афганистане и Больше.

В основном это делается с использованием легитимно выглядящих страниц входа в веб-почту, предназначенных для сбора учетных данных. Исследователи из Trend Micro заявили, что эти страницы были скопированы с фактических страниц входа в веб-почту их жертв и впоследствии модифицированы для фишинга. Например, «mail-nepalgovnp [.] Duckdns [.] Org» был создан, чтобы претендовать на

то, чтобы быть фактическим доменом правительства Непала, «mail [.] Nepal [.] Gov [.] Np».

Интересно, что после того, как учетные данные откачиваются и пользователи «входят в систему», они либо отправляются на законные страницы входа; либо они перенаправляются на другие документы или новостные страницы, связанные либо с COVID-19, либо с политической подачей.

Исследователи заявили, что на некоторых страницах есть майская статья под названием «Индия должна понять, что Китай не имеет ничего общего с позицией Непала в отношении Липулеха» и документ под названием «Разговор посла Янчи с Nepali_Media.pdf», в котором содержится интервью с послом Китая в Непале по поводу Covid-19, инициатива «Один пояс, один путь» и территориальные проблемы в районе Хумла.

Шпионаж

Кампания также включает элемент вредоносного ПО: вредоносные документы, доставляемые по электронной почте, предназначены для установки бэкдора, нацеленного на кибершпионаж. И были доказательства того, что группа планирует запуск мобильных устройств для взлома беспроводных устройств.

«Мы определили сервер, используемый для доставки вредоносного файла .lnk и размещения нескольких фишинговых страниц с учетными данными», - написали исследователи в своем сообщении в среду . «Мы также обнаружили несколько файлов Android APK на их фишинговом сервере. Хотя некоторые из них являются безвредными, мы также обнаружили вредоносные файлы, созданные с помощью Metasploit ».

Процедура заражения электронной почты

Что касается электронной почты, исследователи обнаружили, что в кампании используется много вредоносных исходных файлов, включая файл .lnk, который, в свою очередь, загружает файл .rtf и помещает файл JavaScript на компьютер цели; и файл .zip, содержащий файл .lnk, который, в свою очередь, загружает файл .hta (с помощью JavaScript).

«Все эти случаи заканчиваются либо загрузкой, либо удалением файлов, а затем выполнением кода JavaScript, который представляет собой дроппер, используемый для установки основного бэкдора и стилера», - пояснили исследователи.

Между тем загруженные файлы .rtf в цепочке используют уязвимость CVE-2017-11882; эксплойт позволяет злоумышленникам автоматически запускать вредоносный код, не требуя вмешательства пользователя.

Уязвимость затрагивает все непропатченные версии Microsoft Office, Microsoft Windows и типы архитектуры, начиная с 2000 года. Хотя в ноябре 2017 года была исправлена ошибка, Microsoft предупредила еще в прошлом году, что кампании по электронной почте распространяли вредоносные .rtf-файлы, заминированные с помощью эксплойта.

«Уязвимость CVE-2017-11882 была исправлена в 2017 году, но до сих пор мы все еще наблюдаем эксплойт в атаках», - написала в Твиттере Microsoft Security Intelligence в 2019 году. «Примечательно, что в последние несколько недель мы

наблюдали рост активности. Мы настоятельно рекомендуем применять обновления безопасности».

В этом случае замаскированный .rtf удаляет файл с именем 1.a, который представляет собой фрагмент кода JavaScript. Как выяснила компания Trend Micro, это помещает бэкдор и стилер в папку в ProgramData и напрямую выполняет их или создает запланированную задачу для выполнения удаленных файлов в более позднее время.

«Содержимое вновь созданной папки содержит несколько файлов, в том числе Rekeywiz, которое является законным приложением Windows», - пояснили аналитики. «Это приложение загружает различные системные библиотеки DLL, включая… поддельный DUser.dll [который] расшифровывает основной бэкдор + стилер из файла .tmp в том же каталоге».

После дешифрования полезная нагрузка собирает системную информацию и загружает ее на командно-управляющий сервер (C2), прежде чем настраивать кражу целевых типов файлов.

«[Это] включает такую информацию, как привилегии, учетные записи пользователей, информация о компьютерной системе, антивирусные программы, запущенные процессы, информация о процессоре, информация об операционной системе, часовой пояс, установленные обновления Windows, сетевая информация, список каталогов в Users \% USERNAME% \ Desktop, Users \% USERNAME% \ Downloads, Users \% USERNAME% \ Documents, Users \% USERNAME% \ Contacts, а также информацию обо всех дисках и установленных приложениях », - сообщает Trend Micro.

Ожидается мобильная кампания?

Исследователи увидели несколько мобильных приложений, которые находились в стадии разработки. Некоторые не содержат вредоносного кода (пока); например, на сервере скрывалось мобильное приложение под названием «OpinionPoll», якобы являющееся приложением для проведения опросов для сбора мнений относительно спора о политической карте Непала и Индии.

Другие содержали вредоносные возможности, но казались незавершенными.

«Хотя нам не удалось получить полезную нагрузку, согласно Манифесту, который запрашивает многочисленные разрешения, связанные с конфиденциальностью, такие как местоположение, контакты, журналы вызовов и т. Д., Мы можем сделать вывод, что он идет после личных данных пользователя», - пишут исследователи.

SideWinder ранее использовал вредоносные приложения как часть своей работы, замаскированные под инструменты для фотографий и файлового менеджера, чтобы побудить пользователей загрузить их. После загрузки на мобильное устройство пользователя они использовали уязвимости CVE-2019-2215 и MediaTek-SU для получения прав root.

В этом случае «мы полагаем, что эти приложения все еще находятся в стадии разработки и, вероятно, будут использоваться для взлома мобильных устройств в будущем», - отмечают исследователи.

SideWinder был активен в конце 2019 года, а в 2020 году, по данным компании, был замечен с помощью эксплойта Binder для атаки на мобильные

устройства. Trend Micro заявила, что в начале этого года группа также начала атаки на Бангладеш, Китай и Пакистан, используя файлы-приманки, связанные с COVID-19.

«Как видно из их фишинговых атак и постоянного развития инструментов для мобильных устройств, SideWinder очень активно использует такие актуальные темы, как COVID-19 или различные политические вопросы, в качестве метода социальной инженерии для компрометации своих целей», - заключила компания. «Поэтому мы рекомендуем пользователям и организациям проявлять бдительность». ***(Tara Seals. SideWinder APT Targets Nepal, Afghanistan in Wide-Ranging Spy Campaign // Threatpost (https://threatpost.com/sidewinder-apt-nepal-afghanistan-spy-campaign/162086/). 09.12.2020).***

***

«Остается неизвестным, почему Microsoft разрешает подделку своего собственного домена на собственную инфраструктуру электронной почты.

Целевой фишинг атакует Microsoft.com с целью нацеливания на 200 миллионов пользователей Microsoft Office 365 на ряде ключевых вертикальных рынков, включая поставщиков финансовых услуг, здравоохранения, производства и коммунальных услуг.

Исследователи из Ironscales обнаружили, что кампания нацелена на несколько тысяч почтовых ящиков почти у 100 клиентов фирмы, занимающейся защитой электронной почты, - говорится в отчете, опубликованном в понедельник в Интернете, вице-президентом Ironscales по исследованиям и разработкам Ломи Овадиа. По его словам, нацелены на другие отрасли, включая телекоммуникационные и страховые компании.

Атака особенно обманчива, поскольку использует точную технику подделки домена, «которая происходит, когда электронное письмо отправляется с мошеннического домена, который точно соответствует домену подделанного бренда», - написал Овадия. По его словам, это означает, что даже опытных пользователей, которые проверяют адреса отправителей, чтобы убедиться, что электронная почта является законной, могут обмануть.

Согласно отчету, атака представляет собой реалистично выглядящее электронное письмо, которое пытается убедить пользователей воспользоваться относительно новой возможностью Office 365, которая позволяет им восстанавливать электронные письма, которые были случайно помечены как спам или фишинговые сообщения. Сообщения поступают от отправителя «Microsoft Outlook».

«В частности, мошенническое сообщение состоит из срочных и в некоторой степени внушающих страх формулировок, предназначенных для того, чтобы убедить пользователей без колебаний щелкнуть вредоносную ссылку», - написал Овадия. «Как следует из сообщения, ссылка будет перенаправлять пользователей на портал безопасности, на котором они могут просматривать и принимать меры в отношении «помещенных в карантин сообщений», захваченных стеком фильтрации Exchange Online Protection (EOP), новой функцией, которая была доступна только с тех пор. Сентябрь."

По словам Ironscales, после того, как пользователь нажимает на ссылку, его просят ввести законные учетные данные для входа в Office 365 на поддельной странице входа, контролируемой злоумышленниками, для сбора и продажи в темной сети.

Одним из интересных аспектов кампании является то, что она успешно преодолела контроль безопасного шлюза электронной почты (SEG). По словам Ironscales, как правило, точную подделку домена им не очень сложно обнаружить; Компания обнаружила в предыдущем исследовании, что эта тактика использовалась менее чем в 1% от общего числа атак со спуфингом, которые обходят SEG в конкретный год.

«Даже устаревшие и не облачные инструменты защиты электронной почты достаточно эффективны для предотвращения подобных атак», - отметил Овадия. «Причина, по которой SEG могут традиционно останавливать точную подделку домена, заключается в том, что при правильной настройке этот элемент управления совместим с доменной аутентификацией сообщений, отчетностью и соответствием (DMARC), протоколом аутентификации электронной почты, созданным специально для остановки точной подмены домена (SPF / DKIM)».

Однако Ironscales обнаружил, что серверы Microsoft в настоящее время не применяют протокол DMARC, что означает, что точные сообщения о подделке домена проходят через такие элементы управления, как Office 365 EOP и Advanced Threat Protection.

«Любая другая служба электронной почты, которая уважает и обеспечивает соблюдение DMARC, заблокировала бы такие электронные письма», - написал Овадия. «Остается неизвестным, почему Microsoft разрешает имитацию своего собственного домена против собственной инфраструктуры электронной почты».

Ситуация особенно любопытна, поскольку Microsoft обычно является одним из самых популярных доменных имен, если не самым популярным доменом, имитируемым хакерами в фишинговых кампаниях, заметил он.

Согласно отчету, для смягчения атак Ironscales посоветовал организациям настроить свои системы защиты и защиты электронной почты для DMARC, которая должна обнаруживать и отклонять электронные письма, поступающие из последней кампании Office 365.

«Расширенная защита электронной почты на уровне почтового ящика, которая непрерывно изучает почтовый ящик каждого сотрудника для выявления аномалий на основе данных электронной почты и метаданных, извлеченных из ранее надежных сообщений, может помочь остановить подделку электронной почты, которая ускользает от взлома», - добавил Овадия». ***(Elizabeth Montalbano. Spearphishing Attack Spoofs Microsoft.com to Target 200M Office 365 Users // Threatpost (https://threatpost.com/spearphishing-attack-spoofs-microsoft-office-365/162001/). 08.12.2020).***

***

«Исследователи кибербезопасности из Университета Бен-Гуриона в Негеве недавно обнаружили способ кибератаки, который может позволить

хакерам удаленно ввести в заблуждение лабораторных исследователей и запустить производство опасных токсинов и вирусов.

При этом лабораторное программное обеспечение, отвечающие за проверку состава производимого препарата, может не заметить внесенных изменений.

Израильские специалисты по кибербезопасности из университета Бен-Гуриона нашли и протестировали метод, который может позволить хакерам получить удаленный доступ к компьютерам биоинженеров в исследовательских лабораториях с целью внесения вредоносных изменений в программное обеспечение. В ходе кибератаки хакеры могут удаленно заменить фрагменты синтетической ДНК на вредоносный код.

Синтетическая ДНК обычно создается из химических компонентов с помощью компьютерной программы и используется в различных целях. Например, для разработки вакцин, лекарств или других медицинских препаратов. Включение вредоносного программного кода может помочь хакерам внедрить в лекарство вирус.

Если раньше террористам для распространения вируса или токсина требовалось физически проникнуть в лабораторию и спрятать их внутри вакцины или другого медицинского препарата, то теперь все изменилось, сейчас злоумышленники могут провернуть такую операцию намного проще и быстрей.

При помощи вредоносной программы-трояна хакеры могут удаленно изменить код ДНК, содержащейся в препарате, и лаборатория, выпускающая лекарственное средство, даже не узнает о том, что в их продукте теперь находится опасный патоген.

«Кибератака, изменяющая порядок синтетической ДНК, может привести к синтезу патогенов, опасных белков или токсинов. Это действительно реальная угроза. Мы провели эксперимент и доказали, что измененная нами ДНК, содержащая опасный фрагмент, не была обнаружена программным обеспечением лаборатории. Соответственно, опасное лекарственное средство было направлено в производство», — сообщают исследователи.

В рамках эксперимента израильским киберспециалистам удалось обмануть систему безопасности лабораторий 16 раз из 50. Это означает, что существует неиллюзорная потенциальная угроза, которая может способствовать развитию биотерроризма.

Чтобы подобная атака увенчалась успехом, необходимо выполнить два действия. Сначала злоумышленник должен заразить компьютер ученого вредоносной программой, которая, в свою очередь, подключится к программному обеспечению лаборатории и изменит порядок синтеза ДНК. Эта вредоносная программа работает по тому же принципу, что и трояны, внедряющиеся в банковские программы и изменяющие данные денежных переводов, чтобы отправить деньги другому получателю.

Затем измененная ДНК должна пройти проверку у поставщика, и если изменения в ней не были обнаружены, то атака удалась…». ***(Биотерроризм может стать причиной новых эпидемий // УКРОП (https://укроп.org/bioterrorizm-mozhet-stat-prichinoj-novyh-epidemij/). 12.12.2020).***

***

«Компания McAfee представила отчет под названием The Hidden Costs of Cybercrime («Скрытые издержки киберпреступности»). Согласно выводам этого отчета, подготовленного совместно с «Центром стратегических и международных исследований» (CSIS), киберпреступность обошлась мировой экономике более чем в 1 трлн. долл. – чуть более 1% мирового ВВП. По сравнению с 2018 г. этот показатель вырос более чем на 50%. Тогда он составлял около 600 млрд. долл. В дополнение к этому международному показателю отчет подробно описывает нематериальные убытки, с которыми столкнулись 92% компаний.

Хищение интеллектуальной собственности и денежных средств наносит компаниям ощутимый ущерб. Наименее очевидные издержки киберпреступности связаны со снижением эффективности работы организаций. По данным исследования, 92% компаний сообщили о других негативных для бизнеса последствиях кибератак в дополнение к финансовым убыткам и потере рабочих часов. В отчете подробно рассмотрены следующие скрытые издержки и долгосрочные эффекты киберпреступлений на деятельность предприятий:

Системные простои. Простои оказались распространенной проблемой для двух третей организаций-респондентов. Средний размер убытка за самый длительный в 2019 г. простой составил 762 тыс. долл. Треть (33%) участников исследования сообщили, что инциденты безопасности, повлекшие за собой простой ИТ-систем, обошлись им в сумму от 100 до 500 тыс. долл.

Снижение эффективности. Из-за системных простоев организации в среднем теряли девять рабочих часов в неделю, что привело к снижению эффективности их работы. Среднее время приостановки деятельности составило 18 часов.

Затраты на реагирование на инциденты. По данным отчета, в большинстве организаций среднее время реакции на киберугрозу с момента ее обнаружения до устранения составляло 19 часов. Большинство проблем удается решить своими силами, но крупные инциденты часто требуют привлечения внешних консультантов. На оплату их услуг приходится значительная доля расходов, связанных с реагированием на крупномасштабную кибератаку.

Ущерб для торговой марки и репутации. Стоимость восстановления имиджа торговой марки с привлечением внешних консультантов или новых сотрудников для предотвращения будущих инцидентов также включается в ущерб от киберпреступности. 26% респондентов сообщили, что простои в результате кибератаки нанесли ущерб их торговой марке.

Исследование и анализ выявили недостаточную осведомленность о киберрисках в масштабах организации. По этой причине компании и агентства уязвимы перед продвинутыми атаками с применением методов социальной инженерии. После взлома компьютера одного пользователя редко удается обнаружить проблему вовремя и остановить ее распространение. По данным отчета, 56% опрошенных организаций признались в отсутствии плана по предотвращению киберугроз и реагированию на них. План реагирования имеется у 951 организации, и только 32% респондентов из этого числа считают его эффективным.

В заключительной части отчета приводятся ключевые рекомендации для бизнеса по противодействию киберпреступности. Среди них – единообразное применение основных мер безопасности, повышение прозрачности организаций и правительственных учреждений, стандартизация и координация требований к кибербезопасности, повышение уровня знаний о кибербезопасности в рамках организованного обучения сотрудников, разработка планов по предотвращению кибератак и реагированию на них.

Количественное исследование проводилось в период с апреля по июнь. Были опрошены 1500 руководителей в сфере IT и различных отраслей производства. Привлекались респонденты из США (300), Канады (200), Великобритании (200), Франции (200), Германии (200), Австралии (200) и Японии (200). Организации респондентов – компании из всех отраслей экономики, кроме строительства и недвижимости, со штатом 1000 и более сотрудников. В секторе правительственных учреждений опрос проводился только среди руководителей в сфере ИТ с правом принятия решений. Респонденты отвечали на вопросы в онлайн-режиме.

Кроме того, специалисты CSIS изучили данные об убытках от киберпреступности из открытых источников и сопроводили их комментариями правительственных чиновников. Эти расчеты были скорректированы с учетом уровней национального дохода по данным «Международного валютного фонда». ***(McAfee: глобальные убытки от киберпреступности превысили 1 трлн. долл. // Компьютерное Обозрение (https://ko.com.ua/mcafee_globalnye_ubytki_ot_kiberprestupnosti_prevysili_1_trln_doll_135653). 15.12.2020).***

***

«Переход на дистанционную работу открыл новые ворота для проникновения киберпреступников в периметры организаций. Аналитики полагают, что ключевыми проблемами для бизнеса становятся вредоносное ПО, небезопасные сети и удаленный доступ.

На фоне пандемии хакеры атакуют ИВ-устройства и конечные точки

Продолжающаяся глобальная пандемия коронавируса, которая привела к массовому переходу большинства организаций мира в дистанционные форматы работы и более широкому использованию гибридных ИТ-систем, стала причиной усложнения и увеличения числа ИБ-рисков. Согласно данным аналитиков из Cybersecurity Insiders, в 2020 г. В 72% организаций отметили увеличение количества инцидентов, связанных с безопасностью конечных точек и устройств интернета вещей (ИВ).

Еще 56% респондентов при этом ожидают, что их организация, вероятно, будет скомпрометирована из-за таких атак в следующие 12 месяцев. В исследовании, проведенном при поддержке Pulse Secure, приняли участие 325 человек, принимающих решения в области ИТ и кибербезопасности в США. Они представили самые разнообразные сферы — от финансовых услуг и здравоохранения до энергетики и госсектора.

«Результаты исследования дают понять, что проблема обеспечения безопасности интернета вещей и конечных точек стала куда более серьезной из-за

того, что сотрудники многих организаций были вынуждены работать удаленно, — комментирует полученные данные Скотт Гордон (Scott Gordon), директор по маркетингу Pulse Secure. — Угроза реальна, и она растет. Тем не менее, положительным моментом является то, что организации инвестируют в ключевые ИБ-инициативы, а также проверяют состояние устройств удаленного доступа и систем контроля доступа к сети для решения некоторых из этих проблем».

Компании расплачиваются простоем систем и снижением производительности

Участники опроса выделили еще три ключевые проблемы, с которыми они сталкивались в 2020 г. Среди них оказались вредоносное ПО (78%), проблемы с обеспечением безопасности сетей и удаленным доступом (61%) и скомпрометированными учетными данными (58%). В качестве способов решения указанных проблем ИТ-специалисты называли внедрение решений, которые повышают безопасность устройств (41% опрошенных), усовершенствование проверки состояния своих устройств удаленного доступа (35%) и улучшение возможностей по идентификации и мониторингу ИВ-устройств (22%).

Для тех, кто стал жертвой проблем с безопасностью конечных точек или интернета вещей, наиболее значительным негативным последствием стало снижение производительности пользователей (55%) и ИТ (45%), за которыми последовал простой системы (42%).

«Разнообразие пользователей, устройств, сетей и угроз продолжает расти по мере того, как предприятия используют преимущества большей мобильности рабочей силы, гибкости рабочего места и возможностей облачных вычислений. Организациям необходимо не только обеспечивать безопасность конечных точек и соблюдать политику использования, но и управлять соответствующим доступом к устройствам интернета вещей. Новые элементы управления безопасностью Zero Trust могут усилить динамическое обнаружение, проверку, отслеживание, исправление и контроль доступа устройств», — уверен Хольгер Шульце (Holger Schulze), генеральный директор и основатель Cybersecurity Insiders.

«Действительно, в том числе и устройства интернета вещей оказались целями постоянно увеличивающегося числа кибератак. В связи с этим дополнительные меры предосторожности должны приниматься не только ИТ-специалистами и службами безопасности, но и всей организацией. Обучение пользователей, которое знакомит сотрудников с кибер-гигиеной, следует считать обязательным. Кроме того, сейчас организациям самое время пересмотреть свои инвестиции в технологии безопасности. Безопасные шлюзы электронной почты и решения для контроля доступа должны обеспечивать уровень защиты, необходимый для меняющегося ландшафта угроз. Системы предотвращения вторжений добавляют еще один уровень защиты, экранируя устройства интернета вещей, которые сложно защитить напрямую», — говорит Михаил Родионов, региональный директор Fortinet в России и странах СНГ». ***(Больше 70% компаний в 2020 г. столкнулись с атаками на конечные точки и ИВ-устройства // CNews (https://safe.cnews.ru/news/top/2020-12-15_bolshe_70_kompanij_v_2020_g). 18.12.2020).***

***

«Киберпреступники использовали инструменты удостоверяющего центра Вьетнама для внедрения бэкдоров на системы жертв.

Специалисты ИБ-компании ESET раскрыли новую атаку на цепочку поставок, жертвой которой стал Государственный удостоверяющий центр Вьетнама. В ходе атаки, получившей название SignSight, злоумышленники взломали принадлежащие УЦ инструменты для цифровой подписи с целью установки бэкдоров на систему пользователей.

Как показывают данные телеметрии ESET, взлом произошел между 23 июля и 16 августа 2020 года. По данным специалистов, с помощью хранящихся на сайте УЦ (ca.gov.vn) модифицированных установщиков программного обеспечения хакеры внедрили на системы жертв шпионское ПО PhantomNet или Smanager.

«Компрометация сайта удостоверяющего центра – это хорошая возможность для APT-групп, поскольку посетители, скорее всего, будут иметь высокий уровень доверия к государственной организации, ответственной за цифровую подпись», – пояснил исследователь Матье Фау (Matthieu Faou).

Кода специалисты сообщили УЦ об обнаруженной проблеме, регулятор ответил, что ему уже известно об атаке, и загрузившие модифицированное ПО пользователи были предупреждены.

В ходе атаки злоумышленники модифицировали два установщика – gca01-client-v2-x32-8.3.msi и gca01-client-v2-x64-8.3.msi для 32- и 64-разрядных версий Windows.

Инструмент для цифровой подписи утвержден Государственным комитетом по шифрованию Вьетнама как часть схемы электронной аутентификации. Государственные учреждения и частные компании используют его для цифровой подписи документов с помощью USB-токена (PKI-токена), хранящего цифровую подпись. Для работы этого токена и нужны вышеупомянутые установщики. Поэтому единственный способ заразиться для пользователя – вручную загрузить с официального сайта скомпрометированное ПО и запустить его на своей системе.

После установки на системе жертвы в целях маскировки модифицированное ПО сначала запускает действительную программу GCA, а затем бэкдор PhantomNet, маскирующийся под кажущийся безобидным файл eToken.exe. Бэкдор собирает системную информацию и через плагины получает дополнительные функции с C&C-серверов vgca.homeunix[.]org и office365.blogdns[.]com, использующих название VGCA и других популярных программ.

Помимо Вьетнама жертвы вредоноса были обнаружены на Филиппинах, но механизм его доставки остается неизвестным. Конечная цель злоумышленников также остается неясной: информация об их действиях после взлома практически отсутствует…». ***(Эксперты сообщили о еще одной атаке на цепочку поставок // SecurityLab.ru (https://www.securitylab.ru/news/514962.php). 18.12.2020).***

***

«Система глубокого анализа трафика PT Network Attack Discovery, песочница PT Sandbox, система контроля защищенности MaxPatrol 8, система выявления инцидентов MaxPatrol SIEM и система анализа трафика сетей

АСУ ТП PT Industrial Security Incident Manager обнаруживают активность инструментов, которыми пользовались специалисты компании FireEye для тестирования защищенности своих клиентов. Инструменты попали в руки злоумышленников в ходе недавней хакерской атаки.

Часть похищенного инструментария уже была публично доступна и весьма широко распространена, отмечают эксперты центра информационной безопасности Positive Technologies (PT Expert Security Center). Злоумышленники используют инструменты такого типа для развития атаки внутри инфраструктуры, закрепления в ней и для организации канала удаленного доступа. При этом преступники берут очередной инструмент на вооружение в первые несколько дней (а иногда и часов) после его возникновения. К примеру, группировка Cobalt начала использовать CVE-2017-11882 в своих атаках в течение суток с момента появления публичных данных об этой уязвимости.

Специалисты PT ESC проанализировали данные, которые опубликовали сотрудники FireEye для обнаружения применения злоумышленниками их инструментов (34 правила для Snort1). Любые активности, на которые направлены эти правила, автоматически выявляются системой анализа трафика PT NAD: применение трех инструментов продукт выявляет «из коробки», а для вычисления активности четвертого инструмента эксперты PT ESC загрузили свежие правила детектирования. Таким образом, пользователям PT NAD самостоятельно адаптировать и загружать правила от FireEye не нужно. Технологические сети (сети АСУ ТП) сегодня также являются целями для преступных хакерских группировок. Поэтому необходимые индикаторы для обнаружения активности этих инструментов добавлены и в PT ISIM.

Кроме того, специалисты FireEye выпустили набор YARA-правил для выявления других инструментов тестирования защищенности. Эксперты PT ESC проанализировали их эффективность, выделили оптимальный пакет правил с минимальным уровнем false positive и добавили его в песочницу PT Sandbox, которая проводит комплексный анализ файлов в инфраструктуре. Эти правила позволят PT Sandbox детектировать применение похищенного инструментария, созданного на базе хорошо известных Cobalt Strike, Rubeus и Impacket, а также ряда узкоспециализированных инструментов FireEye.

FireEye также опубликовала список уязвимостей, которые ее собственные сотрудники из red team используют в том числе для тестов на проникновение. Система контроля защищенности MaxPatrol 8 выявит уязвимости, наиболее применимые к ПО в российских компаниях, что поможет ограничить эффективность инструментов FireEye. Эксплуатацию шести уязвимостей можно обнаружить с помощью PT NAD по анализу сетевого трафика. Система выявления инцидентов MaxPatrol SIEM с помощью анализа событий Windows выявляет активность шести наиболее популярных инструментов, которые используются в подавляющем большинстве атак, нацеленных на полную компрометацию инфраструктуры.

«Большинство правил обнаружения в MaxPatrol SIEM не привязано к конкретным группировкам и их инструментам, — комментирует Антон Тюрин, руководитель отдела экспертных сервисов PT Expert Security Center. — Это значит,

что с помощью одного правила система может задетектировать активность сразу нескольких схожих инструментов. Такой подход позволяет покрыть большое количество популярного хакерского софта».

«APT-группировки все чаще прибегают к так называемым атакам на цепь поставок — взломам организаций через их менее защищенных поставщиков или клиентов. Ситуация с FireEye не стала исключением, — комментирует Андрей Войтенко, директор по продуктовому маркетингу Positive Technologies. — Для защиты от подобных угроз недостаточно концентрироваться на предотвращении атак и контролировать только периметр, необходим мониторинг и глубокий анализ происходящего внутри сети, нужен инструментарий для своевременного выявления угроз». ***(Продукты Positive Technologies выявляют применение пентестерских инструментов FireEye, похищенных хакерами // SecurityLab.ru (https://www.securitylab.ru/news/514960.php). 18.12.2020).***

***

«Мошенники рассылают пользователям по всему миру электронные спам-письма. ИБ-специалисты опасаются, что киберпреступники тестируют новый вредоносный инструмент, которому суждено стать серьезной угрозой для бизнеса и потребителей в 2021 году.

Эксперты из компании Vade Secure зафиксировали резкий рост количества спам-писем, попадающих в почтовые ящики пользователей в Италии, Франции, Дании и США. Одна компания получила около 300 тыс. спам-писем всего за один день, что вынудило ее отключить затронутые учетные записи и сбросить учетные данные.

Волна спама является не простой, поскольку электронные письма помещаются в папку «Входящие», минуя уровни защиты. В Vade Security подозревают, что преступники используют инструмент под названием Email Appender, который был впервые обнаружен Gemini Advisory в октябре 2020 года и продается в даркнете по подписке.

Приложение Email Appender позволяет киберпреступникам подтверждать учетные данные скомпрометированной учетной записи, настраивать прокси-сервер, чтобы избежать обнаружения IP-адреса и создавать вредоносные электронное письмо. Использование Email Appender предполагает наличие списка скомпрометированных учетных данных. Перебирая логины и пароли, программа пытается авторизоваться на email-сервере, открыть почтовый ящик жертвы и добавить в него свое вредоносное письмо.

Инструмент имеет пользовательский интерфейс, позволяющий хакеру настроить электронную почту, изменив отображаемое имя адреса отправителя и создав адрес для ответа.

«Распространение Email Appender по принципу подписки — предупреждающий знак о том, что должно произойти в сфере киберпреступности-как-услуги. Незаконные сервисы, доступные в даркнете, позволяют преступникам с низким уровнем технологий проводить успешные атаки программ-вымогателей. Если Email Appender и другие подобные инструменты и дальше будут пользоваться успехом, они могут стать очень популярными в киберпреступном сообществе. В

прошлом мы видели, что хакеры проверяли свои методы на потребительском рынке, прежде чем перейти на рынок бизнеса. Потребители иногда менее разбираются в вопросах безопасности, чем бизнес, а это означает, что они представляют собой относительно легкую цель и позволяют преступникам осваивать новые методы», — пояснили специалисты». ***(Пользователи по всему миру столкнулись с огромной волной спама // SecurityLab.ru (https://www.securitylab.ru/news/514827.php). 15.12.2020).***

***

«Детектированная экспертами международной компании ESET атака на поставку цепочек длилась как минимум с середины 2018 года по осень 2020. Кибероперация получила название Затаенный трезубец (StealthyTrident) и была направлена на слежку за монгольскими чиновниками через корпоративный мессенджер.

Более 400 государственных учреждений Монголии используют в работе бизнес-платформу Able. В состав платформы входит приложение для коммуникаций Able Desktop. Кибериссследователи ESET обнаружили, что именно через это приложение на компьютеры пользователей загружается и устанавливается бэкдор HyperBro. Ранее данный бэкдор использовала хакерская группировка LuckyMouse.

Через механизм обновления Able Desktop пользователи чата подвергались еще одной разновидности атак – с помощью трояна удаленного доступа Tmanger. Аналитики ESET выяснили, что злоумышленники развили успех после компрометации одного или нескольких серверов обновлений Able Desktop.

В исследовании подчеркивается, что беспрепятственная слежка за деятельностью сотрудников правительственных учреждений Монголии в течение двух лет стала возможной из-за компрометации разработчиков приложения на одном из этапов создания популярного корпоративного мессенджера». ***(Раскрыта масштабная атака на государственные организации Монголии // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5706795-Raskryta-masshtabnuyu-ataku-na-gosu.html). 14.12.2020).***

***

«Колледж Роанок отложил весенний семестр почти на месяц после того, как кибератака затронула файлы и доступ к данным.

Колледж Роанок - это частный гуманитарный колледж, расположенный в Салеме, штат Вирджиния, где обучается около 2000 студентов.

Весенний семестр колледжа был первоначально запланирован на 19 января 2021 года, но из-за «киберинцидента» 12 декабря и распространения коронавируса колледж был вынужден перенести начало семестра на 8 февраля 2021 года.

«Отсрочка начала семестра также дает колледжу время, чтобы убедиться, что все сбои в сети, с которыми мы в настоящее время сталкиваемся, устранены. Как многие из вас знают, в колледже Роанок произошло кибер-событие, которое повлияло на нашу способность получать доступ к файлам».

«Пока мы работаем над восстановлением операций, неясно, как долго сеть Роанок-колледжа может быть недоступна. Веб-сайт колледжа в настоящее время работает, но некоторые области не работают из-за необходимости входа пользователя в систему для доступа к определенным функциям», - говорит Роанокский колледж. объяснил в новостях об изменении расписания.

Колледж, вероятно, подвергся атаке вымогателя

Хотя Колледж Роанок конкретно не указал, от какого типа кибератаки они пострадали, исходя из опубликованной информации, весьма вероятно, что они подверглись атаке с использованием программы-вымогателя.

В серии обновлений статуса колледж объясняет, что 12 декабря они пострадали от «киберинцидента», который вынудил их отключить свои ИТ-системы, чтобы остановить распространение атаки.

«В субботу, 12 декабря, в Роанок-колледже произошло кибер-событие, которое повлияло на нашу способность получать доступ к файлам. ИТ-специалисты колледжа отключили сеть колледжа и начали расследование этого инцидента», - поясняет Роанок-колледж в своем информационном сообщении.

В серии последующих обновлений колледж предупреждает сотрудников и студентов, чтобы они не использовали свои компьютеры в сети университетского городка или не получали доступ к своей электронной почте и другим приложениям Office 365, поскольку в настоящее время они не были определены как «безопасная среда».

В опубликованном вчера обновлении колледж заявляет, что они начали восстанавливать файлы на общих дисках «Z:» и «X:» и что пользователи не потеряли никаких данных.

«ИТ-отдел работает над восстановлением содержимого личных дисков Z: и дисковых X: отделов. Однако у нас еще нет ни даты начала восстановления, ни целевой даты проведения восстановительных работ. На данный момент кажется, что пользователи не потеряют содержимое этих дисков в результате киберинцидента», - поясняется в обновлении.

Неизвестно, сколько времени займет процесс восстановления.

Сектор образования все чаще подвергается атакам: операции с программами-вымогателями нацелены на ИТ-системы, когда они больше всего необходимы для дистанционного обучения.

В этом месяце ФБР, Агентство по кибербезопасности и безопасности инфраструктуры (CISA) и Межгосударственный центр обмена и анализа информации (MS-ISAC) выпустили совместное консультативное предупреждение об увеличении количества программ-вымогателей, доставки вредоносных программ и DDoS-атак на K-12. образовательные учреждения». ***(Lawrence Abrams. Roanoke College delays spring semester after cyberattack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/roanoke-college-delays-spring-semester-after-cyberattack/). 22.12.2020).***

***

«Период перед зимними праздниками – излюбленная пора для фишеров. В связи с этим компания GoDaddy решила проверить, могут ли попасться на

удочку мошенников ее собственные сотрудники, и провела тайное тестирование, вызвавшее неоднозначную реакцию общественности.

Как сообщает аризонское новостное издание Copper Courier, ранее в этом месяце GoDaddy разослала своим сотрудникам электронные письма с обещанием выплатить рождественскую премию в размере $650 в качестве благодарности за «рекордный для GoDaddy год». Для того чтобы получить премию, сотрудники должны были прислать ответное письмо с указанием своего адреса и другой персональной информации. На письмо ответили порядка 500 сотрудников, но никаких денег они не получили. Более того, через два дня компания прислала им еще одно письмо, в котором сообщила, что они провалили тест на безопасность и обязаны провести на работе дополнительное время для прохождения обучения.

Новость о тестировании вызвала бурю негодования у пользователей Twitter – некоторые даже заявили о намерении сменить хостинг-провайдера. Хотя компании то и дело тестируют своих сотрудников на уязвимость к фишингу, ложное обещание выплатить премию в разгар пандемии, когда миллионы людей рискуют остаться без крова и еды, выглядит особенно жестоким. Тем более, что за время карантина GoDaddy уволила и переназначила на другие должности сотни работников, хотя этот год оказался для компании действительно рекордным по количеству новых клиентов.

После публикации статьи в Copper Courier, GoDaddy сообщила, что извинилась перед сотрудниками. «GoDaddy очень серьезно относится к безопасности своей платформы. Мы понимаем, что некоторые сотрудники были расстроены попыткой фишинга и сочли ее бестактной, за что мы приносим свои извинения. Хотя тест имитировал предпринимаемые в настоящее время реальные попытки фишинга, нам нужно больше стараться и быть внимательнее к своим сотрудникам», – сообщили в компании». ***(GoDaddy провела весьма неоднозначное тестирование сотрудников на уязвимость к фишингу // SecurityLab.ru (https://www.securitylab.ru/news/515104.php). 25.12.2020).***

***

Діяльність хакерів та хакерські угруповування

«Хакерські атаки протягом 2020 року коштували світовій економіці понад 1 трильйон доларів. Про це свідчать оприлюднені у понеділок, 7 грудня, дані американської компанії McAfee, яка спеціалізується на комп'ютерній безпеці, та Центру стратегічних і міжнародних досліджень (CSIS)…

Завданий цього року хакерами збиток є на 50 відсотків вищим, ніж був ще два роки тому, у 2018 році, встановили дослідники. Таким чином збитки, завдані хакерами у 2020 році, становлять понад один відсоток світового ВВП…

За даними авторів дослідження, відбулося зростання кількості випадків як використання так званих програм-здирників, за допомогою яких зловмисники закодовують дані й вимагають відкуп за їх розкодування, так і кількості фішинг-атак, крадіжок Email-акаунтів, використання шпигунського програмного забезпечення та крадіжок криптовалют. Одним з факторів, який посприяв

збільшенню кількості кіберзлочинів, є той, що багато працівників цього року перейшли на віддалену роботу через пандемію коронавірусу, й мають віддалений доступ до робочих комп'ютерних систем.

Дослідження базується на оцінці даних близько 1500 ІТ-фахівців з компаній, державних установ та різних організацій зі Сполучених Штатів Америки, Канади, Великобританії, Франції, Німеччини, Японії та Австралії. Для оцінювання збитків враховувалися не лише втрати цифрової власності, але й втрати робочого часу, протягом якого не працювали робочі системи, а також іміджеві втрати компаній і установ, які ставали об'єктами хакерських атак. Є й інші приховані втрати від кіберзлочинності — зокрема, зниження рівня задоволеності працівників своєю роботою, вказують автори дослідження…». ***(Ілля Нежигай. Кіберзлочинці у 2020 році завдали у світі збитків на трильйон доларів – дослідження // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1906706-kiberzlochintsi-u-2020-rotsi-zavdali-u-sviti-zbitkiv-na-trilyon-dolariv-doslidzhennya). 08.12.2020).***

***

«Хакеры создали аукционный сайт в даркнете для продажи 250 000 баз данных, украденных с десятков тысяч взломанных серверов MySQL.

Вся коллекция составляет семь терабайт и является частью бизнеса по выкупу баз данных, который резко вырос с октября.

Рост атак с целью выкупа баз данных

Еще в мае BleepingComputer сообщил о злоумышленнике, который крадет базы данных SQL из интернет-магазинов и угрожает жертвам, что их данные станут общедоступными, если они не заплатят 0,06 BTC.

Хотя на веб-сайте хакера в открытом доступе была указана только 31 база данных, количество сообщений о злоупотреблениях для кошелька, оставленных в записке о выкупе, превышало 200, что указывает на гораздо более крупную операцию.

Исследователи Guardicore наблюдали за этой схемой в течение года и заметили резкий рост активности с 3 октября.

Злоумышленник перешел из чистой сети в темную сеть, создав аукционный сайт, на котором перечислены 250 000 баз данных с 83 000 взломанных серверов, которые были обнаружены в общедоступной сети.

Базы данных MySQL, продаваемые на сайте аукциона, имеют размер от 20 байтов до гигабайт и предлагаются за ту же сумму - 0,03 биткойна или 545 долларов США по текущим ценам.

Основываясь на названиях и размерах выставленных на аукцион баз данных, BleepingComputer считает, что это автоматические атаки. Это связано с тем, что субъект продает не только большие базы данных, но также тестовые базы данных и базы данных по умолчанию, содержащие всего 20 байтов данных.

В опубликованном сегодня отчете Guardicore подтверждает, что данные являются результатом нецелевых автоматических атак, которые используют грубую силу для получения доступа к данным.

Когда злоумышленник взламывает сервер MySQL, он выполняет различные команды, которые архивируют и копируют базы данных в инфраструктуру злоумышленника, удаляют их с сервера жертвы, а затем создают записку о выкупе.

Записка о выкупе создается в новой таблице базы данных с названием «предупреждение», содержащей единственную запись.

Эта запись содержит инструкции для жертвы, которые направляют ее на сайт Tor для выплаты выкупа и предоставляют уникальный токен для доступа к личной странице.

Согласно выводам Guardicore, субъект обеспечивает постоянство, создавая пользователя бэкдора (mysqlbackups '@'% '). Это позволяет им снова скомпрометировать сервер в более позднее время.

Исследователи различают два этапа этой кампании двойного вымогательства, которые показывают эволюцию операции.

В первой записке о выкупе от злоумышленника был биткойн-кошелек, куда жертвы могли отправлять деньги, чтобы получить свои базы данных. Телеметрия Guardicore зафиксировала 63 атаки этого типа с четырех разных IP-адресов.

Сайт аукциона является частью второго этапа кампании и следует тенденции, установленной киберпреступными бандами в бизнесе программ-вымогателей для шифрования файлов, такими как REvil, Netwalker, MountLocker и им подобные.

В беседе с BleepingComputer исследователь Guardicore Офир Харпаз сказал, что есть большая вероятность, что развитие операции может не зависеть от первоначального актера.

Помимо сайта утечки, еще одна подсказка заключается в том, что системы мониторинга Guardicore записали разные наборы IP-адресов для двух этапов.

На данный момент в мире насчитывается около пяти миллионов серверов MySQL, доступных через общедоступный Интернет. Такие автоматические атаки, как эти, постоянно обнаруживают новые цели в попытке взломать их.

Поскольку они основаны на тестировании общих учетных данных, администраторам следует сделать приоритетным использование надежных уникальных паролей для баз данных с важными данными.

Администраторам также следует избегать раскрытия баз данных, если это возможно, или, по крайней мере, разрешить доступ к ним через безопасное, не общедоступное соединение и дополнить эти средства защиты хорошей видимостью сети». ***(Ionut Ilascu. 250,000 stolen MySQL databases for sale on dark web auction site // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/250-000-stolen-mysql-databases-for-sale-on-dark-web-auction-site/). 10.12.2020).***

***

«Более 85 000 баз данных MySQL в настоящее время продаются на темном веб-портале по цене всего 550 долларов за базу данных.

Портал, на который сегодня обратил внимание исследователь безопасности, является частью схемы выкупа базы данных, которая действует с начала 2020 года.

Жалобы на такие атаки на БД можно встретить на Reddit, MySQL форумах, форумы техподдержки, в блогах Medium и частных блогах. Так, хакеры

взламывают базы данных SQL, скачивают их, удаляют оригиналы и оставляют владельцам записки с требованием выкупа, если те хотят вернуть свои данные.

Если изначально жертвам предлагали связаться с злоумышленниками по электронной почте, то со временем хакеры изменили тактику и автоматизировали свою схему с помощью сайта, который сначала размещался на sqldb.to и dbrestore.to, а потом переехал в даркнет.

На сайте жертв просят ввести уникальный идентификатор, указанный в вымогательской записке, после чего пострадавший попадает на страницу, где продаются его данные.

Если жертвы не платят в течение девяти дней, их данные выставляются в открытую продажу, на аукцион в другом разделе сайта.

Стоимость восстановления или покупки украденной базы данных может немного варьировать, так как курс биткоина к доллару часто колеблется. Как правило, выкуп равен примерно 500 долларам в криптовалюте, независимо контента БД и пострадавшего сайта. Из-за этого журналисты полагают, что злоумышленники не анализируют взломанные и украденные БД, и процесс полностью автоматизирован.

Биткоин-адреса, которые использует группы, постепенно накапливаются на сайте BitcoinAbuse.com (1, 2, 3, 4, 5, 6, 7, 8). Отмечается, что атаки этой группы легко узнать, ведь обычно хакеры сопровождают свои требования выкупа заголовком «WARNING».

Судя по всему, большинство взломанных злоумышленниками БД происходят с серверов MySQL, однако нельзя исключать, что могли пострадать и другие системы, включая PostgreSQL и MSSQL». ***(Catalin Cimpanu. Hackers are selling more than 85,000 MySQL databases on a dark web portal // ZDNet (https://www.zdnet.com/article/hackers-are-selling-more-than-85000-sql-databases-on-a-dark-web-portal/). 10.12.2020).***

***

«Спонсируемая государством китайская хакерская группа, также известная как APT, подозревается в взломе монгольской компании-разработчика программного обеспечения и взломе приложения чата, используемого сотнями правительственных агентств Монголии.

Согласно отчету, опубликованному словацкой фирмой ESET, атака предположительно произошла в начале этого года, в июне.

Хакеры атаковали приложение под названием Able Desktop, разработанное местной компанией Able Software. Согласно веб-сайту компании, приложение представляет собой надстройку, которая предоставляет возможности мгновенного обмена сообщениями для основного продукта компании - платформы управления человеческими ресурсами (HRM).

Able Software утверждает, что ее платформа используется более чем 430 правительственными учреждениями Монголии, в том числе Канцелярией президента, Министерством юстиции, Министерством здравоохранения, различными местными правоохранительными органами и многими местными органами власти.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, КОТОРЫМ ЗЛОУПОТРЕБЛЯЮТ ХАКЕРЫ КАК МИНИМУМ С 2018 ГОДА

ESET заявляет, что из-за его широкого использования среди государственных служащих, приложение было в центре нескольких усилий по распространению вредоносных программ как минимум с 2018 года.

Первоначальные атаки заключались в добавлении вредоносного ПО в чат-приложение Able Desktop и распространении троянской версии установщика приложения по электронной почте в надежде заставить сотрудников заразить себя.

Полезная нагрузка в этих атаках включала бэкдор HyperBro и троян удаленного доступа PlugX.

Но, хотя эти атаки были успешными, ESET сообщает, что все изменилось в июне 2020 года, когда злоумышленники, похоже, нашли путь внутрь серверной части Able и скомпрометировали систему, которая доставляет обновления программного обеспечения для всех программных приложений Able.

Исследователи ESET утверждают, что злоумышленники использовали эту систему как минимум дважды, чтобы доставить зараженное вредоносным ПО приложение чата Able Desktop через официальный механизм обновления.

Для этих атак злоумышленники снова использовали бэкдор HyperBro, но они изменили PlugX на Tmanager в качестве компонента удаленного доступа.

На момент написания неясно, использовали ли злоумышленники скомпрометированную функцию обновления Able для установки вредоносного ПО на все системы, к которым они могли добраться, или они преследовали только выбранные цели.

Помимо уведомления Able Software, ESET не смогла предоставить такие подробности.

Кроме того, ESET не смог определить атаку на конкретную группу, поскольку все штаммы вредоносных программ, использованные в атаках, ранее использовались различными APT, связанными с Китаем, такими как LuckyMouse и TA428, а также для набора серверной инфраструктуры. известный как ShadowPad - сам связан со многими другими китайскими APT, такими как CactusPete, TICK, IceFog, KeyBoy и зонтичной группой Winnti.

ESET считает, что эти группы либо сотрудничают, используя одни и те же инструменты, либо являются подгруппами, входящими в более крупный субъект угрозы, который контролирует их операции и нацеливание.

Помимо отчета ESET, компания по кибербезопасности Avast также опубликовала собственный отчет об этих атаках, в котором преступники также были связаны с Китаем и классифицированы как кибершпионаж». ***(Catalin Cimpanu. Chinese APT suspected of supply chain attack on Mongolian government agencies // ZDNet (https://www.zdnet.com/article/chinese-apt-suspected-of-supply-chain-attack-on-mongolian-government-agencies/). 10.12.2020).***

***

«В удивительном и неожиданном объявлении в четверг команда безопасности Facebook раскрыла настоящую личность APT32, одной из самых

активных на сегодняшний день спонсируемых государством хакерских групп, которые, как считается, связаны с правительством Вьетнама.

Компания заявила, что сделала этот шаг после того, как обнаружила, что APT32 использует свою платформу для распространения вредоносных программ в попытках заразить пользователей.

«Наше расследование связывало эту деятельность с CyberOne Group [заархивированный веб-сайт, заархивированная страница Facebook], ИТ-компанией во Вьетнаме (также известной как CyberOne Security, CyberOne Technologies, Hành Tinh Company Limited, Planet and Diacauso)», - сказал Натаниэль Глейхер, глава отдела Политика безопасности в Facebook и Майк Двилянски, менеджер по анализу киберугроз.

Связаться с представителем CyberOne для комментариев по телефону не удалось, так как ранее указанный номер телефона не работал. Письма, отправленные в компанию, не принимаются.

APT32 ИСПОЛЬЗОВАЛ FACEBOOK ДЛЯ ДОСТИЖЕНИЯ ЦЕЛЕЙ

По словам Глейхера и Двилянски, APT32 действовал в Facebook, создавая учетные записи и страницы для вымышленных лиц, обычно выдавая себя за активистов или коммерческих структур.

Используя романтические или другие приманки, группа часто делится ссылками со своими целями на различные домены, которые они либо взламывают, либо управляют самостоятельно.

Ссылки обычно ведут к фишингу или вредоносному ПО или даже включают ссылки на приложения для Android, которые группе удалось загрузить в официальный магазин Play, что позволяет им шпионить за своими жертвами.

Основываясь на своем анализе этой кампании, Facebook заявил, что группа нацелена на такие организации, как:

Вьетнамские правозащитники в стране и за рубежом

Иностранные правительства, в том числе в Лаосе и Камбодже

Неправительственные организации

Информационные агентства, а также предприятия в области информационных технологий, гостеприимства, сельского хозяйства и товаров, больниц, розничной торговли, автомобильной промышленности и мобильных услуг.

Facebook заявил, что помимо удаления учетных записей и страниц группы, они также заблокировали домены группы, поэтому их нельзя повторно использовать под новыми учетными записями, которые APT32 может создать в будущем.

Социальная сеть также поделилась правилами YARA и сигнатурами вредоносных программ, поэтому другие социальные сети и службы безопасности также могут принять меры и защитить своих пользователей.

ДЛИННАЯ ЦЕПОЧКА ХАКОВ

Предполагается, что группа APT32 начала свою работу в 2014 году, ее также часто называют OceanLotus.

Ее прошлые операции являются буквально шведским столом деятельности, и группа была связана с нападениями почти на все, что представляет интерес для вьетнамского государства.

Это не только касалось дел соседних стран, но и нападений на политических диссидентов и активистов, и даже на частный бизнес, который, по мнению группы, представляет интерес для вьетнамского правительства.

Лучшим примером такого таргетинга были широкомасштабные атаки группы на автопроизводителей в 2019 году. В ходе того, что эксперты назвали настойчивой кампанией по краже интеллектуальной собственности в поддержку начинающего автомобильного стартапа VinFast, финансируемого государством Вьетнама, группа ударила и украла данные у подобных от BMW, Hyundai, Toyota Австралии, Toyota Японии, и даже Toyota во Вьетнаме, все подряд, в небольшом временном окне.

Кроме того, когда в начале этого года в мире обрушилась пандемия коронавируса, APT32 также переориентировался на сбор данных о COVID-19, даже на правительственных чиновников в Ухане, Китай, где были зарегистрированы первые случаи заболевания, для поиска информации о болезни.

Эта универсальность в нацеливании является основным продуктом зрелого злоумышленника. Но эта универсальность также распространяется на его арсенал хакерских инструментов. Социальная инженерия, скрытые загрузки, ошибки Office, нестандартное вредоносное ПО, злоупотребление инструментами с открытым исходным кодом, общедоступные эксплойты, вредоносное ПО для macOS - группа использовала их все.

Хотя группа часто игнорируется в отчетах о кибербезопасности из-за ее связи с Вьетнамом, группа часто демонстрирует мастерство в изменении тактики и хакерских инструментов на протяжении многих лет, что является признаком того, что у них есть ресурсы и знания для адаптации.

АТРИБУЦИЯ FACEBOOK БУДЕТ СПОРНОЙ И СПОРНЫМ

Согласно Facebook, эта зрелость проистекает из того факта, что за APT32 стоит реальная фирма по кибербезопасности. Но если Facebook точен в своей атрибуции, еще предстоит увидеть.

Действия Facebook удивительны, если не сказать больше, и обязательно привлекут внимание не только правительственных чиновников Вьетнама и всех взломанных стран, но также и индустрии кибербезопасности.

Это потому, что доксинг групп наций-государств - это то, что до сегодняшнего дня обычно оставалось только прокурорам или анонимным линчевателям.

Фирмы кибербезопасности обычно на цыпочках заявляют о приписывании какого-либо правительства, не говоря уже о связях групп с различными спецслужбами или местными подрядчиками.

Кроме Министерства юстиции США и группы, известной как IntrusionTruth, никто не осмелился перейти эту черту.

Но если мы и узнали что-нибудь, так это то, что Министерство юстиции обычно также читает и изучает любую публичную атрибуцию групп национальных государств. Три из четырех доксингов IntrusionTruth в конечном итоге превратились в официальные дела Министерства юстиции». ***(Catalin Cimpanu.***

Facebook links APT32, Vietnam's primary hacking group, to local IT firm // ZDNet (https://www.zdnet.com/article/facebook-doxes-apt32-links-vietnams-primary-hacking-group-to-local-it-firm/). 11.12.2020).

***

«Хакеры провели кибератаку против логистической компании Orian, группы - разработчика программного обеспечения Amital и еще 38 компаний.

…По оценкам высокопоставленных представителей кибериндустрии, скорее всего, за нападением стоит не группировка независимых хакеров, а некие враждебные Израилю элементы или даже государство.

Такой вывод можно сделать из того, что хакеры не предъявили ни Orian, ни другим жертвам никаких финансовых требований». ***(40 израильских фирм подверглись кибератаке // ISRAland Online (http://www.isra.com/news/253363). 13.12.2020).***

***

«Группа иранских хакеров Pay2Key, целенаправленно действующих против Еврейского государства, в воскресенье, 20 декабря, на своем аккаунте в "Твиттер" заявила о взломе компьютеров нескольких компаний, в том числе, ведущего израильского концерна ВПК "Таасия авирит" ("Авиационная промышленность Израиля").

"Тук-тук! Эта ночь длиннее, чем самая длинная ночь для "Таасия авирит", - написали хакеры, разместив логотип концерна.

В "Авиационной промышленности" сообщили, что проверяют эту информацию, отмечает Walla.

Стало известно, что взломаны серверы "Альта", дочерней компании "Таасия авирит". Взломщики опубликовали личные данные больше тысячи сотрудников компании, включая высокопоставленных представителей отдела по обеспечению кибербезопасности. "Альта" считается одной из ведущих компаний в сфере военных электронных систем радаров, связи и радиоэлектронной борьбы.

Примерно в 18:30 pay2key опубликовала сообщение с указанием названий компьютеров, имен сотрудников, в том числе руководителей, а также последовательности букв и цифр, из которых можно было составить адреса электронной почты. Таким образом хакеры доказывают, что произвели взлом системы.

"Самое интересное, что мы получили доступ к серверам компании, включая техническую документацию, видеоролики, исследования, проекты и разработки. Есть ли они у нас? Никогда не знаешь, - написали представители группы. - Вы все еще думаете, что у них самая безопасная сеть"?

Запрос на вымогательство еще не опубликован.

Ранее хакерская группа бросила вызов израильским компаниям, написав у себя в профиле в "Твиттер": "Зима близко для израильской аэрокосмической промышленности. От Pay2Key с любовью!"

За последнюю неделю эта группа произвела и скоординировала кибератаки на как минимум 80 израильских компаний, в том числе, фирму-производителя процессоров Habana Labs, которую приобрел Intel.

Три дня назад злоумышленники провели опрос на своей странице: "Какая сеть наиболее безопасна? Угадайте". Ниже они отметили три варианта: "Авиационная промышленность Израиля", министерство транспорта и министерство здравоохранения.

Позже на сайте скрытых сервисов Darknet хакеры написали: "Дорогие друзья, вы проголосовали, что в аэрокосмической отрасли должна быть самая безопасная сеть. Вероятно, они так и считают. Давайте приступим".

Омри Сегев, гендиректор компании Profero, действующей в сфере кибербезопасности, сообщил "Хаарец", что иранская кибератака готовилась долго и тщательно, и сейчас иранские хакеры набирают темп, намереваясь нанести максимальный ущерб Израилю в сети.

По словам Сегева, не стоит недооценивать иранских хакеров, потому что большая часть израильских сайтов, начиная от сайтов и серверов частных компаний и даже вплоть до инфраструктурных объектов не защищены перед подобным изощренным и профессиональным врагом.

Впервые группу Pay2Key израильские компании, работающие в сфере кибербезопасности Check Point Whitestream, обнаружили в ноябре. Израильские эксперты сначала решили, что это очередная компания, занимающаяся кибершантажом, хотя и более профессиональная.

Такие группы действуют, как правило, по одному сюжету. Они взламывают серверы компании, часть информации скачивают себе, часть кодируют, чтобы к ней нельзя было получить доступа, а затем требуют крупный выкуп в криптовалюте в обмен на получение ключа, позволяющего расшифровать зашифрованные данные.

В последнее время они начали действовать по принципу "двойное вымогательство". Помимо шантажа они публикуют в сети фрагменты похищенных данных, чтобы подстегнуть жертву к выплате выкупа. И Pay2Key действует именно таким образом.

Израильские эксперты отследили предыдущие транзакции, которые показали, что выплаченные биткоины были переведены в иранскую криптовалюту Excoino. Но в Check Point сразу отметили, что речь идет не об обычных киберпреступниках, а о профессионально действующей группе хакеров. Им удается захватить контроль над всей сетью в течение часа, тогда как обычные киберпреступники могут потратить на это много часов, а то и несколько дней.

Эта группа действовала очень терпеливо, на протяжении недель, а то и месяцев незаметно проникая в систему и изучая все ее слабости. В итоге, о взломе стало известно лишь тогда, когда хакеры сами сообщили об украденных данных. При этом, в отличие от рядовых киберпреступников, иранские хакеры тщательно подчищали за собой следы, чтобы их было сложно вычислить.

Если изначально взлом серверов израильских фирм и организаций осуществлялся с политическими и идеологическими мотивами, то в последние месяцы антиизраильски настроенные хакеры начали требовать также денежный

выкуп, что стирает различия между хактивизмом и киберпреступностью». ***(Войны XXI века: иранские хакеры взломали серверы дочерней компании концерна «Таасия авирит» // ДЕТАЛИ (https://detaly.co.il/iranskie-hakery-obyavivshie-vojnu-izrailyu-my-vzlomali-servery-taasiya-avirit/). 20.12.2020).***

***

«В Беларуси хакеры взломали внутреннюю информационную сеть отделов принудительного исполнения при белорусском Минюсте. Взломщики начали транслировать на компьютерах сотрудников видеоролик политического характера.

Как сообщает портал Tut.by, инцидент произошел еще 22 декабря, когда в отделениях ведомства внезапно перестали исправно функционировать рабочие компьютеры, а из баз данных пропали документы. Позже на экранах у силовиков начал транслироваться видеоролик с человеком в костюме Санта-Клауса и маске Гая Фокса. Он оставался включенным в течение нескольких часов.

Хакер сообщил, что ему удалось скачать терабайты персональных данных исполнителей, а также восхитился действиями правоохранителей, тайно помогающих участникам акций протестов. В итоге «Санта» пожелал силовикам оставаться человечными, и пообещал никогда не забыть и не допустить повторения уходящего года». ***(Белорусские силовики получили послание от «Санты» // SecurityLab.ru (https://www.securitylab.ru/news/515094.php). 25.12.2020).***

***

Вірусне та інше шкідливе програмне забезпечення

«Китайське бюро кібербезпеки Міністерства громадської безпеки розіслало попередження через WeChat про те, що користувачам не слід застосовувати чужі пауербанки. Справа в тому, що через них може поширюватися вірус, а точніше троянська програма.

Експерти з кібербезпеки розповіли, що заражені зовнішні акумулятори можуть виконувати два завдання. Перша – вкрасти особисті дані зі смартфона, в тому числі фото, відео, повідомлення та т.д. Друга – вбудувати троянця або іншу шкідливу програму. Це ПО може красти дані з пристрою протягом тривалого часу, завантажувати рекламу і навіть управляти апаратом

Кращий спосіб уникнути проблем – не користуватися загальними пауербанками, особливо в громадських місцях. Також користувачам Android-смартфонів радять не включати режим розробника (Developer Mode), так як пристрій в такому режимі більш вразливий до атак». ***(Митник Михайло. Віруси навчилися передавати через зовнішні акумулятори для смартфонів // TechnoPortal.com.ua (https://technoportal.com.ua/smartfony/56184). 09.12.2020).***

***

«Компания Eset сообщает о выявлении ранее неизвестного бэкдора под названием Crutch и программы для похищения документов. Эти вредоносные

инструменты для кибершпионажа, которые использовались с 2015 г. по крайней мере до начала 2020 г., исследователи связывают с известной киберпреступной группой Turla.

Исследователи Eset обнаружили бэкдор Crutch в сети «Министерства иностранных дел» одной из стран Европейского Союза, что позволяет предположить сосредоточенность киберпреступников на конкретных целях. Эти инструменты были разработаны для загрузки похищенных конфиденциальных документов и других файлов в учетные записи Dropbox, которые контролировались операторами Turla.

«Основная вредоносная деятельность группы Turla – это похищение документов и других конфиденциальных файлов. Утонченность атак и выявленные технические детали подтверждают наличие значительных ресурсов у группы Turla для работы с таким большим и разнообразным арсеналом, – комментирует Матье Фау (Matthieu Faou), исследователь Eset. – Кроме того, Crutch может обойти некоторые уровни безопасности, несанкционированно используя легитимную инфраструктуру, в данном случае Dropbox, с целью проникновения в обычный сетевой трафик и похищения документов».

Для понимания часов работы киберперступников исследователи Eset изучили время загрузки ZIP-файлов в учетные записи Dropbox. Для этого были собраны 506 разных временных меток в период с октября 2018 по июль 2019 г., которые указывают на часы активности злоумышленников, а не работы устройств жертв. Соответственно операторы, скорее всего, работают в часовом поясе UTC+3.

В ходе исследования специалисты Eset выявили связь между загрузчиком Crutch 2016 г. и Gazer. Последний, также известный как WhiteBear, является дополнительным бэкдором, который использовался киберпреступниками Turla в 2016-2017 гг…». ***(Группировка Turla использует Dropbox в кампаниях кибершпионажа // Компьютерное Обозрение(https://ko.com.ua/gruppirovka_turla_ispolzuet_dropbox_v_kampaniyah_kibershpionazha_135515). 03.12.2020).***

***

«Русскоязычные хакеры, стоящие за вредоносным ПО Zebrocy, изменили свою технику доставки вредоносного ПО известным жертвам и начали упаковывать угрозы в виртуальные жесткие диски (VHD), чтобы избежать обнаружения.

Этот метод был замечен в недавних целевых фишинговых кампаниях группы угроз APT28 (Fancy Bear, Sofacy, Strontium, Sednit) для заражения целевых систем с помощью варианта набора инструментов Zebrocy.

Новые варианты Zebrocy обладают низким уровнем обнаружения

Zebrocy поддерживает множество языков программирования (AutoIT, C ++, C #, Delphi, Go, VB.NET). Для недавних кампаний злоумышленник выбрал версию на основе Golang вм**есто более распространенной версии Delphi.

Windows 10 изначально поддерживает файлы VHD и может монтировать их как внешние диски, чтобы пользователи могли просматривать файлы внутри. В

прошлом году исследователи безопасности обнаружили [1, 2], что антивирусные движки не проверяют содержимое VHD, пока не смонтированы образы дисков.

В конце ноября исследователи Intezer обнаружили VHD, загруженный на платформу сканирования Virus Total из Азербайджана. Внутри изображения находились PDF-файл и исполняемый файл, представляющий собой документ Microsoft Word, который является вредоносной программой Zebrocy.

PDF-файл представляет собой презентацию о Sinopharm International Corporation, китайской фармацевтической компании, которая в настоящее время проходит третий этап испытаний вакцины против COVID-19.

Вариант Zebrocy в файле VHD - новый вариант, который мало обнаруживается в Virus Total. На 30 ноября вредоносное ПО обнаружили только девять из 70 машин.

Однако анализ Intezer показал, что новый Zebrocy генетически похож на вариант Delphi, который год назад использовался в кампании против целей в Азербайджане.

Файлы VHD, используемые в других кампаниях

Основываясь на ключах к вредоносному VHD, исследователи обнаружили, что злоумышленник проводил аналогичные кампании как минимум с октября.

Другие образы дисков, использованные в качестве фишинговых приманок, были загружены на Virus Total: один из них 12 ноября из Казахстана, а другой с отметкой времени создания 21 октября.

Оба последних изображения VHD включали в себя образец Zebrocy, олицетворяющий документ Microsoft Word и файл PDF, и у них одинаковый идентификатор диска.

Однако самая старая из них поставляла версию вредоносного ПО на основе Delphi и использовала приманку в формате PDF, написанную на русском языке.

Zebrocy используется годами и представляет собой набор загрузчиков, дропперов и бэкдоров. Вариант, основанный на Голанге, был обнаружен в прошлом году и периодически использовался хакерами.

Использование образов VHD-дисков кажется новой страницей в книге доставки вредоносных программ группы угроз, стоящей за Zebrocy. Этот метод ранее использовался в фишинговых операциях группы Cobalt по распространению загрузчика CobInt в конце декабря 2019 года.

В своем отчете, опубликованном сегодня, Intezer предоставляет индикаторы компрометации для управляющего сервера, файлов VHD и образцов вредоносного ПО Zebrocy, которые использовались в недавних фишинговых кампаниях. ***(Ionut Ilascu. Russian hackers hide Zebrocy malware in virtual disk images // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/russian-hackers-hide-zebrocy-malware-in-virtual-disk-images/). 09.12.2020).***

***

«Разработчики вредоносного ПО TrickBot создали новый модуль, который исследует уязвимости UEFI, демонстрируя усилия злоумышленника по отражению атак на уровне, который дал бы им полный контроль над зараженными машинами.

Имея доступ к прошивке UEFI, злоумышленник установит на скомпрометированном компьютере постоянство, которое сопротивляется переустановке операционной системы или замене накопителей.

Вредоносный код, внедренный в прошивку (буткиты), невидим для решений безопасности, работающих поверх операционной системы, потому что он загружается раньше всего на начальном этапе последовательности загрузки компьютера.

Буткиты позволяют контролировать процесс загрузки операционной системы и саботировать защиту на более высоком уровне. Поскольку код запускается на самой ранней стадии, механизм безопасной загрузки не помогает, так как он зависит от целостности прошивки.

Последствия, связанные с получением злоумышленником такого постоянного присутствия на машине, огромны, особенно в случае TrickBot, чье среднее ежедневное заражение может достигать нескольких тысяч.

Ориентация на платформы Intel

Сегодня в совместном отчете бутика кибербезопасности Advanced Intelligence (AdvIntel) и исследователей из фирмы Eclypsium, занимающейся аппаратным обеспечением и безопасностью, представлены технические подробности о новом компоненте TrickBot.

На этом этапе TrickBoot действует как средство разведки, проверяя наличие уязвимостей в прошивке UEFI зараженной машины. На данный момент проверка нацелена только на платформы Intel (Skylake, Kaby Lake, Coffee Lake, Comet Lake). Тем не менее, модуль также включает в себя код для чтения, записи и стирания прошивки, поэтому его можно использовать для значительных повреждений.

Он проверяет, активна ли защита от записи UEFI / BIOS, с помощью драйвера RwDrv.sys от RWEverything, бесплатной утилиты, которая обеспечивает доступ к аппаратным компонентам, таким как микросхема флэш-памяти SPI, в которой хранится прошивка BIOS / UEFI системы.

Если название инструмента звучит как колокол, это потому, что он использовался LoJax, первым руткитом UEFI, обнаруженным в дикой природе, в результате атаки российских хакеров, известных как APT28 (Fancy Bear, Sednit, Strontium, Sofacy)…

Исследователи говорят, что защита от записи BIOS / UEFI доступна в современных системах, но эта функция часто не активна или неправильно настроена, что позволяет злоумышленникам изменить прошивку или удалить ее, чтобы заблокировать устройство.

Исследователи обнаружили модуль 19 октября и назвали его TrickBoot, каламбуром за его функциональность и название вредоносного ботнета, которое его развертывает.

В образце, проанализированном Advanced Intelligence, исследователи обнаружили имя «PermaDll», связанное с файлом «user_platform_check.Dll» в новом образце TrickBot.

Изучение файла с помощью Eclypsium показало, что злоумышленник реализовал механизм, который проверял однокристальный чипсет в скомпрометированной системе.

Исследователи обнаружили, что роль модуля заключалась в выполнении запросов PCH для определения конкретной модели PCH, запущенной в системе, таким образом идентифицируя платформу. Эта информация также позволяет злоумышленнику проверить, уязвима платформа или нет.

Исследователи также обнаружили, что актер использует функции известного инструмента эксплуатации встроенного ПО и библиотеки под названием fwexpl для следующих целей:

- читать данные с аппаратных портов ввода-вывода
- вызвать драйвер rwdrv.sys для записи данных в аппаратные порты ввода-вывода
- вызвать драйвер rwdrv.sys для чтения данных из адресов физической памяти
- вызвать драйвер rwdrv.sys для записи данных по адресам физической памяти

Исследователи отмечают, что если TrickBoot работает на платформе, отсутствующей в его таблице поиска, он активирует функцию с предварительно установленным Skylake набором значений по умолчанию для операций, требующих доступа к оборудованию.

После идентификации платформы TrickBoot обращается к путям, связанным с регистрами чтения для флэш-памяти (SPIBAR, PRO-PR4) и управлением BIOS (BC - содержит биты блокировки защиты от записи для доступа к BIOS на аппаратном уровне).

Интересной находкой в функции, которая пытается отключить защиту от записи BIOS, является то, что она содержит ошибку, которая считывается с неправильного смещения в регистре управления BIOS, чтобы проверить, установлен ли бит отключения защиты от записи BIOS. Это приводит к тому, что код интерпретирует, что защита от записи активна, и пытается ее отключить.

Основные последствия

Разработка TrickBot такого модуля явным образом свидетельствует о том, что злоумышленник прилагает усилия для расширения своего контроля над скомпрометированными системами. В ботнете уже есть тысячи зараженных машин, на которых злоумышленник может выбирать наиболее ценные цели.

Телеметрия AdvIntel показывает, что ежедневное количество заражений TrickBot с 3 октября по 21 ноября достигло пика - 40 000, а в среднем - от 200 до 4 000. Эти цифры консервативны, поскольку в них не учитываются зараженные компьютеры в частных сетях, которые взаимодействуют извне, используя IP-адрес шлюза.

Выбор наиболее прибыльных жертв осуществляется вручную на основе данных, полученных с помощью сценариев разведки, которые извлекают информацию из сетей, оборудования и программного обеспечения жертвы.

Операторы финансово мотивированы и используют ботнет для доставки программ-вымогателей Ryuk и Conti на дорогостоящие машины. С 2018 года они заработали не менее 150 миллионов долларов. Только у одной недавней жертвы они взяли 2200 BTC (на тот момент они оценивались в 34 миллиона долларов).

TrickBot - действительно киберпреступное предприятие, вовлеченное в несколько схем зарабатывания денег, включая банковское мошенничество и кражу финансовой / личной информации.

Обеспечение устойчивости на уровне UEFI на дорогостоящих машинах может максимизировать прибыль участников, поскольку они могут использовать это преимущество несколькими способами.

Помимо использования имплантатов UEFI в качестве рычага в переговорах по увеличению цены выкупа, киберпреступники могут сохранить доступ к машинам даже после того, как жертва заплатит им за освобождение систем от контроля TrickBot.

Позже, после того как жертва завершит процессы очистки и восстановления, субъект может воспользоваться своим постоянным присутствием в коде UEFI для запуска новой атаки. Они также могут собрать вновь установленные учетные данные для доступа и продать их другой банде.

Более того, это может быть использовано в операциях с чисто разрушительной целью, поскольку это может повлиять на большие операционные среды и критическую инфраструктуру. Еще одним эффектом блокировки устройств является то, что это значительно затрудняет судебное расследование, значительно замедляет процесс восстановления и нарушает другие уровни безопасности.

Действия защиты жесткие

Джесси Майкл, главный исследователь Eclypsium, сказал BleepingComputer, что определение того, была ли система взломана на уровне прошивки UEFI, является сложной задачей.

Более тщательный метод состоит в том, чтобы прочитать содержимое микросхемы памяти SPI, когда система отключена, путем физического подключения устройства программирования флэш-памяти SPI. Однако это решение требует не только опыта, но и длительного простоя компании, поскольку в некоторых случаях микросхема припаяна к материнской плате, и это сопряжено с риском проблем с чтением.

Другой метод - использовать инструменты с открытым исходным кодом (CHIPSEC) или платформу Eclypsium, которая ищет слабые места на низком уровне на уровне оборудования и прошивки, а также может определить, активна ли защита от записи BIOS.

Проверка хэшей прошивки также помогает определить, не был ли изменен код. Кроме того, обновление прошивки - хороший способ убедиться, что она не подвержена известным уязвимостям.

Компрометация на уровне UEFI - редкость даже в наши дни, спустя более пяти лет с тех пор, как код имплантата VectorEDK UEFI от Hacking Team просочился и стал общедоступным.

В настоящее время публично задокументированные атаки такого рода исходят от высокоразвитых, поддерживаемых государством злоумышленников - Lojax от российских хакеров и MosaicRegressor от китайских хакеров, использующих код VectorEDK.

Однако атаки этих злоумышленников являются очень целевыми, в отличие от TrickBot, цель которого - заразить как можно больше систем и выбрать из этого пула ценные цели (крупные компании из любого сектора).

На основе анализа образца TrickBoot модуль только идентифицирует оборудование и проверяет, доступна ли запись в область BIOS. Но это можно легко изменить, чтобы разрешить запись во флэш-память SPI и изменить прошивку системы.

Технический отчет от AdvIntel и Eclypsium содержит индикаторы взлома TrickBoot вместе с правилом Yara, созданным Виталием Кремезом для этого нового модуля». ***(Ionut Ilascu. TrickBot's new module aims to infect your UEFI firmware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/trickbots-new-module-aims-to-infect-your-uefi-firmware/). 03.12.2020).***

***

«Множество техник обфускации подогревают горячую точку для операции взлома по найму.

Группа DeathStalker с повышенной устойчивой угрозой (APT) имеет новое горячее оружие: очень скрытный бэкдор, который исследователи назвали PowerPepper, используемый для слежки за целевыми системами.

По словам исследователей Kaspersky, DeathStalker предлагает услуги наемников и шпионажа, нацеленные на финансовый и юридический секторы. Они отметили, что группа существует как минимум с 2012 года (впервые была замечена в 2018 году), используя тот же набор относительно базовых методов, тактик и процедур (ДТС) и продавая свои услуги лицу, предлагающему самую высокую цену. Однако в ноябре группа была обнаружена с использованием нового имплантата вредоносного ПО с другой тактикой укрытия.

«DeathStalker на протяжении многих лет использовал несколько штаммов вредоносных программ и цепочек доставки, от Janicab на Python и VisualBasic до Powersing на основе PowerShell, минуя Evilnum на основе JavaScript», - говорится в сообщении исследователей в четверг . «DeathStalker также постоянно использует методы защиты от обнаружения и обхода вирусов, а также сложные цепочки доставки, которые могут сбрасывать множество файлов в файловые системы цели».

Однако эта конкретная вредоносная программа выделяется тем, что повышает уровень своей тактики уклонения.

Продвинутая тактика уклонения

Недавно обнаруженный бэкдор приукрашивает ситуацию на фронте обфускации, используя DNS поверх HTTPS в качестве канала связи, чтобы скрыть связь с системой управления и контроля (C2) за легитимным трафиком.

«PowerPepper регулярно опрашивает сервер C2 на предмет выполнения команд», - утверждают исследователи. «Для этого имплант отправляет DNS-запросы типа TXT (с DoH или обычными DNS-запросами, если последний не работает) на серверы имен (NS), которые связаны с вредоносным доменным именем C2… сервер отвечает DNS ответ, встраивающий зашифрованную команду».

PowerPepper также добавляет стеганографию к списку техник уклонения, которые представляют собой практику сокрытия данных внутри изображений. В этом случае вредоносный код внедряется в обычные изображения папоротников или перцев (отсюда и название), а затем извлекается сценарием загрузчика. Загрузчик замаскирован под средство проверки от поставщика услуг идентификации GlobalSign.

Кроме того, он использует настраиваемую обфускацию, при этом части его вредоносных сценариев доставки скрыты во встроенных в Word объектах, по словам исследователей: «Связь с имплантатом и серверами зашифрована, и благодаря использованию надежных подписанных сценариев антивирусное программное обеспечение не работает. обязательно распознает имплант как вредоносный при запуске».

Другие способы уклонения, такие как обнаружение движения мыши, фильтрация MAC-адресов клиента, обработка приложений Excel и инвентаризация антивирусных продуктов, дополняют его набор уловок.

Подстегивая компании шпионажем

PowerPepper был разработан для выполнения удаленных команд оболочки, отправляемых операторами DeathStalker, которые направлены на кражу конфиденциальной деловой информации.

Команды охватывают весь спектр шпионских программ, в том числе для сбора информации о пользователях и файлах компьютера, просмотра сетевых файловых ресурсов, загрузки дополнительных двоичных файлов или копирования содержимого в удаленные места.

PowerPepper обычно распространяется через адресную фишинговую рассылку с вредоносными файлами, доставляемыми в теле письма или по вредоносной ссылке, что типично для DeathStalker. «Лаборатория Касперского» обнаружила приманки, связанные с международными событиями, правилами выбросов углерода и пандемией, причем электронные письма приходили в первую очередь в Европу, но также и в Америку и Азию. Пока что основными целями PowerPepper являются малые и средние организации - организации, которые, как правило, имеют менее надежные программы безопасности.

«PowerPepper еще раз доказывает, что DeathStalker является творческим субъектом угроз: он способен последовательно разрабатывать новые имплантаты и цепочки инструментов за короткий период времени», - сказал Пьер Делчер, эксперт по безопасности Kaspersky, в своем заявлении. «PowerPepper - уже четвертый штамм вредоносного ПО, связанный с этим злоумышленником, и мы обнаружили потенциальный пятый штамм. Несмотря на то, что они не особенно сложные, вредоносное ПО DeathStalker оказалось довольно эффективным». ***(Tara Seals. DeathStalker APT Spices Things Up with PowerPepper Malware // Threatpost (https://threatpost.com/deathstalker-apt-powerpepper-malware/161867/). 03.12.2020).***

***

«Компанія Avast, яка спеціалізується на кібербезпеці, попередила про виявлену небезпеку. Понад три мільйони користувачів встановили 28 шкідливих розширення Google Chrome і Microsoft Edge.

Точніше, як мінімум у 28 сторонніх розширеннях для Google Chrome і Microsoft Edge фахівці виявили приховане шкідливе ПЗ. Розширення пов'язані з дуже популярними в світі платформами: Video Downloader для Facebook, Vimeo Video Downloader, Instagram Story Downloader і VK Unblock.

Шкідливе ПО може перенаправляти користувачів на рекламні або фішингові сайти, красти особисті дані, наприклад, дати народження, адреси електронної пошти та інформацію про активні пристроях. З огляду на кількість завантажень цих розширень в магазинах додатків, у всьому світі можуть постраждати близько трьох мільйонів чоловік.

Дослідник шкідливого ПО в Avast Ян Рубін зазначив:

"Ми припускаємо, що або розширення були спеціально створені з використанням вбудованого шкідливого ПО, або автори дочекалися, поки розширення стануть популярними, а потім випустили оновлення, що містить шкідливі програми. Також можливо, що розробники продали оригінальні розширення комусь ще після їх створення, а потім покупець створив шкідливе ПО".

На даний момент заражені розширення все ще доступні для завантаження. Avast зв'язалася з командами Microsoft і Google Chrome і повідомила про знахідки. І Microsoft, і Google підтвердили, що в даний час вивчають цю проблему. Зараз Avast рекомендує користувачам відключити або видалити розширення на час, поки проблема не буде вирішена, а потім виконати просканувати ПК і видалити шкідливі програми». ***(Мільйони користувачів встановили 28 шкідливих розширень Google Chrome і Microsoft Edge // SVOBODA.FM (http://svoboda.fm/ukraine/277196.html). 19.12.2020).***

***

«Команда исследователей из компании Check Point Research предоставила отчет, касающийся кибератак, осуществленных в ноябре текущего года.

Наиболее активным и опасным вирусом специалисты посчитали ботнет Phorpiex, который используется для шантажа пользователей интимными фотографиями или видеороликами. Именно он в прошлом месяце был наиболее активным в Сети.

Указанный ботнет орудует в Сети с 2010 года и постоянно совершенствуется. Помимо шантажа, он также распространяет другое вредоносное программное обеспечение.

На втором месте по активности в ноябре оказался банковский троян Dridex, который отправляет информацию о заражённом компьютере на удалённый сервер.

На третьем месте рейтинга расположился вирус для Android — Hiddad. С его помощью вредоносное ПО получает права суперпользователя и ворует данные владельца смартфона». ***(Названы три самых активных вируса в мире // iLenta.com (https://ilenta.com/news/internet/news_31187.html). 19.12.2020).***

***

«Исследователи в области безопасности обнаружили новую разновидность вредоносного ПО с возможностями шпионажа и наблюдения,

известную также как шпионское ПО, которое в настоящее время доступно как для Android, так и для iOS.

Названный Goontact, это вредоносная программа имеет возможность собирать от зараженных данных жертв, таких как телефонные идентификаторы, контакты, SMS сообщения, фотографии и информации о местоположении.

Вредоносное ПО Goontact, обнаруженное компанией Lookout, занимающейся мобильной безопасностью, в настоящее время распространяется через сторонние сайты, предлагающие бесплатные приложения для обмена мгновенными сообщениями, предназначенные для доступа к службам сопровождения.

Целевая аудитория этих сайтов в настоящее время ограничена китайскоязычными странами, Кореей и Японией, говорится в отчете Lookout…

Хотя вредоносная программа еще не достигла официальных магазинов приложений Apple и Google, есть признаки того, что пользователи загружают и загружают неопубликованные приложения, зараженные Goontact.

Данные, собранные из этих приложений, отправляются обратно на онлайн-серверы под контролем операторов Goontact. Исходя из языка, используемого для административных панелей этих серверов, Lookout считает, что операция Goontact, скорее всего, управляется китайскоязычными злоумышленниками.

ССЫЛКИ ПРЕДПОЛАГАЮТ СВЯЗЬ С ПРОШЛОЙ КАМПАНИЕЙ ПО СЕКСТОРЦИИ

Апурва Кумар, инженер службы безопасности и разведки в Lookout, сказала ZDNet, что операция Goontact очень похожа на кампанию по изъятию, описанную Trend Micro в 2018 году.

Хотя на данный момент нет никаких вещественных доказательств, Кумар считает, что данные, собранные с помощью этих приложений, впоследствии могут быть использованы для вымогательства у жертв с целью выплаты небольшого выкупа или для их попыток организовать сексуальные контакты с друзьями и знакомыми.

«Мы уведомили Google и Apple об этой угрозе и активно сотрудничаем с ними, чтобы защитить всех пользователей Android и iOS от Goontact», - сказал Кумар ZDNet в электронном письме в минувшие выходные.

«Apple отозвала корпоративные сертификаты, используемые для подписи приложений, и в результате приложения перестанут работать на устройствах», - добавил инженер по безопасности Lookout.

«Play Protect уведомит пользователя, если на его устройстве установлены какие-либо образцы Goontact Android».

Список имен всех приложений, зараженных Goontact, довольно исчерпывающий и слишком длинный, чтобы перечислять его здесь, но его можно найти в конце этого отчета Lookout, на случай, если пользователи захотят проверить, загрузили ли они и установили какое-либо из приложения...» ***(Catalin Cimpanu. New Goontact spyware discovered targeting Android and iOS users // ZDNet (https://www.zdnet.com/article/new-goontact-spyware-discovered-targeting-android-and-ios-users/). 16.12.2020).***

***

«На этой неделе исследователи безопасности обнаружили операцию ботнета, нацеленную на базы данных PostgreSQL для установки майнера криптовалюты.

Ботнет, названный исследователями под кодовым названием PgMiner, является лишь последним в длинном списке недавних киберпреступлений, нацеленных на веб-технологии для получения денежной прибыли.

По словам исследователей из подразделения 42 Palo Alto Networks, ботнет работает, выполняя атаки методом перебора на доступные в Интернете базы данных PostgreSQL.

Атаки проходят по простой схеме.

Ботнет случайным образом выбирает диапазон общедоступной сети (например, 18.xxx.xxx.xxx), а затем перебирает все части этого диапазона IP-адресов в поисках систем, в которых порт PostgreSQL (порт 5432) открыт в сети.

Если PgMiner находит активную систему PostgreSQL, ботнет переходит от фазы сканирования к фазе грубой силы, где он перебирает длинный список паролей в попытке угадать учетные данные для «postgres», учетной записи PostgreSQL по умолчанию.

Если владельцы базы данных PostgreSQL забыли отключить этого пользователя или забыли изменить его пароли, хакеры получают доступ к базе данных и используют функцию PostgreSQL КОПИРОВАТЬ из ПРОГРАММЫ, чтобы расширить свой доступ из приложения базы данных к базовому серверу и взять на себя всю ОС.

После того, как они получат более надежный контроль над зараженной системой, команда PgMiner развертывает приложение для добычи монет и пытается добыть как можно больше криптовалюты Monero, прежде чем они будут обнаружены.

Согласно Unit 42, на момент написания отчета ботнет имел возможность развертывать майнеры только на платформах Linux MIPS, ARM и x64.

Другие примечательные особенности ботнета PgMiner включают тот факт, что его операторы контролируют зараженных ботов с помощью сервера управления и контроля (C2), размещенного в сети Tor, и что кодовая база ботнета напоминает ботнет SystemdMiner

PgMiner отмечает второй раз, когда операция по добыче монет нацелена на базы данных PostgreSQL, аналогичные атаки наблюдались в 2018 году, совершенные ботнетом StickyDB.

Другие технологии баз данных, которые в прошлом также были мишенью для крипто-майнинговых ботнетов, включают MySQL, MSSQL, Redis и OrientDB». ***(Catalin Cimpanu. PgMiner botnet attacks weakly secured PostgreSQL databases // ZDNet (https://www.zdnet.com/article/pgminer-botnet-attacks-weakly-secured-postgresql-databases/). 13.12.2020).***

***

«Посетители метро в Великобритании получили сегодня утром подозрительные электронные письма, и исследователи информационной

безопасности опасаются, что это связано с кражей данных о клиентах и кампанией вредоносного ПО Trickbot…

Сегодня утром на аккаунт Subway UK прокатилась волна твитов, когда люди задавались вопросом, почему сеть сэндвичей на вынос, известная своими не совсем длинными багетами, начала рассылать им электронные письма совершенно неожиданно.

Исследователь безопасности Оливер Хаф, известный автор твитов по информационной безопасности, обратил внимание на очевидную фишинговую кампанию. В электронных письмах, которые он видел, ссылки приводили пользователей к заминированной таблице XLS, а другие говорили, что это очень похоже на то, что они вели ничего не подозревающих пользователей прямо к заражению Trickbot.

Trickbot - это банковский троян, который крадет информацию онлайн-банкинга и личные данные, чтобы преступники могли затем совершить мошенничество с личными данными. Как Национальный центр Cyber Security ставит его: «Trickbot целевые жертвы с хорошо продуманной фишинговых писем, предназначенных появляться как бы отправлены из надежных коммерческих или государственных брендов Эти письма часто содержат вложение (или ссылка на файл), жертвами которого являются получил указание открыть, что приведет к эксплуатации их машины».

Исходный код одного из подозрительных писем, отправленных на Github разработчиком PHP Ричардом Бэруэллом, показал полные заголовки сообщений, которые, по-видимому, указывают на электронную почту компании Campaign Monitor в качестве источника сообщения.

Бэруэлл сообщил The Register, что сегодня он получил два подозрительных письма по ссылке выше, добавив: «Оба письма - как и все письма от Subway, по крайней мере, с мая прошлого года - пришли через CampaignMonitor / cmail.com».

Похоже, что злоумышленники могли получить доступ к системам электронной почты Subway, в свете того, что электронное письмо этим утром, по-видимому, было отправлено законным путем, ранее использовавшимся для подлинных маркетинговых сообщений.

Вчера компания быстрого питания изменила свое приложение для обеспечения лояльности потребителей, перейдя со старого приложения Subcard на приложение с простым названием Subway.

Мы попросили Subway прокомментировать как очевидное нарушение, так и фишинговую кампанию, и обновим эту статью, если получим ответ от частной сети в США. ®

Обновлено, чтобы добавить

Subway отправила нам следующее заявление: «Нам известно о некоторых сбоях в работе наших систем электронной почты, и мы понимаем, что некоторые из наших гостей получили несанкционированное электронное письмо. В настоящее время мы расследуем этот вопрос и приносим извинения за любые неудобства. Как только мы получим дополнительную информацию, мы свяжемся с вами, а до тех пор, в качестве меры предосторожности, мы рекомендуем гостям удалить письмо». ***(Gareth Corfield. Subway email weirdness: Suspicion grows over apparent Trickbot***

trojan delivery campaign // The Register(https://www.theregister.com/2020/12/11/subway_email_oddity_trickbot_links/). 11.12.2020).

***

«Эксперты компании Sonatype обнаружили в официальном репозитории RubyGems вредоносные пакеты pretty_color и ruby-bitcoin. В настоящее время вредоносы уже удалены с платформы.

Спрятанная в упомянутых пакетах малварь была нацелена на Windows-машины и подменяла адреса любых криптовалютных кошельков в буфере обмена на адрес кошелька злоумышленников. В сущности, малварь помогала хакерам перехватывать транзакции и воровать чужую криптовалюту.

Исследователи пишут, что pretty_color содержал легитимные файлы colorize, известного и надежного опенсорсного компонента, что затрудняло обнаружение угрозы.

«Фактически, pretty_color является идентичной копией пакета colorize и содержит весь его код, включая полный файл README», — гласит отчет экспертов.

Также в пакет входил файл с именем version.rb, якобы содержавший метаданные версии, но на самом деле содержавший обфусцированный код, предназначенный для запуска вредоносного скрипта на компьютерах под управлением Windows.

В коде также была замечено язвительное упоминание аналитика угроз ReversingLabs Томислава Малича (Tomislav Maljic), который весной 2020 года выявил более 700 вредоносных библиотек RubyGems, предназначенных для майнинга биткоинов на зараженных машинах. Все обнаруженные тогда вредоносны были клонами различных легитимных библиотек. Они использовали технику typosquatting, то есть имели нарочито похожие на оригиналы имена, и даже работали, но также содержали дополнительные вредоносные файлы.

По словам исследователей Sonatype, пакет ruby-bitcoin и вовсе включает в себя только вредоносный код, (такой же, как в файле version.rb из pretty_color).

Интересно, что текстовый вариант вредоносного скрипта, использованного в этих атаках, был обнаружен экспертами на GitHub, под несвязанной учетной записью, причем так он называется wannacry.vbs, хотя никакой связи с малварью WannaCry здесь определенно нет.

«Подмена адресов биткоин-кошельков в буфере обмена кажется больше похожей на банальное озорство со стороны злоумышленника-любителя, чем на сложную вымогательскую операцию», — резюмируют аналитики Sonatype». ***(Мария Нефёдова. В репозитории RubyGems снова нашли малварь // Хакер (https://xakep.ru/2020/12/17/rubygems-cryptocurrency-stealer/). 17.12.2020).***

***

«Microsoft предупредила о появлении новой малвари Adrozek, которая заражает устройства пользователей и изменяет настройки их браузеров, чтобы размещать рекламу в результатах поиска.

По данным компании, вредоносная программа активна как минимум с мая текущего года и достигла своего пика в августе, когда ежедневно контролировала более 30 000 зараженных браузеров. Однако аналитики считают, что реальное количество зараженных пользователей намного выше, ведь в период с мая по сентябрь 2020 года эксперты фиксировали «сотни тысяч» обнаружений Adrozek по всему миру.

Судя по всему, больше всего пострадавших от новой угрозы находится в Европе, за которой следуют Южная и Юго-Восточная Азия.

В настоящее время малварь распространяется при помощи классических drive-by атак. То есть пользователей перенаправляются с легитимных сайтов на домены злоумышленников, где их обманом вынуждают установить вредоносное ПО, которое затем обеспечивает себе постоянное присутствие в системе, прописываясь в реестр.

Проникнув в систему, Adrozek будет искать локально установленные браузеры, включая Microsoft Edge, Google Chrome, Mozilla Firefox и Яндекс.Браузер. Если цель обнаружена, малварь пытается принудительно установить свое расширение, изменив папку AppData. Чтобы гарантировать, что защита браузера не сработает и не обнаружит несанкционированные модификации, Adrozek также изменяет некоторые DLL-файлы браузера, настройки и отключает защитные механизмы. Так, малварь вносит следующие изменения:

отключает обновления браузера;
отключает проверки целостности файлов;
отключает функции безопасного просмотра;
регистрирует и активирует расширение, добавленного на предыдущем шаге;
позволяет вредоносному расширению работать в режиме инкогнито;
позволяет запуск расширения без получения соответствующих прав;
скрывает расширение с панели инструментов;
изменяет домашнюю страницу браузера по умолчанию;
изменяет поисковую систему по умолчанию.

Все это делается ради того, чтобы Adrozek мог размещать рекламу на страницах результатов поиска. За счет этой рекламы операторы малвари получают доход, направляя трафик на рекламные сайты или реферальные программы.

Хуже того, в случае с Firefox вредонос также извлекает учетные данные из браузера и отправляет их на сервер злоумышленников.

Microsoft пишет, что операции Adrozek чрезвычайно сложны, особенно если говорит об инфраструктуре распространения. С мая 2020 года компания отслеживает 159 доменов, на которых размещались установщики Adrozek. На каждом из доменов размещалось в среднем 17 300 динамически сгенерированных URL-адресов, а на каждом URL-адресе размещалось более 15 300 динамически сгенерированных установщиков Adrozek.

«Хотя многие из доменов содержали десятки тысяч URL-адресов, некоторые имели более 100 000 уникальных URL-адресов, а на одном мы обнаружили почти 250 000 URL-адресов. Эта огромная инфраструктура отражает решимость злоумышленников поддерживать эту кампанию в рабочем состоянии. Некоторые из этих доменов работали всего один день, а другие были активны куда дольше (до

120 дней)», — пишут эксперты и добавляют, что в ближайшие месяцы масштаб операций Adrozek, скорее всего, еще возрастет». ***(Мария Нефёдова. Microsoft рассказала о малвари Adrozek, взломавшей более 30 000 браузеров // Хакер (https://xakep.ru/2020/12/11/adrozek/). 11.12.2020).***

***

«Исследователи безопасности из Menlo Labs сообщили о росте числа так называемых атак drive-by (загрузка без ведома пользователя) с использованием высокоактивной структуры, получившей название SocGholish за широкое использование инструментов и методов социальной инженерии.

Фреймворк SocGholish выдает себя за легитимные обновления браузера, Flash и Microsoft Teams, чтобы обманом заставить пользователей запускать вредоносные ZIP-файлы. Преступники распространяют вредоносные загрузки, используя iFrame для обслуживания взломанных web-сайтов через легитимный ресурс.

«Поскольку файл размещен в iFrame на легитимном сайте, пользователи ошибочно полагают, что файл исходит от легитимного источника, и им предлагается загрузить и запустить файл», — сообщили эксперты.

Механизмы атак drive-by, используемые SocGholish, не включают в себя эксплоиты браузера, но вместо этого он использует три основных метода. Первый заключается в использовании атак типа watering hole (заражение часто посещаемых сайтов) путем установки iFrame на сайты с относительно высоким расположением в рейтинге Alexa и дальнейшего перенаправления пользователей через общие службы облачного хостинга к вредоносному ZIP-файлу.

Второй метод заключается во взломе сайтов, размещенных в системах управления контентом, таких как WordPress, для встраивания iFrames, которые используют большие двоичные объекты JavaScript для запуска загрузки.

Третий метод SocGholish заключается в использовании sites.google.com и JavaScript с целью динамического создания элемента ссылки для загрузки, указывающего на ZIP-файл на легитимном Google Диске.

SocGholish используется для получения начального доступа к конечным точкам, в частности, для распространения банковского трояна Dridex и вымогателя WastedLocker». ***(Хакеры активно используют SocGholish для осуществления атак drive-by // SecurityLab.ru (https://www.securitylab.ru/news/514954.php). 18.12.2020).***

***

«Червеобразный ботнет, распространяющийся через GitHub и Pastebin и устанавливающий на скомпрометированных системах криптовалютные майнеры и бэкдоры, вернулся с новыми функциями и возможностями. Теперь вредонос атакует web-приложения, IP-камеры и маршрутизаторы.

Ранее в этом месяце специалисты из Juniper Threat Labs задокументировали криптомайнинговую кампанию Gitpaste-12, использовавшую GitHub для хостинга вредоносного кода. Вредоносное ПО содержит 12 известных модулей, выполняющихся с помощью команд, загружаемых по URL с Pastebin. Атаки

начались 15 октября и продолжались в течение 12 дней, пока репозиторий на GitHub и URL Pastebin не были заблокированы.

Согласно новому отчету Juniper Threat Labs, вторая волна атак началась 10 ноября. Киберпреступники стали использовать другой репозиторий GitHub, помимо прочего, содержащий криптомайнер для Linux («ls»), файл со списком паролей для брутфорс-атак («pass») и эксплоита для локального повышения привилегий для Linux x86_64.

Первоначальное заражение происходит через X10-unix, двоичный файл на языке программирования Go, который загружает с GitHub полезную нагрузку для следующего этапа атаки.

«Червь проводит широкую серию атак, нацеленных на web-приложения, IP-камер, маршрутизаторов и др., содержащих как минимум 31 известную уязвимость, семь из которых также использовались предыдущим образцом Gitpaste-12, а также пытающихся взломать открытые подключения Android Debug Bridge», - сообщил исследователь Juniper Threat Labs Эшер Лэнгтон (Asher Langton).

В число эксплуатируемых ботнетом уязвимостей входят: уязвимости удаленного кода в F5 BIG-IP Traffic Management User Interface (CVE-2020-5902), Pi-hole Web (CVE-2020-8816), Tenda AC15 AC1900 (CVE-2020-10987) и vBulletin (CVE-2020-17496), а также уязвимость SQL-инъекции в FUEL CMS (CVE-2020-17463).

Помимо установки X10-unix и ПО для майнинга Monero, вредонос также открывает бэкдор, прослушивая порты 30004 и 30006, загружает внешний IP-адрес жертвы в закрытую учетную запись Pastebin и пытается подключиться к соединениям Android Debug Bridge через порт 5555. При успешном подключении Gitpaste-12 переходит к загрузке файла APK Android («weixin.apk»), который в конечном итоге устанавливает версию X10-unix для процессора ARM.

По оценкам Juniper, в общей сложности было обнаружено не менее 100 различных хостов, распространяющих инфекцию». ***(Ботнет Gitpaste-12 вернулся с новым функционалом // SecurityLab.ru (https://www.securitylab.ru/news/514886.php). 16.12.2020).***

***

«Печально известный кейлоггер изменил свою тактику таргетинга и теперь собирает сохраненные учетные данные для менее популярных веб-браузеров и почтовых клиентов.

Шестилетняя вредоносная программа для клавиатурных шпионов под названием Agent Tesla была снова обновлена, на этот раз с расширенным таргетингом и улучшенными функциями кражи данных.

Агент Тесла впервые появился на сцене в 2014 году, специализируясь на кейлоггах (предназначенных для записи нажатий клавиш, сделанных пользователем с целью кражи данных, таких как учетные данные и т. Д.) И кражи данных. С тех пор кейлоггер только набрал обороты - в первой половине 2020 года он участвовал в большем количестве атак, чем, например, печально известные вредоносные программы TrickBot или Emotet.

Исследователи предупреждают, что новейшая итерация вредоносного ПО, обнародованная во вторник, вероятно, добавит к этому количеству атак, поскольку злоумышленники переходят на обновленную версию.

«Злоумышленники, которые переходят на эту версию Agent Tesla, получают возможность нацеливаться на более широкий спектр сохраненных учетных данных, в том числе для веб-браузера, электронной почты, VPN и других служб», - сказал Аарон Райли, аналитик по анализу киберугроз в Cofense анализ.

Тактика кражи данных

Новая версия Agent Tesla включает возможность нацеливания на более широкий диапазон сохраненных учетных данных, таких как менее популярный веб-браузер и почтовые клиенты.

«Это может указывать на повышенный интерес к украденным учетным данным для более специализированного сегмента рынка или определенного вида продукта или услуги», - сказал Райли.

Агент Тесла теперь включает возможность собирать учетные данные для веб-браузера Pale Moon, веб-браузера с открытым исходным кодом на основе Mozilla, доступного для Microsoft Windows и Linux; и почтовый клиент The Bat, почтовый клиент для операционной системы Microsoft Windows, разработанный Ritlabs, SRL.

Ранее было обнаружено, что вредоносная программа способна собирать данные конфигурации и учетные данные от ряда более распространенных VPN-клиентов, FTP-клиентов, почтовых клиентов и веб-браузеров. Это включало Apple Safari, BlackHawk, Brave, CentBrowser, Chromium, Comodo Dragon, CoreFTP, FileZilla, Google Chrome, Iridium, Microsoft IE и Edge, Microsoft Outlook, Mozilla Firefox, Mozilla Thunderbird, OpenVPN, Opera, Opera Mail, Qualcomm Eudora, Tencent. QQBrowser и Яндекс и другие.

Райли сообщила Threatpost, что теперь вредоносная программа также может использовать TOR с ключом для обхода фильтров контента и сетевой безопасности. Кроме того, обновление включает новые сетевые возможности, которые создают более надежный набор методов эксфильтрации, включая использование службы обмена сообщениями Telegram. Хотя возможность эксфильтрации через Telegram API «не нова», - сказала Райли Threatpost, - она «может указывать на растущую тенденцию использования вредоносных программ служб мгновенного обмена сообщениями для инфраструктуры [Command and Control] C2».

Таргетинг

Последняя версия Agent Tesla показала, что вредоносная программа поменяла таргетинг. Новая версия ориентирована в первую очередь на Индию. Хотя ранее это было основной целью Agent Tesla, исследователи говорят, что вредоносное ПО в меньшей степени ориентировано на другие регионы, такие как США и Европа.

Кроме того, Agent Tesla меньше ориентировался на ранее нацеленные на такие отрасли отрасли, как технологическая сфера, и активизировал свои атаки на поставщиков интернет-услуг (ISP).

«Интернет-провайдеры могут рассматриваться в качестве основной мишени для злоумышленников из-за других отраслевых вертикалей, которые полагаются на них при выполнении важных функций», - сказал Райли. «Скомпрометированный

интернет-провайдер может предоставить злоумышленникам доступ к организациям, у которых есть интеграция и права доступа к интернет-провайдеру. Подписчики также будут подвержены риску, поскольку интернет-провайдеры часто хранят электронные письма или другие важные личные данные, которые можно использовать для получения доступа к другим учетным записям и службам».

Будущее агента Тесла

Агент Тесла несколько раз появлялся в прошлом году в различных кампаниях. Например, в апреле 2020 года это было замечено в целевых кампаниях против нефтегазовой отрасли . В августе 2020 года исследователи обнаружили вредоносное ПО, использующее пандемию и добавляющее новые функции, чтобы помочь ему доминировать на сцене корпоративных угроз.

Исследователи предупреждают, что как только злоумышленники осознают преимущества новейшей версии вредоносного ПО, они могут быстрее перейти на него, поскольку могут потребоваться новые функции.

«Несмотря на опасные возможности обеих версий Agent Tesla, организации могут защитить себя, обучая своих сотрудников и поддерживая надлежащие меры по снижению рисков», - сказал Райли». ***(Lindsey O'Donnell. Agent Tesla Keylogger Gets Data Theft and Targeting Update // Threatpost (https://threatpost.com/agent-tesla-targeting-data-tactics/162268/). 15.12.2020).***

***

«Новое вредоносное ПО использует файлы Word с макросами для загрузки сценария PowerShell с GitHub.

Этот сценарий PowerShell дополнительно загружает законный файл изображения из службы хостинга изображений Imgur для декодирования сценария Cobalt Strike в системах Windows.

Несколько исследователей потенциально связали этот штамм с MuddyWater (он же SeedWorm и TEMP.Zagros), поддерживаемой правительством группой повышенной устойчивой угрозы (APT), впервые обнаруженной в 2017 году и направленной в основном на предприятия Ближнего Востока.

Макрос Word запускает скрипт PowerShell, размещенный на GitHub

На этой неделе исследователь Arkbird поделился подробностями о новом вредоносном ПО на основе макросов, которое является уклончивым и порождает полезную нагрузку в несколько этапов.

По словам исследователя, вредоносная программа, которая выглядит «как MuddyWater», поставляется как встроенный макрос в устаревшем файле Microsoft Word (* .doc) в стиле группы APT.

В тестах BleepingComputer при открытии документа Word запускается встроенный макрос. Далее макрос запускает powershell.exe и передает ему расположение сценария PowerShell, размещенного на GitHub (в архиве).

В однострочном скрипте PowerShell есть инструкции по загрузке реального файла PNG из службы хостинга изображений Imgur.

Хотя само это изображение может быть безобидным, его значения пикселей используются сценарием PowerShell при вычислении полезной нагрузки следующего этапа.

Метод сокрытия кода, секретных данных или вредоносной полезной нагрузки в обычных файлах, таких как изображения, известен как стеганография.

Такие инструменты, как Invoke-PSImage делают это возможным, сценарий PowerShell в пикселях файла PNG и генерируя однострочную команду для выполнения полезной нагрузки.

Как замечено BleepingComputer и показано ниже, алгоритм вычисления полезной нагрузки запускает цикл foreach для перебора набора значений пикселей в изображении PNG и выполняет определенные арифметические операции для получения функциональных команд ASCII.

Декодированный скрипт выполняет полезную нагрузку Cobalt Strike

Декодированный сценарий, полученный в результате изменения значений пикселей PNG, представляет собой сценарий Cobalt Strike.

Cobalt Strike - это законный набор инструментов для тестирования на проникновение, который позволяет злоумышленникам развертывать «маяки» на скомпрометированных устройствах, чтобы удаленно «создавать оболочки, выполнять сценарии PowerShell, выполнять эскалацию привилегий или запускать новый сеанс для создания прослушивателя в системе жертвы».

Фактически, декодированный шелл-код содержит строку EICAR, чтобы обмануть инструменты безопасности и группы SOC, чтобы они ошибочно приняли эту вредоносную нагрузку за антивирусный тест, выполняемый профессионалами в области безопасности.

Однако, по словам Arkbird, полезная нагрузка действительно связывается с сервером управления и контроля (C2) через модуль WinINet для получения дальнейших инструкций.

Домен, связанный с сервером C2 Mazzion1234-44451.portmap.host, больше не был доступен на момент написания.

Однако исследователь отметил, что «домен был зарегистрирован около 20 декабря 2020 года. В аккаунте GitHub скрипт перенесен на 24 декабря, дату отправки в [VirusTotal]».

Появление этой ускользающей разновидности вредоносного ПО в преддверии праздников дает противникам еще одно преимущество: маскировать свои шаги, когда большая часть сотрудников, вероятно, будет отсутствовать и менее бдительна.

Хотя авторитетная атрибуция является сложной задачей, учитывая возможность атак подражателя, исследователь безопасности Флориан Рот из Nextron Systems добавил индикаторы взлома (IOC), связанные с этим вредоносным ПО, в список MuddyWater IOC.

Исследователь также предоставил правила YARA, которые можно использовать для обнаружения варианта в вашей среде.

Ниже приведены IOC, связанные с загруженными макросами документами Word, используемыми в этой вредоносной кампании:

d1c7a7511bd09b53c651f8ccc43e9c36ba80265ba11164f88d6863f0832d8f81

ed93ce9f84dbea3c070b8e03b82b95eb0944c44c6444d967820a890e8218b866

Если вы получили подозрительный документ Word в фишинговом письме или любым другим способом, не открывайте его и не запускайте в нем «макросы».

Это не первый случай, когда законные сервисы, такие как GitHub и Imgur, используются для обслуживания вредоносного кода.

Недавно появился ботнет- червь Gitpaste-12. использовал как GitHub, так и Pastebin для размещения своей вредоносной нагрузки и уклонения от обнаружения.

Кроме того, известно, что группы программ-вымогателей, такие как CryLocker, злоупотребляют Imgur для хранения данных». ***(Ax Sharma. GitHub-hosted malware calculates Cobalt Strike payload from Imgur pic // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/github-hosted-malware-calculates-cobalt-strike-payload-from-imgur-pic/). 28.12.2020).***

***

«Специалисты компаний «Лаборатория Касперского» и «Яндекс» обнаружили масштабную потенциально вредоносную кампанию, в ходе которой злоумышленники внедряют вредоносный код в расширения для браузеров. Эксперты выявили более двадцати модифицированных расширений, в том числе популярные Frigate Light, Frigate CDN и SaveFrom.

С помощью внедренного в расширения вредоносного кода злоумышленники могут получать доступ к учетным записям пользователей в одной из популярных соцсетей (ее название специалисты не приводят), а также без их ведома накручивать просмотры видеороликов, в том числе рекламных, на различных площадках. В фоновом режиме расширения генерируют мошеннический трафик, проигрывая видео в скрытых вкладках, а также перехватывают токены для доступа к соцсети.

Как уточнили эксперты, мошенническая схема запускается только в случае активного использования браузера, а сам код оснащен механизмом защиты от обнаружения. Единственное, что могли заметить пользователи, - замедление работы устройства. По словам ведущего эксперта «Лаборатории Касперского» Сергея Голованова, число потенциальных жертв мошеннической схемы превышает миллион.

Компания «Яндекс» выявила скрытый поток трафика и отключила расширения в Яндекс.Браузере. Продукты «Лаборатории Касперского» также блокирует такую активность. Результаты совместного расследования обеих компаний уже переданы разработчикам социальной сети и наиболее популярных браузеров, чтобы помочь им предотвратить подобные атаки в будущем.

Как пояснил руководитель отдела интернет-безопасности и противодействия мошенничеству компании «Яндекс» Антон Митягин, генерируемый вредоносными расширениями трафик очень сложно обнаружить, так как он смешивается с реальными действиями пользователей. В данном случае, заметив подозрительный трафик, специалисты компании обратились за помощью к «Лаборатории Касперского». ***(Злоумышленники внедряют вредоносный код в расширения для браузеров // SecurityLab.ru (https://www.securitylab.ru/news/515085.php). 24.12.2020).***

***

«Как раз к рождественским праздникам Emotet отправляет подарок Trickbot.

После почти двухмесячного затишья ботнет Emotet вернулся с обновленной полезной нагрузкой и кампанией, которая достигает 100 000 целей в день.

Emotet начал свою жизнь как банковский троян в 2014 году и постоянно развивался, чтобы стать полнофункциональным механизмом доставки угроз. Он может устанавливать набор вредоносных программ на машины жертвы, включая кражи информации, сборщики электронной почты, механизмы самораспространения и программы-вымогатели. Последний раз он был опубликован в октябре, и его целью были добровольцы Национального комитета Демократической партии (DNC); а до этого он стал активным в июле после пятимесячного перерыва, сбросив троян Trickbot. До этого, в феврале, это было замечено в кампании по рассылке SMS-сообщений якобы из банков жертв.

«Ботнет Emotet - один из самых распространенных отправителей вредоносных писем, когда он активен, но он регулярно бездействует на недели или месяцы», - сказал Брэд Хаас, исследователь Cofense, во вторник в блоге. «В этом году один такой перерыв длился с февраля до середины июля, и это самый длительный перерыв, который Cofense видела за последние несколько лет. С тех пор они наблюдали регулярную активность Emotet до конца октября, но ничего с того момента до сегодняшнего дня».

По словам исследователей, ботнет также остается верным своей форме с точки зрения полезной нагрузки. «В октябре наиболее распространенными вторичными полезными нагрузками были TrickBot, Qakbot и ZLoader; сегодня мы наблюдали за TrickBot», - сказал Хаас.

Вредоносное ПО TrickBot - это хорошо известный и сложный троян, впервые разработанный в 2016 году как банковское вредоносное ПО. Подобно Emotet, он имеет историю трансформации и добавления новых функций, позволяющих избежать обнаружения или расширить свои возможности заражения. Пользователи, зараженные трояном TrickBot, увидят, что их устройство становится частью ботнета, который злоумышленники используют для загрузки вредоносного ПО второго уровня - исследователи назвали его «идеальным дроппером практически для любых дополнительных вредоносных программ».

Типичными последствиями заражения TrickBot являются захват банковских счетов, мошенничество с использованием крупных электронных средств и атаки программ-вымогателей. Совсем недавно в нем реализованы функции, предназначенные для проверки прошивки UEFI / BIOS целевых систем. Он серьезно возродился после того, как в октябре инфраструктура вредоносного ПО была удалена Microsoft и другими.

Несколько охранных фирм заметили последнюю кампанию, причем Proofpoint через Twitter отметил: «Мы видим более 100 тысяч сообщений на английском, немецком, испанском, итальянском и других языках. Приманки используют захват потоков с вложениями Word, защищенными pw почтовыми индексами и URL-адресами».

Перехват потоков - это трюк, который Emotet добавил осенью, отмеченный исследователями из Palo Alto Networks. Операторы будут вставлять себя в существующий разговор по электронной почте, отвечая на реальное письмо, отправленное от цели. У получателя нет оснований полагать, что письмо является вредоносным.

Шеррод ДеГриппо, старший директор по исследованию и обнаружению угроз в Proofpoint, сказал Threatpost, что кампания на этой неделе является довольно стандартным тарифом для Emotet.

«Наша команда все еще изучает новые образцы, и пока мы обнаружили лишь незначительные изменения. Например, двоичный файл Emotet теперь используется как DLL вместо .exe», - сказал ДеГриппо. «Мы обычно наблюдаем сотни тысяч электронных писем в день, когда работает Emotet. Эта кампания им на высоте. Поскольку эти кампании продолжаются, мы проводим подсчеты на постоянной основе. Объемы в этих кампаниях аналогичны объемам других кампаний в прошлом, обычно от 100 000 до 500 000 в день».

Она добавила, что самое интересное в кампании - это время.

«Обычно мы видим, что Emotet прекращает свою деятельность с 24 декабря до начала января», - отметила она. «Если они продолжат эту схему, эта недавняя деятельность будет для них невероятно короткой и необычной».

Между тем исследователи Malwarebytes отметили, что злоумышленники поочередно переключаются между различными фишинговыми приманками, чтобы заставить пользователей социальной инженерии активировать макросы, включая темы COVID-19. Исследователи также наблюдали, как банда Emotet загружает свои полезные данные с поддельным сообщением об ошибке.

Команда Хааса Кофенс наблюдала за той же деятельностью, отметив, что это знаменует эволюцию банды Emotet.

«Новый Emotet maldoc включает в себя заметное изменение, которое, вероятно, предназначено для того, чтобы жертвы не заметили, что они только что были заражены», - сказал он. «Документ по-прежнему содержит вредоносный код макроса для установки Emotet и по-прежнему утверждает, что является «защищенным» документом, требующим от пользователей включения макросов, чтобы его открыть. Старая версия не давала видимого ответа после включения макросов, что могло вызвать подозрения у жертвы. В новой версии создается диалоговое окно, в котором говорится, что «Word обнаружил ошибку при попытке открыть файл». Это дает пользователю объяснение, почему он не видит ожидаемого контента, и повышает вероятность того, что он проигнорирует весь инцидент, пока Emotet работает в фоновом режиме».

ДеГриппо сказал Threatpost, что первоначальный взгляд на электронные письма показывает, что некоторые из перехваченных потоков просят получателей открыть вложение .zip и предоставить пароль для доступа.

По словам исследователей, за возрождением вредоносного ПО, несмотря на отсутствие каких-либо существенных изменений по сравнению с предыдущими действиями, администраторы должны наблюдать.

«Больше всего Emotet опасаются за его союзы с другими преступниками, особенно с теми, кто занимается программами-вымогателями. Триада Emotet -

TrickBot - Ryuk посеяла хаос под Рождество в 2018 году», - сообщает Malwarebytes. «Хотя некоторые злоумышленники соблюдают праздники, это также прекрасная возможность для запуска новых атак, когда у многих компаний ограниченный персонал. Этот год стал еще более важным в свете пандемии и недавней катастрофы SolarWinds. Мы призываем организации быть особенно бдительными и продолжать предпринимать шаги по защите своих сетей, особенно в отношении политик безопасности и контроля доступа». ***(Tara Seals. Emotet Returns to Hit 100K Mailboxes Per Day // Threatpost (https://threatpost.com/emotet-returns-100k-mailboxes/162584/). 23.12.2020).***

***

Програми-вимагачі

«Поставщик облачного хостинга и ИТ-услуг Netgain был вынужден отключить некоторые из своих центров обработки данных после атаки вымогателя в конце ноября.

Netgain предлагает хостинг и облачные ИТ-решения, включая управляемые ИТ-услуги и среды «настольный компьютер как услуга», компаниям, работающим в сфере здравоохранения и бухгалтерского учета.

В серии писем, отправленных клиентам и просмотренной BleepingComputer, Netgain заявляет, что они стали жертвами атаки вымогателя 24 ноября 2020 года.

4 декабря клиенты начали получать электронные письма от Netgain, в которых говорилось, что они могут испытывать «сбои в работе или замедление работы системы» из-за кибератаки на хостинг-провайдера.

«В настоящее время наш план реагирования на инциденты и меры по сдерживанию требуют от нас принятия дополнительных мер предосторожности, а также установки дополнительного программного обеспечения безопасности в ответ на эту кибератаку. Мы ожидаем, что вы столкнетесь с перебоями в работе или замедлением работы системы сегодня и в ближайшие дни как мы предпримем эти действия ", - поясняет клиентам электронное письмо от Netgain от 4 декабря.

На следующий день Netgain заявил, что они были вынуждены закрыть свои центры обработки данных, чтобы изолировать и сдержать атаку программ-вымогателей.

«Как вы знаете, в ответ на инцидент кибербезопасности мы приняли защитные меры для изоляции и сдерживания угрозы, в том числе отключили ряд наших центров обработки данных. Знайте, что мы понимаем влияние этого сбоя на ваш бизнес и Команда работает круглосуточно, 24-7, чтобы сдержать эту угрозу и восстановить услуги», - говорится в электронном письме от 5 декабря.

Сегодня клиент Netgain по имени Crystal Practice Management, который предлагает программные решения для управления офисом для оптометристов и специалистов по терапии зрения, отправил своим клиентам по электронной почте информацию об атаке Netgain.

По данным Crystal PM, тысячи серверов Netgain пострадали от атаки вымогателя, и что Netgain работает круглосуточно, пытаясь вернуть свои серверы в

оперативный режим. К сожалению, до сих пор нет ETA, когда эти серверы вернутся в сеть.

BleepingComputer много раз связывался с Netgain, но не получил ответов на наши запросы об этой атаке.

Мы также не определили, какая операция вымогателя атаковала Netgain, и ни один злоумышленник не взял на себя ответственность». ***(Lawrence Abrams. Ransomware forces hosting provider Netgain to take down data centers // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ransomware-forces-hosting-provider-netgain-to-take-down-data-centers/). 08.12.2020).***

***

«Гигант электроники Foxconn подвергся атаке с использованием программ-вымогателей на мексиканском предприятии в выходные дни Дня благодарения, где злоумышленники украли незашифрованные файлы перед шифрованием устройств.

Foxconn - крупнейшая компания по производству электроники в мире с зарегистрированной выручкой в размере 172 млрд долларов в 2019 году и более 800000 сотрудников по всему миру. Дочерние компании Foxconn включают Sharp Corporation, Innolux, FIH Mobile и Belkin.

BleepingComputer отслеживает, по слухам, атаку вымогателя Foxconn, произошедшую в выходные дни Благодарения.

Сегодня программа-вымогатель DoppelPaymer опубликовала файлы, принадлежащие Foxconn NA, на своем сайте утечки данных программ-вымогателей. Утечка данных включает общие бизнес-документы и отчеты, но не содержит никакой финансовой информации или личных данных сотрудников.

Источники в индустрии кибербезопасности подтвердили, что Foxconn подверглась атаке около 29 ноября 2020 года на их завод Foxconn CTBG MX, расположенный в Сьюдад-Хуарес, Мексика.

Этот объект открылся в 2005 году и используется Foxconn для сборки и доставки электронного оборудования во все регионы Южной и Северной Америки.

«Наше здание площадью 682 000 квадратных футов было построено еще в 2005 году и расположено в Сьюдад-Хуаресе, штат Чиуауа, Мексика, на границе с Эль-Пасо, штат Техас. [..] Foxconn CTBG MX стратегически расположен для поддержки всего американского региона», веб-страница Foxconn CTBG MX описывает объект.

После атаки веб-сайт учреждения не работал и в настоящее время показывает посетителям ошибку…

В записку о выкупе включена ссылка на страницу жертвы Foxconn на сайте оплаты Tor DoppelPaymer, где злоумышленники требуют выкуп в размере 1804,0955 BTC, или примерно 34 686 000 долларов по сегодняшним ценам на биткойны.

В интервью DoppelPaymer банда вымогателей подтвердила, что они атаковали предприятие Foxconn в Северной Америке 29 ноября, но не атаковали всю компанию.

В рамках этой атаки злоумышленники утверждают, что зашифровали около 1200 серверов, украли 100 ГБ незашифрованных файлов и удалили 20–30 ТБ резервных копий.

«Мы зашифровали сегмент NA, а не весь foxconn, это примерно 1200-1400 серверов, и мы не были ориентированы на рабочие станции. У них также было около 75 ТБ разных резервных копий, которые мы смогли - мы уничтожили (примерно 20-30 ТБ)», - рассказали в DoppelPayment. нас о нападении.

В заявлении для BleepingComputer Foxconn подтвердила атаку и сообщила, что постепенно возвращают свои системы в эксплуатацию.

«Мы можем подтвердить, что информационная система в США, которая поддерживает некоторые из наших операций в Северной и Южной Америке, была объектом кибербезопасной атаки 29 ноября. Мы работаем с техническими экспертами и правоохранительными органами над проведением расследования для определения полной последствия этого незаконного действия, а также установить виновных и привлечь их к ответственности».

«Система, пострадавшая в результате этого инцидента, тщательно проверяется и поэтапно вводится в эксплуатацию», - сказал Foxconn BleepingComputer.

Другие жертвы, на которые в прошлом нападал DoppelPaymer, включают Compal, PEMEX (Petróleos Mexicanos), город Торранс в Калифорнии, Университет Ньюкасла, округ Холл в Джорджии, Banijay Group SAS и Bretagne Télécom». ***(Lawrence Abrams. Foxconn electronics giant hit by ransomware, $34 million ransom // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/foxconn-electronics-giant-hit-by-ransomware-34-million-ransom/). 07.12.2020).***

***

«Программа-вымогатель Clop утверждает, что украла 2 миллиона кредитных карт у E-Land Retail за год, закончившийся атакой программы-вымогателя в прошлом месяце.

E-Land Retail, дочерняя компания E-Land Global, управляет многочисленными розничными магазинами одежды, включая New Core и NC Department Store.

В прошлом месяце E-Land Retail пришлось закрыть 23 универмага NC и New Core после атаки вымогателя CLOP.

Во время атаки E-Land Retail заявила, что конфиденциальные данные клиентов находятся в безопасности, поскольку они были зашифрованы на другом сервере.

«Хотя эта атака программы-вымогателя нанесла некоторый ущерб сети и системе компании, информация о клиентах и конфиденциальные данные зашифрованы на отдельном сервере».

«Он находится в безопасном состоянии, потому что им управляют», - сообщил генеральный директор E-Land Retail Чан-Хён Сок в уведомлении на их веб-сайте.

Однако в интервью BleepingComputer операторы программ-вымогателей CLOP заявили, что они взломали E-Land более года назад и незаметно воруют кредитные карты с помощью вредоносного ПО для POS, установленного в сети.

«Больше года назад взломали их сеть, все как обычно. Подумали, что делать, установили POS зловред и оставили на год. Перед блокировкой карты собирали и расшифровывали, целый год компания делала не подозревал и ничего не сделал», - сказала банда CLOP BleepingComputer.

Используя установленную вредоносную программу для POS-терминалов, CLOP сообщил BleepingComputer, что за последний год они украли данные Track 2 для 2 миллионов кредитных карт.

Вредоносное ПО для торговых точек используется для сканирования памяти POS-терминалов при совершении транзакций по кредитным картам. При обнаружении данных кредитной карты вредоносная программа копирует информацию о кредитной карте как данные дорожки 1 или дорожки 2 и передает ее обратно на сервер злоумышленника.

Похищенные кредитные карты, которые, по утверждению CLOP, были украдены, представлены в виде данных дорожки 2, которые включают номер кредитной карты, дату истечения срока действия и другую информацию. Однако он не содержит CVV-кода кредитной карты, поэтому злоумышленники могут использовать его только для создания поддельных кредитных карт для покупок в магазине.

CLOP также сообщил BleepingComputer, что они нацелены примерно на 90 тысяч IP-адресов, но не уверены, сколько на самом деле было зашифровано.

BleepingComputer неоднократно пыталась связаться с E-Land Global и E-Land Retail, но не получила ответа на наши электронные письма». **(Lawrence Abrams. Ransomware gang says they stole 2 million credit cards from E-Land // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ransomware-gang-says-they-stole-2-million-credit-cards-from-e-land/). 03.12.2020).**

***

«Как стало известно BleepingComputer, универмаг Kmart в США подвергся атаке с использованием программ-вымогателей, которые повлияли на внутренние службы компании.

Sears Holding Corp изначально владела и Kmart, и Sears, но после того, как компания объявила о банкротстве в 2018 году, в 2019 году она была куплена Transform Holdco LLC (Transformco).

Хотя Kmart был нарицательным в США, его количество за последние два года сократилось до 35 магазинов.

Домен Kmart для Windows поражен программой-вымогателем

BleepingComputer узнал, что на этой неделе Kmart подвергся кибератаке со стороны программы-вымогателя Egregor, которая зашифровала устройства и серверы в сети.

Записка с требованием выкупа, предоставленная BleepingComputer, показывает, что домен Windows KMART был взломан в результате атаки.

В то время как интернет-магазины продолжают работать, сайт отдела кадров Transformco, 88sears.com, в настоящее время не работает. По словам сотрудников, причиной сбоя стала недавняя атака программы-вымогателя.

Egregor известен тем, что крадет незашифрованные файлы перед развертыванием своих программ-вымогателей. Затем операция вымогателя угрожает опубликовать данные на сайтах утечки данных вымогателей, если выкуп не будет уплачен.

Неизвестно, украли ли злоумышленники данные, сколько устройств было зашифровано, или сумма выкупа, которую потребовала киберпреступная группа Egregor.

Egregor - это новая программа-вымогатель, начавшая шифрование жертв в сентябре 2020 года. Злоумышленники сообщили BleepingComputer, что после завершения операции Maze Ransomware многие из их партнеров переключились на операцию Egregor.

Эта миграция опытных злоумышленников позволила Эгрегору быстро собрать множество жертв за короткий период времени.

Другие известные компании, недавно подвергшиеся атаке Эгрегора, включают Cencosud, Crytek, Ubisoft и Barnes and Noble.

BleepingComputer обратилась к Kmart и их материнской компании Transformco, но пока не получила ответа». ***(Lawrence Abrams. Kmart nationwide retailer suffers a ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/kmart-nationwide-retailer-suffers-a-ransomwa re-attack/). 03.12.2020).***

***

«Операция вымогателя Egregor взломала транспортное агентство TransLink метро Ванкувера с помощью кибератаки, вызвавшей сбои в работе служб и платежных систем.

1 декабря TransLink объявил, что у них возникли проблемы с их системами информационных технологий, которые затронули телефоны, онлайн-сервисы и возможность оплачивать проезд с помощью кредитной или дебетовой карты. Проблемы с информационными технологиями не повлияли на все транспортные услуги.

После восстановления платежных систем TransLink опубликовал заявление о том, что ИТ-проблемы были вызваны атакой программы-вымогателя.

«Теперь мы можем подтвердить, что TransLink стал целью атаки программ-вымогателей на некоторые объекты нашей ИТ-инфраструктуры. Эта атака включает в себя обмен данными с TransLink посредством распечатанного сообщения», - говорится в заявлении TransLink.

За атакой TransLink стояла программа-вымогатель Egregor

Репортер Global BC Джордан Армстронг написал в Твиттере фотографию записки о выкупе и заявил, что принтеры TransLink неоднократно печатали записки о выкупе…

По изображению записки с требованием выкупа BleepingComputer может подтвердить, что за атакой стояла операция вымогателя Egregor.

Egregor - также единственный известный вымогатель, который запускает скрипты, которые распечатывают записки о выкупе бомбы на доступных принтерах, как описано Армстронгом в своем твите. Банда Эгрегора использовала ту же тактику во время недавней кибератаки Cencosud, когда принтеры чеков начали неоднократно печатать записки о выкупе, чтобы привлечь внимание общественности к атаке.

Egregor - это новая организованная операция по борьбе с киберпреступностью, которая в партнерстве с филиалами взламывает сети и развертывает свои программы-вымогатели. В рамках этой договоренности аффилированные лица зарабатывают 70% генерируемых ими выкупов, а операторы Egregor получают 30% -ную долю дохода.

Известно, что аффилированные лица, которые взламывают сеть, крадут незашифрованные файлы перед шифрованием устройств с помощью программы-вымогателя Egregor. Затем хакеры используют эти украденные файлы в качестве дополнительного рычага, сообщая жертвам, что они будут публично освобождены, если не будет уплачен выкуп.

Эта банда вымогателей начала свою деятельность в сентябре 2020 года после того, как другая группа вымогателей, известная как Maze, прекратила свою деятельность. Злоумышленники сообщили BleepingComputer, что многие из аффилированных лиц, которые работали с Maze, перешли в Egregor, что позволило новой операции быстро собрать множество жертв.

Эти атаки охватывают множество известных компаний по всему миру, включая Kmart, Cencosud, Crytek, Ubisoft и Barnes and Noble». ***(Lawrence Abrams. Metro Vancouver's transit system hit by Egregor ransomware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/metro-vancouvers-transit-system-hit-by-egregor-ransomware/). 04.12.2020).***

***

«Кадровое агентство Randstad NV объявило сегодня, что их сеть была взломана вымогателем Egregor, который во время атаки украл незашифрованные файлы.

Randstad - крупнейшее в мире кадровое агентство с офисами на 38 рынках и владелец известного сайта по трудоустройству Monster.com. В Randstad работает более 38000 человек, а выручка в 2019 году составила 23,7 миллиарда евро.

На этой неделе операция по вымогательству Egregor опубликовала, как они утверждают, 1% данных Randstad, украденных во время недавней кибератаки. Эти утекшие данные представляют собой архив размером 32,7 МБ, содержащий 184 файла, включая бухгалтерские таблицы, финансовые отчеты, юридические документы и другие различные деловые документы.

После того, как злоумышленники опубликовали свои данные, Randstad выпустил уведомление системы безопасности, подтверждающее, что на них напала программа-вымогатель Egregor.

Randstad заявляет, что пострадали только ограниченное количество серверов и что их сети и бизнес-операции продолжали работать без сбоев.

Компания подтвердила, что данные были украдены, но все еще расследует, был ли доступ к личным данным клиентов сотрудников. В настоящее время они считают, что были украдены только данные, касающиеся их операций в США, Польше, Италии и Франции.

«На сегодняшний день наше расследование показало, что группа Egregor получила несанкционированный и незаконный доступ к нашей глобальной ИТ-среде и к определенным данным, в частности, связанным с нашими операциями в США, Польше, Италии и Франции», - сообщил Рандстад. «Теперь они опубликовали то, что, как утверждается, является подмножеством этих данных. Расследование продолжается, чтобы определить, к каким данным был получен доступ, включая личные данные, чтобы мы могли принять соответствующие меры в отношении идентификации и уведомления соответствующих сторон»,

Операция по вымогательству Egregor была чрезвычайно активной на прошлой неделе, когда были успешны атаки на транспортную систему метро Ванкувера TransLink и большой универмаг Kmart.

Egregor - это новая организованная операция по предоставлению программ-вымогателей для киберпреступлений, которая сотрудничает с аффилированными лицами с целью взлома сетей и развертывания их программ-вымогателей. В рамках этой договоренности филиалы зарабатывают 70% любых вносимых ими выкупов, а операторы Egregor получают 30% -ную долю дохода.

Банда программ-вымогателей начала действовать в середине сентября 2020 года после того, как известная группа программ-вымогателей, известная как Maze, прекратила свою деятельность. Злоумышленники сообщили BleepingComputer, что многие из филиалов, которые работали с Maze, перешли на Egregor, что позволило новой операции быстро наращивать свои атаки.

Другие громкие атаки Эгрегора включают Cencosud, Crytek, Ubisoft и Barnes and Noble». ***(Lawrence Abrams. Largest global staffing agency Randstad hit by Egregor ransomware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/largest-global-staffing-agency-randstad-hit-by-egregor-ransomware/). 04.12.2020).***

***

«Операторы программ-вымогателей атаковали район школ города Хантсвилл в Алабаме, вынудив их закрыть школы на оставшуюся часть недели и, возможно, на следующей неделе.

Округ школ города Хантсвилла является шестым по величине школьным округом в Алабаме с почти 24 000 учащихся, 2 300 служащими и 37 школами. Из-за пандемии COVID-19 школьный округ предлагал как обучение в школе, так и полностью онлайн-обучение.

30 ноября, когда ученики вернулись с перерывов на День Благодарения, школьный округ произвел досрочное увольнение учеников после кибератаки, нарушившей их ИТ-системы.

Чтобы предотвратить распространение программы-вымогателя на устройства, предоставленные студентам и преподавателям, округ потребовал,

чтобы все выданные округом устройства были выключены и оставались выключенными, пока не будет сказано иное.

«Учащиеся, семьи, преподаватели и сотрудники должны отключить свои устройства, выданные округом, и убедиться, что устройства остаются выключенными до дальнейшего уведомления. Кроме того, заинтересованным сторонам следует избегать входа на любые платформы HCS как в школе, так и дома», - говорится в заявлении школьного округа Хантсвилла. сообщение родителям.

Вскоре после этого школьный округ Хантсвилла признал, что это была атака с использованием программ-вымогателей, и что они были вынуждены закрыть школы на оставшуюся часть недели и, возможно, на следующую неделю, когда они выздоравливают.

Семьи были предупреждены о том, что они должны с подозрением относиться к любым электронным письмам от школьного округа Хантсвилла с просьбой предоставить информацию об учениках, поскольку это могут быть фишинговые атаки со стороны злоумышленников…

Поскольку банды программ-вымогателей обычно крадут незашифрованные данные перед шифрованием устройств, некоторые родители выразили обеспокоенность по поводу того, была ли скомпрометирована информация об учениках…

На данный момент неизвестно, какая операция вымогателя стала причиной атаки…». ***(Lawrence Abrams. Alabama school district shut down by ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/alabama-school-district-shut-down-by-ransomware-attack/). 01.12.2020).***

***

«Злоумышленники, стоящие за атакой, взломали как минимум 85 000 серверов MySQL и в настоящее время продают как минимум 250 000 взломанных баз данных.

Исследователи предупреждают об активной кампании вымогателей, нацеленной на серверы баз данных MySQL. Программа-вымогатель PLEASE_READ_ME на сегодняшний день взломала не менее 85 000 серверов по всему миру и разместила не менее 250 000 украденных баз данных на сайте для продажи.

MySQL - это система управления реляционными базами данных с открытым исходным кодом. Атака использует слабые учетные данные на серверах MySQL с выходом в Интернет, которых во всем мире около 5 миллионов. С момента первого наблюдения за кампанией вымогателей в январе исследователи заявили, что злоумышленники изменили свои методы, чтобы усилить давление на жертв и автоматизировать процесс оплаты выкупа.

«Атака начинается с подбора пароля к службе MySQL. В случае успеха злоумышленник выполняет последовательность запросов к базе данных, собирая данные о существующих таблицах и пользователях», - сказали Офир Харпаз и Омри Маром, исследователи из Guardicore Labs, в сообщении в четверг. «К концу

выполнения данные жертвы исчезают - они архивируются в заархивированном файле, который отправляется на серверы злоумышленников, а затем удаляется из базы данных».

Оттуда злоумышленник оставляет записку о выкупе в таблице с именем «WARNING», в которой требуется уплата выкупа в размере до 0,08 BTC. В записке с требованием выкупа жертвам (дословно) сообщается: «Ваши базы данных загружаются и сохраняются на наших серверах. Если мы не получим ваш платеж в течение следующих 9 дней, мы продадим вашу базу данных тому, кто предложит самую высокую цену, или воспользуемся им иным образом».

Исследователи считают, что злоумышленники, стоящие за этой кампанией, заработали не менее 25 000 долларов за первые 10 месяцев года.

Исследователи заявили, что PLEASE_READ_ME (так называемый, потому что это имя базы данных, которую злоумышленники создают на взломанном сервере) является примером нецелевой, временной атаки вымогателя, которая не проводит время в сети, кроме нацеливания на то, что требуется для фактической атаки. - это означает, что обычно нет бокового движения.

Ученые предупреждают, что атака может быть простой, но и опасной, поскольку она почти не содержит файлов. «В цепочке атаки нет бинарных полезных нагрузок, что делает атаку «безвредной», - сказали они. «Только простой скрипт, который ломается в базе данных, крадет информацию и оставляет сообщение».

Тем не менее, бэкдор-пользователь mysqlbackups '@'% 'добавляется в базу данных для сохранения, предоставляя злоумышленникам доступ к скомпрометированному серверу в будущем.

Эволюция атаки

Исследователи впервые наблюдали атаки PLEASE_READ_ME в январе, в том, что они назвали «первой фазой» атаки. На этом первом этапе от жертв требовалось перевести BTC непосредственно в кошелек злоумышленника.

Вторая фаза кампании вымогателей началась в октябре, что, по словам исследователей, ознаменовало собой эволюцию методов, тактики и процедур (ДТС) кампании. На втором этапе, по словам исследователей, атака переросла в попытку двойного вымогательства, то есть злоумышленники публикуют данные, вынуждая жертв заплатить выкуп. Здесь злоумышленники размещают в сети TOR сайт, на котором можно совершать платежи. По словам исследователей, жертв, платящих выкуп, можно идентифицировать с помощью токенов (в отличие от их IP / домена).

«Веб-сайт является хорошим примером механизма двойного вымогательства - он содержит все просочившиеся базы данных, за которые не был уплачен выкуп», - заявили исследователи. «На веб-сайте перечислены 250 000 различных баз данных с 83 000 серверов MySQL с 7 ТБ украденных данных. На данный момент [мы] зафиксировали 29 инцидентов этого варианта, происходящих с семи разных IP-адресов».

Нападение вымогателей продолжилось на больницы, школы и другие организации в 2020 году. Использование тактики «двойного вымогательства» впервые появилось в конце 2019 года на операторах Maze - но быстро прижились в

течение последних нескольких месяцев различных злоумышленниками позади клоп, DoppelPaymer и семейства вымогателей Sodinokibi.

Заглядывая вперед, исследователи предупреждают, что операторы PLEASE_READ_ME пытаются улучшить свою игру, используя масштабное двойное вымогательство: «Факторинг их операций сделает кампанию более масштабируемой и прибыльной», - сказали они». ***(Lindsey O'Donnell. PLEASE_READ_ME Ransomware Attacks 85K MySQL Servers // Threatpost (https://threatpost.com/please_read_me-ransomware-mysql-servers/162136/). 10.12.2020).***

***

«Группа опубликовала файлы, украденные у бразильского производителя самолетов в результате атаки вымогателя в прошлом месяце.

Хакеры сбросили конфиденциальные данные компании, которые были украдены во время атаки вымогателей в прошлом месяце на производителя самолетов Embraer. Согласно опубликованному отчету, скомпрометированные данные появились на новом темном веб-сайте, созданном для публикации просочившейся информации.

Этот шаг, по-видимому, является местью за отказ бразильской компании заплатить выкуп за атаку, которая вместо этого решила восстановить пораженные системы из резервной копии, согласно отчету ZDNet, опубликованному в начале понедельника. Согласно отчету, файлы были опубликованы на недавно созданном темном веб-сайте, управляемом бандой вымогателей RansomExx, также известной как Defray 777.

Embraer - третий по величине производитель авиалайнеров после Boeing и Airbus. Компания признала в заявлении от 30 ноября, что 25 ноября произошла кибератака, в ходе которой была получена доступ к «только одной среде файлов компании».

«В результате этого происшествия Компания немедленно приступила к процедурам расследования и разрешения происшествия, а также приступила к активной изоляции некоторых из своих систем для защиты системной среды, что оказало временное воздействие на некоторые из своих операций» - говорится в сообщении.

Embraer не уточнил, какой атаке подверглась компания и были ли данные украдены из среды доступа. Согласно отчету, сотни мегабайт файлов данных, найденных на сайте RansomExx, включают папки, относящиеся к данным сотрудников, субподрядам цепочки поставок и исходному коду, 3D-моделям и фотографиям самолетов Embraer.

Embraer - не единственная компания, у которой утечка данных появилась на сайте утечки, который, как сообщается, был запущен в субботу на выходных. …на сайте также появились данные, украденные у других компаний, ставших жертвами группы вымогателей.

В последнее время банды программ-вымогателей проявляют особую активность в многочисленных громких атаках на крупные компании. RansomExx / Defray - одна из небольших групп, действующих в настоящее время, хотя,

возможно, запуск сайта утечки свидетельствует о том, что в ближайшие месяцы они увеличат свою активность.

Другие группы вымогателей, которые также управляют утечки сайтов для данных, украденных в вымогателей атак включают Conti, цок, Эгрегор и Revil, среди других. Некоторые из этих групп за последние несколько месяцев провели ряд серьезных атак, некоторые из которых привели к утечке данных на их сайты.

На прошлой неделе Egregor ударил по метрополитену Ванкувера Translink и американскому ритейлеру Kmart с помощью программ-вымогателей. До этого в октябре группа также провела крупные атаки на продавца книг Barnes & Noble и игровые компании Ubisof и Crytek .

Клоп и Конти также несут ответственность за нападения в последние месяцы. На прошлой неделе Клоп скакал с 2 миллионами кредитных карт после атаки на южнокорейскую розничную группу E-Land. Тем временем Conti в ноябре скрылся с данными производителя чипов Advantech, опубликовав список файлов на своем сайте утечки, чтобы попытаться оказать давление на компанию, чтобы она заплатила огромный выкуп в размере 750 биткойнов, или около 14 миллионов долларов». ***(Elizabeth Montalbano. RansomExx Ransomware Gang Dumps Stolen Embraer Data: Report // Threatpost (https://threatpost.com/ransomexx-ransomware-gang-dumps-stolen-embraer-data-report/161918/). 07.12.2020).***

***

«Программы-вымогатели, требующие от жертв миллионы долларов и обновляемые новыми функциями, могут стать еще одной серьезной угрозой для бизнеса.

Программа-вымогатель MountLocker впервые появилась в июле и шифрует сети жертв, когда злоумышленники требуют биткойны в обмен на ключ дешифрования. Как и другие формы программ-вымогателей, хакеры-преступники, стоящие за ним, угрожают утечкой украденной информации из организации-жертвы, если выкуп в биткойнах не будет выплачен.

Исследователи кибербезопасности в BlackBerry анализируют MountLocker и говорят, что те, кто стоит за ним, «явно только разогреваются» - и это семейство программ-вымогателей может стать серьезной угрозой в будущем.

Исследователи отмечают, что MountLocker использует партнерскую схему для поиска жертв, вероятно, ведет переговоры с хакерами, которые уже скомпрометировали сеть с помощью вредоносных программ, чтобы сделать развертывание вымогателей как можно более простым и широко распространенным - и предоставляет средства для обе стороны незаконно зарабатывают деньги на компрометации сети.

«Филиалы часто представляют собой отдельные организованные преступные группы, которые ищут легкий - и не такой простой - доступ в сети», - сказал ZDNet Том Боннер, известный исследователь угроз в Blackberry.

«Как только они установят точку опоры, они начнут переговоры с операторами программ-вымогателей, обычно через темные веб-каналы, чтобы получить программу-вымогатель для монетизации доступа к среде жертвы», - добавил он.

Хотя хакеры могут взломать сеть с помощью вредоносных программ, обычно посторонние получают доступ к сети, взламывая слабые, часто используемые пароли или пароли по умолчанию, а затем повышают свои привилегии оттуда.

В этом случае команда MountLocker распространилась по сети с помощью общедоступных инструментов, развертывающих программы-вымогатели по сети всего за 24 часа. После запуска команды на выполнение программы-вымогателя жертвы оказываются заблокированными от своей сети и сталкиваются с семизначным требованием выкупа.

Анализ кампаний показал, что в прошлом месяце появилась обновленная версия MountLocker, призванная сделать его еще более эффективным при шифровании файлов, а также обновленную возможность уклоняться от обнаружения программным обеспечением безопасности.

Хотя MountLocker, похоже, все еще находится на относительно ранней стадии разработки, он уже доказал свою эффективность, требуя жертв по всему миру, и, вероятно, станет более плодовитым по мере развития.

«С момента своего создания группа MountLocker была замечена как для расширения, так и для улучшения своих услуг и вредоносного ПО. Хотя их текущие возможности не особенно развиты, мы ожидаем, что эта группа продолжит развиваться и набирать популярность в краткосрочной перспективе», - говорится в исследовании. бумага.

Как и все формы программ-вымогателей, MountLocker использует общие уязвимости системы безопасности для своего распространения, поэтому один из лучших способов защиты от них - это гарантия того, что пароли по умолчанию не используются, применяется двухфакторная аутентификация и сети обновлены последними патчами безопасности для защиты от известных уязвимостей…». ***(Danny Palmer. This new ransomware is growing in strength and could become a major threat, warn researchers // ZDNet (https://www.zdnet.com/article/this-new-ransomware-is-growing-in-strength-and-could-become-a-major-threat-warn-researchers/). 1.12.2020).***

***

«Группа вымогателей Pay2Key в воскресенье опубликовала подробности о внутренних файлах, полученных от Habana Labs, израильского стартапа по производству микросхем, приобретенного год назад Intel.

Хакерская группа, связанная с иранцами через охранную фирму Check Point, опубликовала снимок экрана с исходным кодом, переданным Habana Labs через Twitter, вместе со ссылкой на адрес .onion, доступный в браузере Tor. Веб-сайт содержит имена файлов, связанных с программным обеспечением для совместной работы кода Gerrit от Habana Labs, данными DomainController и документами, которые, по всей видимости, были получены от производителя микросхем AI.

Пока писалась эта история, аккаунт @ pay2key был заблокирован за нарушение правил Twitter.

В файле ReadMe, размещенном на веб-сайте .onion, говорится, что у Intel и Habana Labs есть семьдесят два часа, чтобы остановить дальнейшие утечки, которые, по мнению неустановленного автора, могут включать информацию Active

Directory и соответствующие пароли, а также весь сервер Gerrit компании, который, как утверждается, состоит данных на 53 ГБ.

В декабре 2019 года Intel приобрела Habana Labs, производителя микросхем-ускорителей глубокого обучения для центров обработки данных, за 2 миллиарда долларов. Производитель микросхем из Санта-Клары отказался комментировать этот вопрос.

Check Point в прошлом месяце сообщила, что вымогателя Pay2Key ранее не было. В нем говорится, что имя было зарегистрировано в службе криптографической идентификации KeyBase.io в июне, а программа-вымогатель начала появляться в октябре.

По сообщениям Check Point, с тех пор программное обеспечение для похищения данных было использовано как минимум против трех израильских компаний и как минимум против одной европейской компании, согласно Swascan.

Программа-вымогатель обычно включает в себя доступ к серверу без авторизации, шифрование найденных файлов и последующее требование выкупа за ключ дешифрования. Оплата не гарантирует расшифровки файлов или какой-либо гарантии, что эти файлы не были скопированы и не были доступны где-либо еще.

Check Point заявляет, что группа Pay2Key осуществляет «двойное вымогательство», угрожая расшифровать файлы и опубликовать их, чтобы заставить жертв заплатить. На сегодняшний день запрошенные выплаты выкупа обычно составляли от 7 до 9 биткойнов, что в настоящее время составляет от 135 до 173 тысяч долларов.

Причина, по которой Check Point считает, что группа Pay2Key состоит из иранцев, заключается в том, что прошлые выплаты выкупа проходили через Excoino, иранский обмен криптовалюты, доступный для лиц с действующим иранским номером телефона и иранским идентификационным номером / кодом Melli. ®» ***(Thomas Claburn. Ransomware masterminds claim to have nabbed 53GB of data from Intel's Habana Labs // The Register (https://www.theregister.com/2020/12/14/habana_labs_ransomware/). 14.12.2020).***

***

«Разработчик вкусов и ароматов Symrise пострадал от атаки вымогателя Clop, в ходе которой злоумышленники якобы украли 500 ГБ незашифрованных файлов и зашифровали почти 1000 устройств.

Symrise - крупный разработчик веществ, придающих вкус и аромат, используемых в более чем 30 000 продуктов по всему миру, в том числе от Nestle, Coca-Cola и Unilever. Выручка Symrise в 2019 году составила 3,4 миллиарда евро, в компании работает более 10 000 человек.

На прошлой неделе немецкие СМИ сообщили, что компания Symrise подверглась кибератаке, которая вынудила их отключить свои системы, чтобы предотвратить распространение атаки.

«Чтобы оценить последствия и предотвратить возможные последствия, компания остановила все основные системы», - сказал Симриз Handelsblatt.

Symrise также заявил, что они временно остановили производство и закрыли объекты для дальнейшего расследования масштабов атаки.

Атакован бандой вымогателей Clop

Банда вымогателей Clop взяла на себя ответственность за атаку на Symrise и сообщила BleepingComputer, что они якобы зашифровали 1000 устройств.

Клоп сообщил BleepingComputer, что они взломали сеть Symrise, используя вредоносное ПО, распространяемое через фишинговые электронные письма. Как только они получили доступ к сети, Clop заявил, что они украли 500 ГБ незашифрованных файлов перед развертыванием своей программы-вымогателя.

В качестве доказательства этой кражи Clop разместил изображения якобы украденных файлов на своем сайте утечки данных. Просочившиеся изображения предназначены для паспортов, бухгалтерских документов, аудиторских отчетов, конфиденциальных косметических ингредиентов и электронных писем.

Программа-вымогатель Clop также стоит за атаками на Маастрихтский университет, Software AG IT, ExecuPharm, Indiabulls и E-Land, где они также утверждали, что украли 2 миллиона кредитных карт…». ***(Lawrence Abrams. Flavors designer Symrise halts production after Clop ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/flavors-designer-symrise-halts-production-after-clop-ransomware-attack/). 20.12.2020).***

***

«Злоумышленник распространяет поддельные установщики для Windows и Android для игры Cyberpunk 2077, которая устанавливает программу-вымогатель, называющую себя CoderWare.

Чтобы обманом заставить пользователей установить вредоносное ПО, злоумышленники обычно распространяют их в виде установщиков для геймеров, читов и взломов для программного обеспечения, защищенного авторским правом .

На этой неделе аналитик вредоносных программ Касперского Татьяна Шишкова обнаружила вымогатель для Android, маскирующийся под мобильную версию игры Cyberpunk 2077. Игра распространялась с поддельного веб-сайта, выдающего себя за законный магазин Google Play.

Шишкова написала в Твиттере, что программа-вымогатель CoderWare использует жестко запрограммированный ключ, что означает, что при необходимости можно создать дешифратор для бесплатного восстановления файлов.

«Алгоритм RC4 с жестко запрограммированным ключом (в этом примере - «219834534534354357389127389 21») используется для шифрования. Это означает, что если вы зашифровали файлы с помощью этого # вымогателя, их можно расшифровать, не заплатив выкуп».

Вы можете увидеть жестко запрограммированный ключ «219834534534354357389127389 21» в исходном коде программы-вымогателя…

Версия для Windows выпущена в ноябре

Эта программа-вымогатель аналогична той, что была обнаружена командой MalwareHunterTeam в ноябре и была замаскирована под установщик Windows Cyberpunk 2077. Как и версия для Android, эта программа-вымогатель называет себя CoderWare, но является разновидностью вымогателя BlackKingdom.

Вариант для Windows представлял собой скомпилированный на Python исполняемый файл, который шифрует файлы жертвы и добавляет расширение .DEMON к именам зашифрованных файлов.

Неизвестно, использует ли версия Windows жестко запрограммированный ключ в настоящее время.

Как видите, при попытке бесплатно установить защищенное авторским правом программное обеспечение вы сталкиваетесь с огромным риском заражения вредоносным ПО. Этот риск становится еще более значительным, когда вы пытаетесь установить приложения Android из сторонних магазинов приложений». ***(Lawrence Abrams. Ransomware masquerades as mobile version of Cyberpunk 2077 // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ransomware-masquerades-as-mobile-version-of-cyberpunk-2077/). 17.12.2020).***

***

«Поддерживаемая Ираном хакерская группа Fox Kitten была связана с операцией вымогателя Pay2Key, которая недавно начала нацеливаться на организации из Израиля и Бразилии.

«Мы оцениваем со средней или высокой степенью уверенности, что Pay2Key - это новая операция, проводимая Fox Kitten, иранской APT-группой, которая в ноябре-декабре 2020 года начала новую волну атак, в которых участвовали десятки израильских компаний», - сообщает компания ClearSky, занимающаяся разведкой угроз.

Согласно опубликованному сегодня отчету, «эта кампания является частью продолжающейся киберконфронтации между Израилем и Ираном, причем последняя волна атак нанесла значительный ущерб некоторым из пострадавших компаний».

Поддерживаемая Ираном хакерская группа Fox Kitten (также известная как Parisite компанией по кибербезопасности ICS Dragos) действует по крайней мере с 2017 года и известна своей организацией и участием в кампаниях кибершпионажа и кражи данных.

Они также продали доступ к взломанным корпоративным сетям другим злоумышленникам на подпольных форумах и были обнаружены при использовании эксплойтов CVE-2020-5902 в атаках, нацеленных на уязвимые устройства F5 BIG-IP.

Fox Kitten также предоставляет доступ к сетям скомпрометированных объектов другой иранской хакерской группе, известной как APT33 (также известной как Elfin, Magnallium).

Pay2Key - это относительно новая операция по вымогательству, которая в течение последнего месяца была нацелена на израильские и бразильские организации.

Банда вымогателей демонстрирует навыки APT

Начиная с октября 2020 года Fox Kitten использует атаки программ-вымогателей Pay2Key в качестве прикрытия для кражи конфиденциальной информации из промышленных, страховых и логистических компаний.

Группа использовала уязвимости в продуктах Pulse Secure, Fortinet, F5 и Global Protect VPN или общедоступный протокол удаленного рабочего стола (RDP), чтобы получить доступ к сетям целей и развернуть полезные нагрузки вредоносных программ.

«Способность операторов Pay2Key быстро распространить программу-вымогатель в течение часа по всей сети», как обнаружила Check Point, также дает намек на то, что группа, скорее всего, является спонсируемой государством операцией с навыками APT-класса и Ресурсы.

Они также настроили поворотное устройство, которое будет использоваться в качестве прокси-сервера исходящей связи между зараженными устройствами и серверами C2, что помогает им избежать или снизить риск обнаружения перед шифрованием всех доступных сетевых систем.

Согласно израильским фирмам по кибербезопасности Profero и Security Joes, индикаторы компрометации, обнаруженные во время атак программ-вымогателей Pay2Key, также связывают их с предыдущими иранскими деструктивными атаками.

В ходе недавних атак Pay2Key не использовались программы-вымогатели

Еще один намек на то, что операции Pay2Key направлены на кражу информации, заключается в том, что группа даже не развернула полезные нагрузки вымогателей в сетях недавних жертв, а вместо этого использовала украденные данные только в целях вымогательства.

Израильские СМИ сообщили, что злоумышленники (предположительно, операторы Pay2Key) взломали израильскую компанию по разработке программного обеспечения для морских и грузовых перевозок Amital в начале этого месяца и использовали полученный доступ для компрометации 40 клиентов Amital в ходе атаки на цепочку поставок.

Другой злоумышленник, отслеживаемый как BlackShadow, заявил о кибератаке против израильской страховой компании Shirbit и потребовал 1 миллион долларов, чтобы предотвратить утечку украденного.

Хотя атака, которая скомпрометировала системы Shirbit, очень похожа на атаки Pay2Key, пока не известно, связаны ли они каким-либо образом.

«Нет, мы еще не нашли никакой связи между Fox Kitten, Pay2Key и BlackShadow», - сказал BleepingComputer ведущий исследователь киберразведки ClearSky Охад Зайденберг.

«По нашим оценкам, курс действий был направлен на создание паники, информационную войну и отказ от получения выкупа».

Искра атак Pay2Key

Израильские исследователи кибербезопасности считают, что эти атаки участились из-за недавнего убийства иранского ученого-ядерщика.

Profero также связал атаки Pay2Key с иранскими участниками угроз в ноябре после отслеживания кошельков группы для выплаты выкупа на иранских биржах биткойнов.

«Мы со средней степенью уверенности считаем, что эта кампания (Pay2Key) является частью информационной войны с Ираном, направленной на создание паники в Израиле и других странах мира», - добавила ClearSky.

«Группа вымогателей pay2key публично угрожала Израилю, это может указывать на то, что эта операция является всего лишь пропагандистской кампанией, направленной на то, чтобы вызвать страх с отвлечением внимания от реального противника»…» ***(Sergiu Gatlan. Iranian nation-state hackers linked to Pay2Key ransomware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/iranian-nation-state-hackers-linked-to-pay2key-ransomware/). 17.12.2020).***

***

«Программа-вымогатель MountLocker недавно получила обновление, которое сократило ее размер вдвое, но сохранило уязвимость, которая потенциально может позволить узнать случайный ключ, используемый для шифрования файлов.

Эта операция вымогателя началась в июле 2020 года и нацелена на корпоративные сети . Его операторы крадут данные перед их шифрованием и угрожают жертвам утечкой файлов, если их требования о многомиллионном выкупе не будут выполнены.

Обрезанный новый вариант

Во второй половине ноября исследователи вредоносных программ увидели вторую версию MountLocker в дикой природе с подсказками о том, что ее операторы готовятся к налоговому сезону .

Исследование Виталия Кремеза, реверс-инженера и генерального директора Advanced Intelligence (AdvIntel), показывает, что разработчики программ-вымогателей добавили расширения файлов (.tax, .tax2009, .tax2013, .tax2014), связанные с программным обеспечением TurboTax, для подготовки документов налоговой декларации.

В опубликованном сегодня техническом анализе BlackBerry Research and Intelligence Team отмечает, что новый вариант MountLocker поставляется с отметкой времени компиляции от 6 ноября.

Разработчики вредоносного ПО уменьшили размер 64-битного варианта вредоносного ПО до 46 КБ, что примерно на 50% меньше, чем у предыдущей версии. Для этого они удалили список расширений файлов с более чем 2600 записями, предназначенными для шифрования.

Теперь он нацелен на гораздо меньший список, который исключает легко заменяемые типы файлов: .EXE, .DLL, .SYS, .MSI, .MUI, .INF, .CAT, .BAT, .CMD, .PS1, .VBS, .TTF, .FON, .LNK.

Новый код очень похож на старый, самым большим изменением является процесс удаления теневых копий тома и завершения процессов, который теперь выполняется с помощью сценария PowerShell перед шифрованием файлов.

Порок

BlackBerry заявляет, что 70% кода в новом MountLocker совпадает с кодом в предыдущей версии, включая небезопасную функцию Windows API GetTickCount, созданную вредоносным ПО для генерации случайного ключа шифрования (сеансового ключа).

GetTickCount устарел в пользу GetTickCount64. В своем списке рекомендаций по криптографии Microsoft перечисляет обе функции как небезопасные методы генерации случайных чисел.

BlackBerry заявляет, что использование API GetTickCount предлагает «небольшую возможность» для поиска ключей шифрования с помощью перебора.

Исследователи добавляют, что успех этой попытки зависит от знания значения счетчика метки времени во время выполнения программы-вымогателя.

MountLocker шифрует файлы на зараженных компьютерах с помощью потокового шифра ChaCha20, а затем сеансовый ключ шифруется 2048-битным открытым ключом RSA, встроенным в его код.

Входить и разноситься

Как и в случае с другими программами-вымогателями, разработчики MountLocker полагаются на аффилированные лица для взлома корпоративных сетей. Используемые ими методы обычно используются в атаках программ-вымогателей.

Исследование BlackBerry кампаний MountLocker показало, что субъекты часто получают доступ к сети жертвы через подключение к удаленному рабочему столу (RDP) со скомпрометированными учетными данными.

В этих атаках были замечены маяки Cobalt Strike и инструмент запроса активного каталога AdFind для разведки и перемещения по сети, в то время как FTP использовался для кражи файлов до этапа шифрования.

В инциденте, проанализированном BlackBerry, филиал MountLocker получил доступ к сети жертвы и приостановил работу на несколько дней перед возобновлением деятельности.

Исследователи считают, что злоумышленник сидит на месте, потому что они вели переговоры с разработчиками о присоединении к партнерской программе.

После получения программы-вымогателя злоумышленнику потребовалось около 24 часов, чтобы провести разведку, украсть файлы, переместиться в сторону и развернуть MountLocker.

Исследователи BlackBerry говорят, что быстрые операции, подобные этой, являются нормальным явлением для атак со стороны филиалов MountLocker, поскольку они могут украсть данные и зашифровать ключевые машины в сети за часы.

Несмотря на то, что эта разновидность программ-вымогателей является новой, она явно стремится к большим деньгам и, вероятно, расширит операции для получения максимальной прибыли. На его сайте утечки в настоящее время перечислено несколько жертв, которые не заплатили, но их число намного больше.

Даже если стоящая за ним группа не является «особенно продвинутой» на данный момент, исследователи ожидают, что она продолжит свои усилия в краткосрочной перспективе». ***(Ionut Ilascu. MountLocker ransomware gets slimmer, now encrypts fewer files // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/mountlocker-ransomware-gets-slimmer-now-encrypts-fewer-files/). 11.12.2020).***

***

«На прошлой неделе город Индепенденс, штат Миссури, подвергся атаке с использованием программ-вымогателей, которые продолжают мешать работе городских служб.

В начале месяца Independence подвергся атаке со стороны вымогателей, в результате чего им пришлось выключить свою ИТ-систему, когда они оправлялись от атаки.

«В Городе Индепенденс недавно произошло событие, которое привело к техническим трудностям и нарушению работы множества служб. Похоже, что эти сбои являются результатом события, связанного с вымогательством, которое было обнаружено и остановлено до того, как оно могло заразить всю сеть города», - Город Независимости Об этом говорится в заявлении городского менеджера Зака Уокера.

Уокер также заявил, что они выполняют полное сканирование системы и восстанавливают зашифрованные машины из доступных резервных копий. Процесс восстановления вызывает дальнейшие перебои в работе городских служб, включая отправку счетов за коммунальные услуги и онлайн-платежи.

«Чтобы защитить целостность наших систем, когда мы начали замечать некоторую вредоносную активность, мы отключили все наши системы», - сказал Уокер KSHB Kansas City. «Одна из систем, которая была взломана, когда мы добровольно отключили ее, была система выставления счетов за коммунальные услуги».

Из-за проблем с их системами городские власти не будут взимать плату за просрочку платежей за пропущенные платежи из-за атаки программ-вымогателей.

Уокер заявляет, что они все еще расследуют, не украли ли злоумышленники данные города, включая данные жителей и сотрудников.

К сожалению, большинство группировок программ-вымогателей теперь крадут незашифрованные файлы до того, как злоумышленники развернут программу-вымогатель. Затем эти файлы используются в стратегиях двойного вымогательства, когда банды вымогателей угрожают выпустить файлы на сайте утечки данных, если выкуп не будет уплачен.

Злоумышленники сообщили BleepingComputer, что жертв обычно больше беспокоит утечка украденных данных, чем потеря зашифрованных файлов.

На данный момент ни одна из операций вымогателей не привлекла внимание к атаке». ***(Lawrence Abrams. Ransomware attack causing billing delays for Missouri city // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ransomware-attack-causing-billing-delays-for-missouri-city/). 15.12.2020).***

***

«В последние годы программы-вымогатели превратились из простого шифрования файлов / отключения сетей с требованием выкупа до сложных атак, которые часто связаны с фактическим доступом к данным, кражей, а иногда и с угрозой публикации. Эти изощренные атаки вредоносного ПО часто уничтожают резервные копии и предоставляют преступникам еще больше рычагов воздействия на своих жертв, вынуждая их платить выкуп. Программы-вымогатели

нацелены не только на предприятия - они часто используются для атак на больницы, исследовательские учреждения и другие государственные службы, которые особенно важны во время этой глобальной пандемии.

Атаки программ-вымогателей все чаще ассоциируются с крупными изощренными киберпреступными организациями, когда центральная структура предоставляет инструменты, обучение и возможности для сбора выкупа и отправки своих «партнеров» для причинения вреда. Пока жертвы продолжают платить выкуп, Ransomware может расширяться. Программы-вымогатели также адаптируются для новых преступных целей. Все чаще хакеры, связанные с такими странами, как Иран и Северная Корея, используют программы-вымогатели, чтобы генерировать приток денежных средств в свои экономические потоки и обходить экономические санкции. Столкнувшись с острой необходимостью остановить распространение программ-вымогателей, правоохранительные органы отказываются от своей старой стратегии, заключающейся в том, чтобы не поощрять жертв платить выкуп. Регулирующие органы, такие как OFAC и SEC, вводят правила, чтобы жертвы не платили выкуп, чтобы избежать атаки программ-вымогателей. Эти правила вооружают правоохранительные органы новым механизмом правоприменения, позволяя им наказывать компании, решившие платить выкуп в случае атаки программ-вымогателей. Соответственно, они сигнализируют о новой области нормативного правоприменения, которая, вероятно, станет самым мощным инструментом правительства для сдерживания распространения программ-вымогателей.

Изменения в законодательстве по борьбе с программами-вымогателями

В отсутствие доказательств доступа к данным или кражи инцидент с программами-вымогателями не может рассматриваться как нарушение и, следовательно, может выходить за рамки любых требований к отчетности о киберинцидентах. Соответственно, в этих обстоятельствах организация могла заплатить выкуп, потенциально позволяя ей восстановить функциональность и избежать репутационного ущерба, который может возникнуть после публикации успешной атаки. Но сохранение этих атак в неведении создает волновой эффект в кибербезопасности, благодаря которому преступники просто продолжают совершать атаки программ-вымогателей.

В октябре OFACвыпустила консультативное сообщение, в котором разъясняется, что любой платеж, произведенный субъекту, на который наложены санкции, даже если платеж осуществляется под давлением атаки программы-вымогателя, будет нарушением федеральных санкций. Примечательно, что санкции OFAC предусматривают строгую ответственность, поэтому намерение жертвы не является защитой, равно как и незнание потерпевшей о том, что платеж направляется субъекту санкций. Фактически, Консультативный совет развеивает любую надежду на то, что OFAC может рассматривать недостаток знаний и намерений жертвы как смягчающий фактор - как это иногда бывает в других контекстах. В Консультативном сообщении четко указано, что OFAC намеревается агрессивно применять эти правила, даже если жертва не знала, что она платит стороне, подпадающей под санкции: «OFAC может налагать гражданские санкции за нарушение санкций на основе строгой ответственности, что означает, что лицо,

подпадающее под действие санкций США юрисдикция может быть привлечена к гражданской ответственности, даже если она не знала или не имела оснований знать, что она совершала транзакцию с лицом, которая запрещена законами и постановлениями о санкциях, администрируемыми OFAC». Это вызывает серьезную озабоченность: в контексте платежей от программ-вымогателей, когда преступник скрывает свою истинную личность, может быть сложно точно определить, кто получит выкуп, и является ли сторона, требующая выплаты, санкционированным лицом. Злоумышленники-вымогатели также вынуждают жертв совершать выкуп небанковскими методами, часто с использованием конкретных криптовалют, таких как Monero, поэтому нельзя даже полагаться на информацию о проводе или другие способы идентификации получателя платежа. В этих обстоятельствах жертва практически не может быть полностью уверена в том, что выкуп не направлен на санкционированное лицо.

Развивающаяся угроза программ-вымогателей в сочетании с рекомендациями OFAC также, вероятно, увеличит количество событий, которые необходимо раскрывать в соответствии с последними рекомендациями SEC по кибербезопасности. В руководстве описаны требования к раскрытию информации в отношении программ-вымогателей и других кибератак. Согласно руководству, компании должны раскрывать существенную информацию в периодических отчетах в соответствии с обязательствами Закона о ценных бумагах и Закона о биржах, а в некоторых случаях - в текущих отчетах. Требования к раскрытию информации связаны с существенностью, что требует от компании раскрытия «такой дополнительной существенной информации, если таковая имеется, которая может быть необходима для того, чтобы сделать требуемые заявления, в свете обстоятельств, при которых они сделаны, не вводя в заблуждение. Комиссия по ценным бумагам и биржам будет рассматривать информацию как существенную, если существует «существенная вероятность того, что разумный инвестор сочтет информацию важной при принятии инвестиционного решения или что раскрытие пропущенной информации будет рассматриваться разумным инвестором как существенное изменение общий набор доступной информации ». Регулирующие риски, связанные с выплатой выкупа, а также более широкие криминальные цели сегодняшних атак программ-вымогателей, вероятно, будут означать, что о новых атаках необходимо будет сообщать как о существенных событиях.

Выводы

Новые рекомендации OFAC по программам-вымогателям поднимают важные вопросы о приоритетах OFAC в области правоприменения, а также о его ожиданиях в отношении соблюдения. Например, Консультативный совет поднимает вопрос о том, можно ли когда-либо проводить транзакцию со стороной, которая не полностью идентифицировала себя, и, по крайней мере, предполагает необходимость повышенной должной осмотрительности в этих обстоятельствах, если организация все же решит платить выкуп, несмотря на юридический риск. Консультативный совет также предполагает, что OFAC может более ограниченно рассматривать смягчающие обстоятельства, такие как недостаток знаний и принуждение, во внимание к нарушениям санкций в других контекстах, помимо

программ-вымогателей. Один из открытых вопросов - определить, какой вес OFAC придаст

Хотя само по себе не является незаконным выплата выкупа преступнику, не связанному с субъектом санкций, часто невозможно определить, кто виноват в нападении. Любая организация, рассматривающая возможность выплаты выкупа, и экосистема, которая может поддержать такой платеж, должны учитывать этот риск при оценке решения о том, платить ли выкуп или нет.

Фирмы должны учитывать влияние требований OFAC (и других нормативных актов, которые неизбежно появятся для решения проблем, связанных с программами-вымогателями) при заключении договоров с третьими сторонами, чтобы их партнеры понимали, что от них будет ожидать в случае инцидента с программами-вымогателями. Похоже, что цель правоохранительных органов состоит в том, чтобы сочетание улучшенной отчетности и препятствий для выплаты выкупа отключило и, в конечном итоге, предотвратило будущие угрозы программ-вымогателей». ***(Seetha Ramachandran, Nolan Goldberg, Hena M. Vora. Regulatory Crackdown on Ransomware // Proskauer Rose LLP (https://www.privateequitylitigation.com/2020/12/regulatory-crackdown-on-ransomware/). 14.12.2020).***

***

«Медицинский центр Большого Балтимора (GBMC) в минувшие выходные (5-6 декабря) подвергся атаке с использованием программ-вымогателей, из-за которой процедуры, запланированные на понедельник, могли быть отложены. Кибератаки на поставщиков медицинских услуг и больницы находятся на рекордно высоком уровне, что особенно сложно, когда больницы пытаются удовлетворить растущую потребность в услугах во время пандемии.

GMBC заявила, что информация о пациентах не использовалась ненадлежащим образом, и она работает с правоохранительными органами и экспертами по кибербезопасности, чтобы восстановиться после инцидента.

Это страшное напоминание о том, насколько важно для больниц, медицинских центров и поставщиков медицинских услуг сохранять меры по предотвращению кибербезопасности в качестве главного приоритета, даже когда COVID-19 бушует по всей стране и требует больших затрат на ресурсы здравоохранения. Киберпреступники не сочувствуют стрессу, который испытывают лица, обеспечивающие уход во время пандемии, и фактически используют его, чтобы воспользоваться уязвимыми системами в самый неподходящий момент». ***(LINN FOSTER FREEDMAN. Greater Baltimore Medical Center Hit with Ransomware // Robinson+Cole (https://www.dataprivacyandsecurityinsider.com/2020/12/greater-baltimore-medical-center-hit-with-ransomware/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+DataPrivacyAndSecurityInsider+%28Data+Privacy+%2B+Security+Insider%29). 10.12.2020).***

***

«Программы-вымогатели - одна из самых серьезных угроз для бизнеса. Организация, ставшая жертвой атаки программ-вымогателей, в ходе которой киберпреступники используют вредоносное ПО для шифрования сети, выводя ее из строя, быстро обнаружит, что вообще не может вести бизнес.

Киберпреступники блокируют подобные сети по одной простой причине: это самый быстрый и простой способ заработать деньги на скомпрометированной организации, и их вряд ли поймают.

Злоумышленники требуют выкуп в обмен на ключ дешифрования файлов - и в течение 2020 года требования к вымогательству росли, и теперь банды вымогателей регулярно требуют от жертв миллионы долларов в биткойнах.

SEE: выигрышная стратегия кибербезопасности (специальный отчет ZDNet) | Скачать отчет в формате PDF (TechRepublic)

Прискорбная реальность такова, что программы-вымогатели продолжают пользоваться успехом, потому что значительное число жертв уступают вымогательским требованиям преступников, платя выкуп. Хотя полиция и компании, занимающиеся кибербезопасностью, заявляют, что организации не должны платить преступникам, многие считают, что это самый быстрый и простой способ восстановить свою сеть и предотвратить долгосрочный экономический ущерб, хотя он по-прежнему создает множество постоянных проблем.

А банды вымогателей все чаще прибегают к новой тактике, пытаясь заставить жертв заплатить; они угрожают утечкой украденных данных от жертвы, а это означает, что конфиденциальные корпоративные данные или личная информация клиентов и клиентов в конечном итоге становятся доступными для других преступников.

«С точки зрения финансово мотивированного преступника, программы-вымогатели остаются наиболее прибыльным типом кибератак, особенно когда жертвами становятся крупные предприятия. В конце 2020 года киберпреступники активизируют свои атаки, чтобы максимизировать свою финансовую выгоду и повысить шансы на получение оплаты. "- говорит Анна Чанг, аналитик по исследованию угроз кибербезопасности подразделения 42 Palo Alto Networks.

Атаки программ-вымогателей стали более мощными и прибыльными, чем когда-либо прежде - до такой степени, что продвинутые киберпреступные группы переключились на их использование вместо своих традиционных форм преступности - и весьма вероятно, что они просто станут еще более мощными в 2021 г.

Например, что, если банды вымогателей могут поразить сразу несколько различных организаций в рамках скоординированной атаки? Это даст возможность незаконно заработать крупную сумму денег за очень короткий промежуток времени - и один из способов, которым злоумышленники могут попытаться сделать это, - это поставить под угрозу облачные службы с помощью программ-вымогателей.

«Следующее, что мы увидим, - это, вероятно, больше внимания уделяется облаку. Поскольку все переходят в облако, COVID-19 ускорил развертывание облаков во многих организациях, поэтому в большинстве организаций данные

хранятся в облаке», - говорит Эндрю Роуз., постоянный директор по информационной безопасности в Proofpoint.

Мы узнали о масштабах повсеместных сбоев, которые могут возникнуть, когда киберпреступники нацелены на умные часы и производителя носимых устройств Garmin с помощью программ-вымогателей. Атака оставила пользователей по всему миру без доступа к его сервисам на несколько дней.

Если бы злоумышленники могли получить доступ к облачным сервисам, используемым несколькими организациями, и зашифровать их, это вызвало бы массовые нарушения сразу во многих организациях. И вполне возможно, что в этом сценарии банды вымогателей потребуют десятки миллионов долларов в качестве платы за вымогательство из-за того, что поставлено на карту.

Деструктивная природа программ-вымогателей может также привести к их использованию с помощью хакерских операций, не мотивированных исключительно деньгами.

Первый пример этого был в 2017 году, когда NotPetya разрушил сети организаций по всему миру и нанес ущерб в миллиарды долларов. Хотя атака была разработана, чтобы выглядеть как программа-вымогатель, на самом деле вредоносная программа была разработана для полного уничтожения, поскольку не было даже способа заплатить требование выкупа.

NotPetya был приписан российским военным, и вполне вероятно, что идея использования программ-вымогателей в качестве чисто разрушительной кибератаки не осталась незамеченной другими национальными государствами. Для правительства или вооруженных сил, которые не хотят, чтобы их противник знал, кто стоит за разрушительной атакой вредоносного ПО, выдача себя за киберпреступников может стать полезным средством уловки.

«Мы уже видели прецедент, созданный субъектами национального государства, которые использовали это, но что, если они перейдут к следующему шагу? Деструктивные возможности программ-вымогателей, безусловно, привлекательны для злоумышленников, и они могут использовать его для вызывают сбои ", - говорит Сандра Джойс, старший вице-президент и глава отдела глобальной разведки FireEye.

«По мере того, как мы продолжаем видеть рост числа программ-вымогателей в преступном подполье, мы должны помнить о том, что национальные государства наблюдают за ними и могут использовать их в качестве своего любимого оружия», - добавляет она.

Программы-вымогатели по-прежнему будут представлять серьезную угрозу, но предприятия могут защитить себя от них, применив небольшое количество относительно простых методов кибербезопасности.

Организации должны убедиться, что у них есть хорошо управляемый план применения исправлений кибербезопасности и других обновлений. Эти исправления часто выпускаются потому, что компании-разработчики программного обеспечения узнали об известных уязвимостях в своих продуктах, которые могут быть использованы киберпреступниками - быстрое и своевременное применение исправлений предотвращает их использование злоумышленниками как средство проникновения в сеть.

SEE: Cybersecurity: Давайте перейдем к тактике (специальная функция ZDNet / TechRepublic) | Загрузите бесплатную версию в формате PDF (TechRepublic)

Еще один метод, который киберпреступники используют для проникновения в сети, - это использование слабых паролей, либо покупка их на форумах темной сети, либо просто угадывание общих паролей или паролей по умолчанию.

Чтобы предотвратить это, организациям следует поощрять сотрудников использовать более сложные пароли, а учетные записи должны иметь дополнительную безопасность многофакторной аутентификации, поэтому, если злоумышленнику удастся взломать учетные данные для входа в сеть, им будет труднее передвигаться. Это.

Компании также должны быть готовы к тому, что может произойти, если они в конечном итоге станут жертвами атаки программ-вымогателей. Регулярное создание резервных копий сети и их хранение в автономном режиме означает, что если произойдет худшее и программа-вымогатель зашифрует сеть, ее можно будет восстановить с относительно недавней точки - и не уступая требованиям киберпреступников.

Потому что в конечном итоге, если хакерские банды перестанут зарабатывать деньги на программах-вымогателях, они больше не будут заинтересованы в проведении кампаний». ***(Danny Palmer. Ransomware: Attacks could be about to get even more dangerous and disruptive // ZDNet (https://www.zdnet.com/article/ransomware-why-these-attacks-could-get-even-more-dangerous-and-disruptive/). 23.12.2020).***

***

«Гигант бытовой техники Whirlpool подвергся атаке вымогателей со стороны банды вымогателей Nefilim, которая украла данные перед шифрованием устройств.

Whirlpool - один из крупнейших в мире производителей бытовых приложений под своим именем и KitchenAid, Maytag, Brastemp, Consul, Hotpoint, Indesit и Bauknecht. В Whirlpool работает 77000 человек в 59 производственных и технологических исследовательских центрах по всему миру, и выручка компании в 2019 году составила около 20 миллиардов долларов.

На выходных банда вымогателей Nefilim опубликовала файлы, украденные из Whirlpool во время атаки программы-вымогателя. Утечка данных включала документы, связанные с выплатами сотрудникам, запросами на размещение, запросами медицинской информации, проверками биографических данных и многим другим.

Источник в индустрии кибербезопасности сообщил…, что банда вымогателей Nefilim атаковала Whirlpool в первые выходные декабря.

В заявлении для BleepingComputer Whirlpool подтвердила атаку и что их системы были полностью восстановлены после атаки…

Nefilim не является особо активной операцией по вымогательству, но известен своими атаками на других крупных и известных жертв в прошлом.

Другие жертвы, на которые напал Nefilim, включают Orange SA, Dussman Group, Luxottica и Toll Group .

Updae 12/28/20 : системы Whirlpool полностью восстановлены, а не восстанавливаются медленно, как было заявлено изначально». ***(Lawrence Abrams. Home appliance giant Whirlpool hit in Nefilim ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/home-appliance-giant-whirlpool-hit-in-nefilim-ransomware-attack/). 28.12.2020).***

***

«Транспортная и логистическая компания Forward Air пострадала от атаки вымогателей со стороны новой банды вымогателей, которая повлияла на бизнес-операции компании.

Forward Air - ведущая компания в сфере грузоперевозок и авиаперевозок, базирующаяся в Теннесси, США. Выручка компании за 2019 год составила 1,4 миллиарда долларов, в ней работает более 4300 человек.

На прошлой неделе FreightWaves сообщил, что Forward Air подверглась кибератаке, вынудившей их отключить свои системы, чтобы предотвратить распространение атаки. Позже Forward Air подтвердила эту атаку в заявлении для BleepingComputer.

«15 декабря Forward Air обнаружила инцидент в области ИТ-безопасности, который повлиял на функциональность определенных компьютерных систем. В соответствии с нашими протоколами информационной безопасности мы немедленно отключили наши системы, уведомили правоохранительные органы и привлекли нескольких сторонних экспертов, чтобы они помогли нам в проведении «Внутреннее расследование. Наша ИТ-команда усердно работает над восстановлением затронутых систем и служб и их возвращением в работу как можно скорее», - говорится в заявлении Forward Air для BleepingComputer.

Согласно FreightWaves, атака привела к нарушению работы бизнеса, поскольку документы, необходимые для выдачи груза с таможни, хранились в системах остановки и недоступны.

В настоящее время веб-сайт Forward Air не работает и просто отображает сообщение об «инциденте с ИТ-безопасностью» и о том, что сайт не работает, пока они восстанавливают затронутые системы…

Источники сообщили сегодня BleepingComputer, что Forward Air подверглась кибератаке в результате новой операции вымогателя, известной как Hades.

Обновление от 21.12.20, 18:37 EST: после того, как мы опубликовали нашу историю, Forward Air подала форму 8-K в Комиссию по ценным бумагам и биржам, сообщив, что они подверглись атаке с использованием программ-вымогателей.

«15 декабря 2020 года Forward Air Corporation (далее «Компания») обнаружила инцидент с использованием программ-вымогателей, повлиявший на ее операционные и информационные системы, что вызвало задержки обслуживания для многих ее клиентов. Сразу после обнаружения инцидента Компания инициировала протоколы реагирования, начали расследование и привлекли к работе специалистов по кибербезопасности и криминалистике. Компания также взаимодействовала с соответствующими правоохранительными органами», - говорится в форме 8-K.

Банда вымогателей Hades, стоящая за этой атакой, начала действовать около недели назад в атаках на предприятие, организованных человеком.

При шифровании жертвы создается записка с требованием выкупа под названием «HOW-TO-DECRYPT- [extension] .txt», которая напоминает заметки, используемые группой программ-вымогателей REvil…

В записках о выкупе указан URL-адрес сайта Tor, уникальный для каждой жертвы. Этот URL-адрес приводит вас на сайт Tor, содержащий информацию об атаке и адрес Tox-мессенджера, который жертвы могут использовать для связи со злоумышленниками, что является одинаковым для всех жертв.

Когда мы связались через Tox с злоумышленниками, они не пожелали предоставить какую-либо информацию о своих атаках. Однако они поделились учетной записью Twitter, название которой указывает на то, что они будут использовать ее для утечки файлов, украденных во время атак.

Неизвестно, сколько денег требуется для восстановления файлов, а образец вымогателя не обнаружен». ***(Lawrence Abrams. rucking giant Forward Air hit by new Hades ransomware gang // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/trucking-giant-forward-air-hit-by-new-hades-ransomware-gang/). 21.12.2020).***

***

«…Microsoft и McAfee возглавили новую коалицию по борьбе с вымогательским ПО, в которую вошли девятнадцать ИТ- и ИБ-компаний, а также некоммерческих организаций.

Группа получила название Ransomware Task Force (RTF), и ее специалисты сосредоточатся на оценке существующих технических решений, обеспечивающих защиту от атак программ-вымогателей.

RTF будет заказывать экспертные статьи по данной теме, привлекать заинтересованные стороны из разных отраслей, выявлять пробелы в текущих решениях, а затем разработает общую “дорожную карту”, чтобы поставленные задачи решались всеми членами группы.

Конечным результатом стараний RTF должна стать стандартизированная структура для борьбы с атаками вымогателей, основанная на общем отраслевом консенсусе, а не на индивидуальных рекомендациях, полученных от отдельных подрядчиков…» ***(Мария Нефёдова. Microsoft и McAfee сформировали рабочую группу для борьбы с шифровальщиками // Xakep (https://xakep.ru/2020/12/23/ransomware-task-force/). 23.12.2020).***

***

«Копания Sangoma сообщила о кибератаке на свои системы после того, как операторы вымогательского ПО Conti похитили и опубликовали ее документы.

Sangoma является производителем аппаратного и программного обеспечения для VoIP-телефонии. Наиболее популярный продукт компании – технология FreePBX, позволяющая организациям создавать в своих сетях недорогие корпоративные телефонные системы.

На этой неделе операторы вымогательского ПО Conti опубликовали на своем сайте утечек более 26 ГБ данных, похищенных у Sangoma в результате недавней кибератаки. Утекшая информация включает файлы, относящиеся к бухгалтерскому учету, финансам, приобретениям, льготам и зарплате сотрудников, а также юридические документы. В четверг, 24 декабря, Sangoma подтвердила кибератаку на свои системы и последующую за ней утечку данных.

Сейчас, когда жертвой хакеров становится производитель программного обеспечения, есть риск того, что злоумышленники могли модифицировать его продукты с целью доставки вредоносного ПО в сети его клиентов в рамках атаки на цепочку поставки. Ярким примером такого сценария является взлом техасского производителя платформы для управления IT-ресурсами SolarWinds. Тем не менее, Sangoma уверила своих клиентов в том, что никаких признаков взлома клиентских учетных записей или продуктов Sangoma обнаружено не было…». ***(Вымогатель Conti похитил документы у популярного производителя ПО для VoIP-телефонии // SecurityLab.ru (https://www.securitylab.ru/news/515107.php). 25.12.2020).***

***

Програми-трояни

«Аналитики Palo Alto Networks сообщают, что как минимум с октября текущего года операторы трояна njRAT используют Pastebin в качестве управляющего сервера, чтобы избежать внимания со стороны ИБ-исследователей.

Отчет компании гласит, что Pastebin используется злоумышленниками для загрузки и выполнения пейлоадов вторичного уровня, что полностью избавляет их от необходимости иметь традиционный командно-управляющий сервер.

Пейлоады хакеров различаются по форме и формату. Так, в некоторых случаях дампы закодированы base64, в других случаях их истинную природу скрывают шестнадцатеричная кодировка и JSON; некоторые дампы сжаты, а другие представляют обычный текст, содержащий вредоносные URL-адреса.

Среди образцов, изученных экспертами, одна полезная нагрузка оказалась исполняемым файлом .NET, который злоупотреблял функциями Windows API для кейлоггинга и кражи данных. Другие образцы, аналогичные по функциям, требовали нескольких уровней декодирования для обнаружения конечного пейлоада. Эксперты полагают, что данные в формате JSON в теории могут быть файлами конфигурации малвари. Также контент с Pastebin использовался хакерами для указания на загрузки различного ПО, включая, например, ProxyScraper.

«Судя по нашему анализу, авторы малвари заинтересованы в размещении своих полезных нагрузок второго уровня на Pastebin, а также в шифровании или обфускации этих данных для обхода защитных решений.

Есть вероятность, что авторы вредоносных программ будут использовать подобные Pastebin сервисы в долгосрочной перспективе», — заключают исследователи». ***(Мария Нефёдова. Операторы njRAT используют Pastebin как***

управляющий сервер // Xakep (https://xakep.ru/2020/12/11/njrat-pastebin-2/). 11.12.2020).

***

«Троян удаленного доступа (RAT), продаваемый на подпольных форумах, превратился в злоупотребление Tor при сохранении устойчивости на зараженных машинах.

В четверг Сивагнанам Гн и Шон Галлахер из Sophos Labs сообщили о продолжающемся исследовании вредоносного ПО, которое существует с 2019 года.

Получивший название SystemBC, RAT превратился из виртуальной частной сети (VPN) через прокси-сервер SOCKS5 в бэкдор, который использует сеть Tor для обеспечения устойчивости и усложняет отслеживание подключенных командно-управляющих серверов (C2).

По словам исследователей, вредоносная программа SystemBC для Windows способна выполнять команды Windows, развертывать сценарии, внедрять вредоносные библиотеки DLL, удаленное администрирование и мониторинг, а также устанавливать бэкдоры для операторов, чтобы подключать вредоносное ПО к C2 для получения команд.

Sophos Labs сообщает, что в течение года SystemBC развивалась и функции были улучшены, что привело к росту популярности среди покупателей, включая операторов программ-вымогателей.

После развертывания RAT скопирует и запланирует себя как услугу, но пропустит этот шаг при обнаружении антивирусного программного обеспечения Emsisoft. Затем устанавливается соединение с C2 через маяковое соединение с удаленным сервером на одном из двух жестко заданных доменов - с адресами, различающимися по образцам, - а также с легким клиентом Tor.

«Коммуникационный элемент Tor в SystemBC, по-видимому, основан на mini-tor, библиотеке с открытым исходным кодом для облегченного подключения к анонимной сети Tor», - отмечают исследователи. «Код mini-Tor не дублируется в SystemBC [...], но реализация ботом клиента Tor очень похожа на реализацию, используемую в программе с открытым исходным кодом, включая широкое использование Windows Crypto Next Gen (CNG) Базовые криптографические функции API (BCrypt) ".

За последние несколько месяцев SystemBC был отслежен в «сотнях» развертываний, включая недавние атаки программ-вымогателей Ryuk и Egregor. Команда утверждает, что бэкдор был развернут после того, как кибератаки получили доступ к учетным данным сервера в этих атаках, а SystemBC действовала как ценное средство устойчивости к основным используемым штаммам вредоносного ПО.

SystemBC был развернут как готовый инструмент, который, вероятно, был получен в результате сделок «вредоносное ПО как услуга», заключенных на подпольных форумах, и в некоторых случаях присутствовал на зараженных машинах в течение нескольких дней - или недель - за раз.

«SystemBC - привлекательный инструмент для операций такого типа, поскольку он позволяет одновременно работать с несколькими целями с помощью

автоматизированных задач, что позволяет автоматизировать развертывание программ-вымогателей с использованием встроенных инструментов Windows, если злоумышленники получают надлежащие учетные данные, "Добавляет Sophos Labs». ***(Charlie Osborne. This 'off the shelf' Tor backdoor malware is now a firm favorite with ransomware operators // ZDNet (https://www.zdnet.com/article/this-off-the-shelf-tor-backdoor-malware-is-now-a-firm-favorite-with-ransomware-operators/). 17.12.2020).***

***

«Список десятков интернет-магазинов, взломанных группой веб-скимминга, был случайно пропущен дроппером, который использовался для развертывания скрытого трояна удаленного доступа (RAT) на взломанных сайтах электронной коммерции.

Злоумышленники используют эту RAT для поддержания устойчивости и восстановления доступа к серверам взломанных интернет-магазинов.

После подключения к магазинам злоумышленники развертывают скрипты скиммера кредитных карт, которые крадут и выводят личные и финансовые данные клиентов с помощью цифровых скимминговых атак (также известных как Magecart).

Сонные крысы на серверах интернет-магазина

Исследователи из Sansec, компании по обеспечению безопасности, специализирующейся на защите магазинов электронной коммерции от атак веб-скимминга, заявили, что вредоносная программа была доставлена в виде 64-битного исполняемого файла ELF с помощью дроппера вредоносных программ на основе PHP.

Чтобы избежать обнаружения и затруднить анализ, безымянный RAT предназначен для маскировки под серверный демон DNS или SSH, чтобы не выделяться в списке процессов сервера.

Вредоносная программа также работает в спящем режиме почти в течение дня, просыпаясь только один раз в день рано утром, в 7 часов утра, чтобы подключиться к своему командному серверу и запросить команды.

Образцы RAT, собранные Sansec с нескольких взломанных серверов, были скомпилированы злоумышленниками, стоящими за этими атаками как на Ubuntu, так и на Red Hat Linux.

«Это может указывать на то, что в этой кампании участвовало несколько человек», - говорится в отчете, опубликованном сегодня Сансеком.

«Или, например, что исходный код RAT общедоступен и, возможно, продается на рынках даркнета».

Пипетка RAT проливает фасоль

Несмотря на довольно продвинутую вредоносную программу RAT, которую они использовали в качестве бэкдора для взломанных серверов электронной коммерции, группа Magecart также сделала одну ошибку новичка, включив список взломанных интернет-магазинов в код своего дроппера.

Sansec захватил дроппер RAT злоумышленников и обнаружил, что он также содержит список из 41 скомпрометированного хранилища помимо обычного

вредоносного кода, используемого для анализа настроек развертывания для нескольких сценариев Magecart.

Это можно объяснить тем фактом, что дроппер был написан кем-то, у кого, кажется, гораздо меньше опыта работы с PHP, поскольку он «использует блоки разделяемой памяти, которые редко используются в PHP, но гораздо чаще встречаются в программах на языке C».

Sansec также обратился к интернет-магазинам, включенным в код вредоносного ПО Magecart, чтобы сообщить им, что на их серверы проникли.

За последние пару месяцев исследователи Sansec обнаружили несколько скиммеров Magecart и образцы вредоносных программ, которые используют инновационные тактики для сохранения или уклонения от обнаружения.

Сценарий кражи кредитных карт, найденный в трех разных магазинах, все еще активный, когда BleepingComputer сообщил информацию на прошлой неделе, скрывается на виду на взломанных сайтах с использованием кода CSS, поскольку он избегает обнаружения с помощью обычных методов, таких как автоматические сканеры безопасности и даже ручной аудит кода безопасности.

Они также недавно обнаружили вредоносное ПО для веб-скимминга, способное маскироваться под SVG-кнопки социальных сетей, и почти невозможно избавиться от кражи кредитных карт, которая объединяет постоянный бэкдор». ***(Sergiu Gatlan. Stealthy Magecart malware mistakenly leaks list of hacked stores // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/stealthy-magecart-malware-mistakenly-leaks-list-of-hacked-stores/). 18.12.2020).***

***

«Недавно обнаруженное семейство вредоносных программ на основе Python нацелено на процессы Outlook и учетные данные браузера жертв Microsoft Windows.

Исследователи обнаружили нового трояна, ворующего информацию, который нацелен на системы Microsoft Windows с атакой возможностей кражи данных - от сбора учетных данных браузера до нацеливания на файлы Outlook.

По словам исследователей, троян под названием PyMicropsia (из-за того, что он построен на Python) был разработан группой угроз AridViper, которая известна своей атакой на организации на Ближнем Востоке.

«AridViper - активная группа угроз, которая продолжает разрабатывать новые инструменты как часть своего арсенала», - заявили исследователи из исследовательской группы Unit42 в Пало-Альто в понедельник. «Кроме того, исходя из различных аспектов PyMicropsia, которые мы проанализировали, некоторые разделы вредоносного ПО все еще не используются, что указывает на то, что это, вероятно, семейство вредоносных программ, которое активно разрабатывается этим субъектом».

Возможности трояна по краже информации включают загрузку файлов, загрузку / выполнение полезной нагрузки, кражу учетных данных браузера (и возможность очищать историю просмотров и профили), создание снимков экрана и ведение кейлоггеров. Кроме того, вредоносная программа может собирать информацию о файлах, удалять файлы, перезагружать машины, собирать

информацию с USB-накопителя и записывать аудио; а также собирать файлы .OST Outlook и убивать / отключать процессы Outlook.

OST-файл, также известный как автономный файл данных Outlook, используется учетными записями Microsoft, учетными записями Exchange и учетными записями Outlook.com «для хранения синхронизированной копии информации вашего почтового ящика на вашем локальном компьютере», согласно Microsoft. Файлы OST могут содержать сообщения электронной почты, контакты, задачи, данные календаря и другую информацию об учетной записи.

Троян

Троян был преобразован в исполняемый файл Windows с помощью PyInstaller, пакета Python, позволяющего приложениям превращаться в автономные исполняемые файлы. После загрузки вредоносная программа «реализует свои основные функции, выполняя цикл, в котором она инициализирует различные потоки и периодически вызывает несколько задач с целью сбора информации и взаимодействия с оператором C2», по словам исследователей.

Злоумышленник использует как встроенные библиотеки Python, так и определенные пакеты для целей кражи информации, включая PyAudio (включение возможностей кражи звука) и mss (разрешение снимков экрана).

«Ожидается, что встроенные библиотеки Python будут использоваться для различных целей, таких как взаимодействие с процессами Windows, реестром Windows, сетью, файловой системой и т.д.», - заявили исследователи.

PyMicropsia имеет отношение к семейству вредоносных программ Micropsia, еще одного вредоносного ПО AridViper, известного своей нацеленностью на Microsoft Windows. Эти ссылки включают перекрытия кода; аналогичные тактики, приемы и процедуры (TTP), такие как использование rar.exe для сжатия данных для извлечения; и аналогичные структуры тракта URI связи с управлением и контролем (C2).

Micropsia также сделала ссылки на определенные темы в коде и реализациях C2, включая предыдущие ссылки на телешоу, такие как Теория большого взрыва и Игра престолов. Следует отметить, что в переменных кода PyMicropsia исследователи обнаружили ссылки на несколько известных имен актеров, актеров Фрэн Дрешер и Киану Ривз, что, по словам исследователей, «похоже, соответствует предыдущим наблюдениям за темами».

AridViper: активное развитие

Изучая возможности PyMicropsia, исследователи заявили, что они также выявили два дополнительных образца, размещенных в инфраструктуре злоумышленника.

Дополнительные образцы, которые загружаются и используются трояном во время развертывания, обеспечивают сохраняемость и возможности кейлоггеров. Они не основаны на Python / PyInstaller.

Хотя PyMicropsia предназначена только для операционных систем Windows, исследователи обнаружили в коде фрагменты, которые проверяют наличие других операционных систем (например, «posix» или «darwin»). Posix, или интерфейс переносимой операционной системы, представляет собой семейство стандартов,

используемых для обеспечения совместимости между операционными системами; и Дарвин - Unix-подобная операционная система с открытым исходным кодом.

«Это интересное открытие, поскольку мы не были свидетелями того, чтобы AridViper нацелилась на эти операционные системы раньше, и это может представлять собой новую область, которую актор начинает исследовать», - заявили они. «На данный момент найденный код очень прост и может быть частью усилий по копированию и вставке при построении кода Python, но в любом случае мы планируем держать его в поле зрения при исследовании новых действий». ***(Lindsey O'Donnell. New Windows Trojan Steals Browser Credentials, Outlook Files // Threatpost (https://threatpost.com/windows-trojan-steals-browser-credentials-outlook-files/162223/). 14.12.2020).***

***

«Вредоносная банда Dridex доставляет неприятный подарок к праздникам, используя рассылку спама под видом подарочных карт Amazon.

Dridex - это модульный банковский троян, который может выполнять различные вредоносные действия, включая кражу информации для входа в систему, регистрацию нажатий клавиш, создание снимков экрана, а также загрузку и установку дополнительных вредоносных программ.

Dridex особенно опасен, потому что, как известно, он предоставляет злоумышленникам DoppelPaymer и BitPaymer доступ к скомпрометированным сетям для развертывания их программ-вымогателей.

Фишинговая кампания Dridex хочет отправить подарок

При распространении вредоносных программ банды вредоносных программ обычно используют текущие события и праздники в качестве тем для фишинговых кампаний, чтобы побудить людей открыть вредоносные вложения.

Так обстоит дело в недавней фишинговой кампании, обнаруженной фирмой Cybereason, занимающейся кибербезопасностью, которая выдавала себя за подарочный сертификат Amazon, отправленный по электронной почте.

Эти электронные письма, показанные ниже, выдают себя за подарочный сертификат на 100 долларов, который пользователи должны погасить, нажав кнопку фишингового письма.

При нажатии кнопки загружаются вредоносные документы Word с именами, похожими на Amazon_Gift_Card, Order_Gift_Cart и Amazon_eGift-Card.

При открытии во вложениях будет указано, что они были созданы в онлайн-версии Microsoft Office, и получателю будет предложено нажать кнопку «Включить содержимое». Однако это приведет к запуску вредоносных макросов, которые загружают и устанавливают вредоносное ПО Dridex и, возможно, другие полезные нагрузки на компьютер жертвы.

С приближением праздников и когда так много людей празднуют удаленно, подарочные карты Amazon, вероятно, станут обычным подарком в этом сезоне. В связи с этим важно помнить, что Amazon никогда не предложит вам загрузить файл, чтобы выкупить подарочный сертификат.

Вместо этого в электронном письме с законной подарочной картой Amazon будет содержаться код, который вы активируете на сайте Amazon, чтобы пополнить свой счет.

Если вы получаете электронные письма под видом подарочных карт с предложением загрузить и открыть документы Word, немедленно закройте их. Если вы все еще не уверены в законности карты eGift, свяжитесь с отправителем по телефону (не по электронной почте!) И спросите, отправили ли он вам подарок». ***(Lawrence Abrams. Fake Amazon gift card emails deliver the Dridex malware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fake-amazon-gift-card-emails-deliver-the-dridex-malware/). 25.12.2020).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Суд Парижа у понеділок, 7 грудня, оголосив вирок у справі росіянина Александра Винника, обвинуваченого у вимаганні та відмиванні грошей у складі злочинної групи…

Його засудили до п'яти років тюремного ув'язнення і штрафу в розмірі 100 тисяч євро. Після вироку Винник може бути екстрадований в США, де його звинувачують у відмиванні грошей на суму близько 4 мільярдів доларів.

За даними слідства, Винник був причетний до розробки програми-здирника Locky. За заявою прокуратури Парижа, цілий ряд французьких компаній постраждали від цієї шкідливої програми і платформи BTC-e, створення якої також приписується Виннику.

Звинувачення вимагало для росіянина 10 років ув'язнення і штрафу в 750 тисяч євро.

Сам росіянин звинувачення на свою адресу не визнав.

У той же час суд Парижа зняв з Винника частину звинувачень у відмиванні грошей і повністю відхилив звинувачення в порушенні роботи автоматизованих систем ряду організацій і приватних осіб. Також з нього були зняті звинувачення у використанні вірусу Locky для здійснення кібератак.

Винника заарештували в Греції в 2017 році за запитом США, де йому може загрожувати до 55 років позбавлення волі за звинуваченням у шахрайстві і відмиванні грошей через біткоіни.

Крім США його екстрадиції зажадала і Росія - в 2018 році Винник зізнався російським правоохоронним органам в розкраданні 750 млн руб. Однак в січні 2020 року Греція видала Винника Франції.

Вирок паризького суду не означає, що Винник відбуде весь термін у Франції. Не виключено, що влада цієї країни погодиться на екстрадицію росіянина в США». ***(Франція засудила хакера з РФ до 5 років за вимагання та відмивання грошей // Європейська правда (https://www.eurointegration.com.ua/news/2020/12/8/7117393/). 08.12.2020).***

***

«Росіянин Андрій Тюрін, який зізнався в причетності до однієї з найбільших кібератак проти банківської системи США, заслуговує покарання майже в 20 років позбавлення волі «як вельми зухвалий і активний хакер» – таку позицію федеральному судді США висловили представники обвинувачення…

У вересні минулого року Андрій Тюрін визнав провину за декількома пунктами звинувачення, а саме в крадіжці даних понад 80 мільйонів клієнтів американського фінансового холдингу JPMorgan Chase & Co та інших організацій. Ці дії були частиною злочинної схеми на сотні мільйонів доларів, відзначає агентство.

Слідство стверджує, що Тюрін діяв спільно з іншим росіянином, Гері Шалоном, щоб отримати незаконний доступ до інформації про клієнтів 12 фінансово-аналітичних організацій, банків, інших фірм, включаючи Fidelity Investments, E-Trade Financial і Dow Jones & Co. Спільники використовували ці відомості для розсилки спаму, який рекламує різні акції з метою отримання прибутку від їх зростання, заявляють слідчі.

У службовій записці, переданій 1 грудня окружному судді Манхеттена Лорі Тейлор Суейн, уряд закликав засудити Тюріна на термін від 15 років і 8 місяців до приблизно 19 з половиною років позбавлення волі. Вердикт, як очікується, буде оголошений 3 грудня.

Андрій Тюрін був екстрадований у США з Грузії у вересні 2018 року. Представники Секретної служби США відзначали, що Тюріна можуть засудити до тюремного ув'язнення тривалістю до 92 років. Росіянин спочатку заявляв про свою невинуватість, але потім, згідно з матеріалами суду, пішов на угоду з прокуратурою.

Гері Шалон в 2015 році був заарештований в Тель-Авіві і згодом також екстрадований в США. Його справа поки що не закрита. За інформацією джерел, знайомих зі ситуацією, Шалон також співпрацює зі слідством». ***(Російського хакера можуть засудити до 20 років ув'язнення у США // Радіо Свобода (https://www.radiosvoboda.org/a/news-rosiyskyi-khaker-us/30980693.html). 02.12.2020).***

***

«Человек, ранее являвшийся несовершеннолетним, признал себя виновным в совершении федеральных правонарушений среди несовершеннолетних в связи с кибератакой, вызвавшей массовое нарушение работы Интернета в октябре 2016 года.

Об этом объявили исполняющий обязанности помощника генерального прокурора Брайан С. Рэббитт из уголовного отдела Министерства юстиции, прокурор США Скотт Мюррей из округа Нью-Гэмпшир и ответственный специальный агент Джозеф Р. Бонаволонта из Бостонского отделения ФБР.

Согласно соглашению о признании вины, данное лицо участвовало в сговоре с целью совершения компьютерного мошенничества и злоупотреблений, используя

ботнет и намеренно повредив компьютер. Поскольку на момент совершения преступления данное лицо было несовершеннолетним, личность человека не разглашается в соответствии с Законом о преступности несовершеннолетних, см. 18 USC § 5031 и след. Признание себя виновным было принято на закрытом судебном заседании перед главным судьей Ландией Б. Маккафферти в округе Нью-Гэмпшир. Судья Маккафферти назначил этому человеку приговор на 7 января 2021 года.

Согласно неопечатанным судебным документам, примерно с 2015 года по ноябрь 2016 года данное лицо вступило в сговор с другими, чтобы создать и использовать одну или несколько онлайн-ботнетов для запуска кибератак на компьютеры-жертвы (в частности, нацеленные на компьютеры, принадлежащие онлайн-игрокам или игровым платформам), чтобы захватить эти компьютеры полностью отключены или иным образом значительно ухудшают их функциональность. Эти атаки часто называют «распределенным отказом в обслуживании» или «DDoS-атаками»…

Согласно судебным документам, в сентябре и октябре 2016 года данное лицо и другие лица создали ботнет, который был вариантом так называемого ботнета «Mirai», для использования при проведении DDoS-атак. Mirai заразил устройства «Интернета вещей», такие как подключенные к Интернету видеокамеры и рекордеры, и превратил их в ботов, которые использовались для запуска DDoS-атак.

Согласно судебным документам, 21 октября 2016 года данное лицо и другие лица использовали созданный ими ботнет для запуска нескольких DDoS-атак, чтобы вывести игровую платформу Sony PlayStation Network в автономный режим на длительный период. DDoS-атаки затронули распознаватель доменных имен Dyn, Inc. из Нью-Гэмпшира, в результате чего веб-сайты, в том числе относящиеся к Sony, Twitter, Amazon, PayPal, Tumblr, Netflix и Южному Нью-Гэмпширскому университету (SNHU), стали либо полностью недоступен или доступен только с перерывами в течение нескольких часов в этот день. В результате индивидуальных DDoS-атак Dyn, Sony, SNHU и другие юридические и физические лица понесли убытки, включая потерю доходов от рекламы и затрат на исправление. По оценкам Sony, полученные в результате убытки включали примерно 2,7 миллиона долларов чистой выручки.

Это дело расследовало ФБР при содействии Национального агентства по борьбе с преступностью и полицейской службы Северной Ирландии. Дело ведет старший прокурор Мона Седки из отдела компьютерных преступлений и интеллектуальной собственности уголовного отдела и помощник прокурора США Джорджиана Макдональд из округа Нью-Гэмпшир. Бывший помощник прокурора США Арнольд Х. Хуфтален оказал существенную помощь». ***(Individual Pleads Guilty to Participating in Internet-of-Things Cyberattack in 2016 // U.S. Department of Justice (https://www.justice.gov/opa/pr/individual-pleads-guilty-participating-internet-things-cyberattack-2016). 09.12.2020).***

***

«Полиция Италии арестовала двух человек якобы за использование вредоносного ПО для кражи 10 ГБ конфиденциальных данных и военных секретов оборонной компании Leonardo SpA.

Леонардо - один из крупнейших в мире оборонных подрядчиков, 30% компании которого принадлежит Министерству экономики и финансов Италии. Как многонациональная компания, они имеют штаб-квартиру в Италии, но имеют большое присутствие в Великобритании, США и других странах.

По сообщениям итальянских СМИ, полиция арестовала одного человека по обвинению в использовании USB-ключей для заражения 94 рабочих станций трояном cftmon.exe. Вероятно, этот троян был назван в честь легитимного файла Windows, расположенного в C: \ Windows \ system32 \ ctfmon.exe, чтобы избежать обнаружения.

Сообщается, что вредоносная программа использовалась в течение двух лет, с 2015 по 2017 год, для кражи данных и их отправки обратно на сервер управления и контроля на fujinama.altervista.org.

Этот сервер C2 с тех пор был захвачен Polizia di Stato, который разместил сообщение об изъятии на веб-сайте, как показано ниже.

Извлеченные данные включали конфиденциальную бухгалтерскую информацию, военные секреты и конструкции самолетов.

"В целом, данные для 10 гигабайт, то есть около 100 000 файлов, касающихся административно-бухгалтерского управления, использования людских ресурсов, закупок и распределения капитальных товаров, а также конструкции компонентов гражданских самолетов и военных самолетов для итальянских и ", - сообщает Agi.it. - Также были захвачены учетные данные для доступа к личной информации сотрудников Leonardo Spa .

Глава кибернетической группы Леонардо также был помещен под домашний арест за то, что якобы искажал масштабы атаки и препятствовал расследованию.

Прокуратура заявляет, что системы безопасности Леонардо не обнаружили вредоносное ПО, поскольку оно было разработано сотрудником и ранее не обнаруживалось антивирусными программами.

В ответ на эту новость Леонардо выступил с заявлением, что расследование началось после подачи официальной жалобы в суд.

«Что касается текущих мер, принятых судебной системой Неаполя, Леонардо объявляет, что расследование основано на жалобе службы безопасности Компании, за которой последовали другие. Меры касаются бывшего сотрудника, который не является сотрудником Леонардо, и не -исполнительный работник Общества».

"Компания, которая, очевидно, является потерпевшей стороной в этом деле, с самого начала обеспечивала максимальное сотрудничество и будет продолжать делать это, чтобы позволить следователям прояснить инцидент, а также для собственной защиты. Наконец, следует отметить, что секретность или стратегические данные обрабатываются в отдельных областях, без связи, а не на заводе в Помильяно», - говорится в заявлении Леонардо». ***(Lawrence Abrams. Police arrest two in data theft cyberattack on Leonardo defense corp // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/police-arrest-two-in-data-theft-cyberattack-on-leonardo-defense-corp/). 05.12.2020).***

***

«Четверых китайских граждан приговорили к тюремному заключению на прошлой неделе за участие в схеме по установке малвари на телефоны, которые выпускает китайская компания Gionee.

В схеме участвовал Сюй Ли, работник Shenzhen Zhipu Technology – дочерней компании Gionee, и Чжу Ин, Цзя Чжэцзян, Пан Ци – заместитель генерального директора и инженеры-программисты фирмы Beijing Baice Technology.

Согласно документам, опубликованным властями Китая, две компании заключили секретное соглашение в конце 2018 года, чтобы создать пакет средств для разработки (SDK), который позволит контролировать проданные телефоны Gionee.

Компания Shenzhen Zhipu Technology устанавливала SDK под видом обновления приложения блокировки экрана Story Lock Screen. Однако власти Китая сообщают, что SDK вел себя как троян и делал из зараженных устройств ботов, что позволяло двум компаниям контролировать телефоны.

Как сказано в документах, между декабрем 2018 и октябрем 2019 более 20 миллионов устройств Gionee по всему миру получили более 2,88 млрд рекламных объявлений. Они принесли компаниям доход в 27,85 млн юаней ($4,26 млн).

Схема перестала работать, когда неизвестный баг стал блокировать доступ к некоторым телефонам Gionee. Это привело к тому, что техническая поддержка материнской компании начала расследование, в ходе которого они предъявили официальную жалобу китайским властям.

В ноябре 2019 года четырех подозреваемых арестовали. Согласно отчету, они не отрицали улик следствия и признали свою вину, чтобы сократить тюремный срок. Каждый из участников приговорен к сроку от 3 до 3,5 лет заключения. Также каждому выставили штраф в 200,000 юаней ($30,500).

Shenzhen Zhipu Technology была оштрафована на 400,000 китайских юаней ($61,000)». ***(Четверых приговорили к тюремному заключению за установку малвари на 20 миллионов смартфонов Gionee // SecureNews (https://securenews.ru/four-were-sentenced-to-prison-for-installing-malware-on-20-million-gionee-smartphones/). 09.12.2020).***

***

«Сиэтл - 21-летний Палмдейл, Калифорния, мужчина был приговорен к трем годам лишения свободы сегодня в окружном суде США в Сиэтле для федеральных преступлений, связанных с его компьютерной хакерской схемой и его хранение детской порнографии нашло на своих цифровых устройствах, объявил США Адвокат Брайан Т. Моран. РАЙАН С. ХЕРНАНДЕС, также известный как Райан Уэст, который использовал онлайн-прозвище «RyanRocks», в январе 2020 года признал себя виновным по двум пунктам подсчета. На слушании приговора окружной судья США Джон К. Кугенур приказал ХЕРНАНДЕСУ отбыть семь лет под надзором. освободить после тюрьмы. Он будет обязан зарегистрироваться как сексуальный преступник.

Согласно материалам дела, в 2016 году, будучи несовершеннолетним, ХЕРНАНДЕС и его партнер использовали метод фишинга для кражи учетных данных сотрудника Nintendo, которые использовались для получения доступа и загрузки конфиденциальных файлов Nintendo, связанных с его консолями и играми. Эта украденная информация, включая предварительную информацию о предполагаемой консоли Nintendo Switch, стала достоянием общественности. В октябре 2017 года после расследования взлома агенты ФБР связались с ХЕРНАНДЕСОМ и его родителями в их доме в Калифорнии. ХЕРНАНДЕС пообещал прекратить любую дальнейшую злонамеренную деятельность и подтвердил, что понимает последствия любого взлома в будущем.

Тем не менее, по крайней мере, с июня 2018 года по июнь 2019 года ХЕРНАНДЕС вернулся к своей злонамеренной деятельности, взламывая несколько серверов Nintendo и крадя конфиденциальную информацию о различных популярных видеоиграх, игровых консолях и инструментах разработчика. ХЕРНАНДЕС хвастался своими хакерскими атаками на нескольких онлайн-платформах и социальных сетях, таких как Twitter и Discord, и слил часть украденной информации другим. ХЕРНАНДЕС также руководил онлайн-форумом под названием «Подземная встреча Райана», на котором он и другие обсуждали продукты Nintendo и делились информацией о возможных уязвимостях сети Nintendo, а также на котором он делился конфиденциальной информацией, которую он украл.

В июне 2019 года агенты ФБР обыскали дом ХЕРНАНДЕЗА и изъяли многочисленные электронные устройства, включая компьютеры, жесткие диски и устройства обхода, используемые для доступа к пиратским видеоиграм и программному обеспечению. На этих устройствах они обнаружили тысячи конфиденциальных файлов Nintendo. Судебно-медицинский анализ его устройств также показал, что ХЕРНАНДЕС использовал Интернет для сбора более тысячи видео и изображений несовершеннолетних, вовлеченных в откровенно сексуальное поведение, которые хранились и отсортировывались в каталоге папок, который он назвал «Плохие вещи».

По условиям соглашения о признании вины и обвинители, и адвокаты рекомендовали три года тюрьмы. Судья Кугенур рекомендовал поместить ХЕРНАНДЕЗА в тюрьму Управления тюрем для заключенных с когнитивными проблемами. ХЕРНАНДЕС согласился выплатить Nintendo 259 323 доллара в качестве возмещения расходов на исправление, вызванных его поведением.

Дело расследовала кибер-оперативная группа ФБР в Сиэтле, а судебное преследование вел помощник прокурора США Стивен Масада». ***(California hacker who stole proprietary information from Nintendo sentenced to three years in prison // U.S. DEPARTMENT OF JUSTICE (https://www.justice.gov/usao-wdwa/pr/california-hacker-who-stole-proprietary-information-nintendo-sentenced-three-years). 01.12.2020).***

***

«21 клиент WeLeakInfo был арестован по всей Великобритании за использование украденных учетных данных, загруженных из WeLeakInfo,

после операции, координируемой Национальным агентством по борьбе с преступностью Великобритании (NCA).

Офицеры NCA изъяли биткойн на сумму более 41000 фунтов стерлингов, а также предупредили еще 60 человек из Англии, Уэльса и Северной Ирландии с о недопустимости дальнейших действий.

Их также предупредили лично, чтобы они не использовали украденные учетные данные, загруженные с WeLeakInfo, чтобы избежать ареста и судебного преследования.

«Еще 69 человек в Англии, Уэльсе и Северной Ирландии в возрасте от 16 до 40 лет посетили сотрудники Cyber Prevent, предупредив их об их потенциально преступной деятельности», - говорится в сообщении NCA.

«Программа Cyber Choices NCA и полиции Великобритании направлена на то, чтобы предотвратить непреднамеренное попадание молодых людей в киберпреступность и направить их на более позитивные пути в сфере технологий».

Были арестованы только те, кто использовал украденные учетные данные.

Девять из 21 арестованного мужчины (в возрасте от 18 до 38 лет) были задержаны по подозрению в нарушении Закона о неправомерном использовании компьютеров, девять - в мошенничестве, а в отношении троих ведется расследование.

NCA добавила, что некоторые из арестованных клиентов WeLeakInfo также купили инструменты для киберпреступлений, такие как крипторы и трояны удаленного доступа (RAT), на основании доказательств, обнаруженных во время и после арестов.

Кроме того, было обнаружено, что трое из них «хранят неприличные изображения детей или связаны с ними».

«Благодаря идентификации клиентов в Великобритании в WeLeakInfo, мы смогли найти и арестовать тех, кого мы считаем, использовали украденные персональные учетные данные для совершения новых кибер и мошенничества преступления,» Пол Creffield, от национального подразделения киберпреступности НКИ, добавил.

«NCA и правоохранительные органы Великобритании очень серьезно относятся к таким преступлениям, и они могут привести к огромным финансовым потерям для жертв».

Удаление WeLeakInfo

WeLeakInfo.com был веб-сайтом, который предоставлял подписчикам онлайн-поисковую систему, обеспечивающую доступ к личной информации, обнаруженной в результате утечки данных. Сайт продавал подписки для тех, кто хотел получить доступ, обеспечивая неограниченный поиск для просмотра и копирования украденной информации.

ФБР заблокировало сайт и конфисковало домен в январе 2020 года в сотрудничестве с Национальным полицейским управлением Великобритании, Национальным полицейским корпусом Нидерландов, Немецким Bundeskriminalamt и Полицейской службой Северной Ирландии.

Сайт использовался киберпреступниками для получения доступа к незаконно собранной информации после более чем 10 000 утечек данных и организован в базу

данных с более чем 12 миллиардами проиндексированных записей, содержащих личную информацию (например, имена, адреса электронной почты, имена пользователей, номера телефонов и учетные данные пользователей).

В рамках операции по уничтожению в Ирландии и Нидерландах также были арестованы два человека по подозрению в причастности к управлению сайтом.

Онлайн-платежи с отслеживанием IP-адресов двух лиц показали, что они, возможно, принимали активное участие в работе сайта и что они заработали 200000 фунтов стерлингов от его работы». ***(Sergiu Gatlan. UK NCA visits WeLeakInfo users to warn of using stolen data // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/uk-nca-visits-weleakinfo-users-to-warn-of-using-stolen-data/). 28.12.2020).***

***

«Сотрудники правоохранительных органов США, Германии, Франции, Швейцарии и Нидерландов нейтрализовали web-домены и серверную инфраструктуру трех VPN-сервисов, которые предоставляли киберпреступникам возможности для осуществления кибератак.

В ходе расследования выяснилось, что три домена insorg.org, safe-inet.com и safe-inet.net предлагали посетителям услуги «пуленепробиваемого хостинг-провайдера» Safe-Inet. По данным Министерства юстиции США и Европола, серверы доменов часто использовались для маскировки реальных личностей операторов вымогательского ПО, web-скиммеров (Magecart), online-фишеров и хакеров, участвующих во взломе учетных записей. Услуги предоставлялись некой организацией, описанной полицией как «пуленепробиваемый хостинг-провайдер».

Правоохранительные органы со всего мира провели скоординированную нейтрализацию серверов как минимум в пяти разных странах в дополнение к отключению доменов. В Европоле планируют проанализировать собранную информацию и возбудить дела для выявления и принятия мер против некоторых пользователей Safe-Inet.

Как заявили сотрудники Европола, в ходе расследования было выявлено около 250 компаний по всему миру, за которыми злоумышленники шпионили для осуществления потенциальных атак с использованием программ-вымогателей через инфраструктуру Safe-Inet.

«Мы знаем о сложившейся проблеме, в ближайшие дни работа сервиса будет восстановлена», — сообщается в Twitter-аккаунте Safe-Inet.

Пуленепробиваемый хостинг (bulletproof hosting) – виртуальный хостинг или выделенный сервер, владельцы которого лояльно относятся к содержимому размещенных на нем сайтов и не реагируют на обращения правообладателей и других заинтересованных сторон. В связи с этим такие серверы пользуются большой популярностью у спамеров, операторов online-казино и распространителей запрещенного контента». ***(Полиция обезвредила популярный пуленепробиваемый хостинг Safe-Inet // SecurityLab.ru (https://www.securitylab.ru/news/515064.php). 23.12.2020).***

***

«Крис Калверт из Respond Software (ныне часть FireEye) описывает проблемы, которые снижают эффективность датчиков сетевой безопасности.

У нас есть серьезная проблема с датчиками в мире кибербезопасности. И это плохо. В частности, когда речь идет о датчиках обнаружения и предотвращения вторжений в сеть (IDS / IPS). Кажется, что многие команды центров безопасности (SOC) полностью отказались от своей эффективности. Но проблема заключается в эффективности датчика или в том, как эти датчики были спроектированы, управлялись и применялись в окружающей среде?

Ответ заключается в том, что эту проблему вызывают три конкретных проблемы, в том числе:

Поставщик управляемых услуг безопасности (MSSP), который считает, что чем меньше данных, тем лучше. Почему они делают это дело? Во-первых, существует человеческое узкое место, которое естественным образом возникает, когда необходимо проанализировать большие объемы данных. Больше данных означает более высокие затраты и больше времени, необходимого для их анализа, что традиционно не сулит ничего хорошего для бизнес-модели MSSP. Более того, у людей есть верхний предел анализа потоковых данных, с которым они могут справиться, который намного ниже верхнего предела машины.

Феномен конвергентных устройств. Легче включить датчик в брандмауэр, когда это все одно конвергентное устройство, которым можно управлять вместе как единым пакетом. Однако очень часто это не лучшее место для размещения датчика. Я называю это вооружением периметра, но зоны бокового обнаружения и расшифрованные зоны наблюдения являются важными передовыми практиками, которые часто игнорируются.

И наконец, уступчивость - наш злейший враг. Сетевой мониторинг важен, но организация все равно может соответствовать требованиям, даже если он практически не работает, и мой анализ отрасли показывает, что от 70 до 85 процентов развернутых датчиков не работают для своих владельцев. Хотя соблюдение требований является важным аспектом любой программы кибербезопасности, простое соблюдение требований еще не означает создание безопасной среды.

Видимость, чувствительность и защита

При оценке сетей датчиков сети необходимо учитывать три аспекта, включая видимость, чувствительность и полезность защиты. Научное управление сеткой датчиков на основе данных позволит измерить несколько ключевых характеристик производительности, включая объем генерируемых предупреждений и общий наблюдаемый трафик (видимость), количество и разнообразие сигнатур, которые сигнализируют (чувствительность), а также не SOC распознают и не могут реагировать на реальные инциденты (защитная полезность).

Начнем с наглядности. Что вы хотите увидеть? Собственно, вопрос должен быть «кого ты хочешь видеть?» потому что серверы очень редко переходят по ссылкам без участия пользователя. Сегодня большинство атак происходит из-за

того, что пользователь нажимает на ссылку или злонамеренный инсайдер сотрудничает, особенно в случае программ-вымогателей. Это еще одна причина для развертывания боковых датчиков, которые отслеживают разведку и боковые перемещения злоумышленника в вашей сети. Это фактически подводит нас к следующей теме - чувствительности.

Чувствительность сетевого датчика напрямую зависит от количества, разнообразия и эффективности подписей, включенных на ваших устройствах. Там примерно 20 000 подписей, из них, может быть, 2 500 современные и актуальные. Однако многие компании, особенно MSSP, разрешают только 100 или меньше. Это означает, что клиенты MSSP платят за датчик, в котором 0,5 процента общей чувствительности или 4 процента предполагаемой релевантной чувствительности включены для активного мониторинга. MSSP делают это только для уменьшения объема, чтобы аналитики по безопасности человека могли управлять данными, генерируемыми этими датчиками. Эти устройства существуют для сигнализации о потенциально злонамеренных действиях, но мы, по сути, ослепили их, значительно снизив их ценность в процессе.

Еще один фактор, связанный с чувствительностью сетевого датчика, - это постоянная настройка сигнатуры. Многие команды расследуют предупреждение о подписи, определят, что это ложное срабатывание, а затем навсегда отключат подпись. Это ужасная и опасная практика, поскольку я обычно вижу, что определенные сигнатуры приводят к сложному сочетанию ложноположительного, истинно-положительного или бездействия. Единичная подпись не может быть отклонена просто потому, что она однажды ложно сработала; вам нужна контекстная и ситуационная информация в каждом случае, чтобы сделать это определение.

Далее идет защитная полезность, которая представляет собой причудливый способ сказать: «Уберем ли мы плохих парней?» Я знаю и видел огромное количество датчиков, которые ничего не обнаруживали месяцами или даже годами. Почему мы платим за решения для мониторинга и ежегодное обслуживание при таких плохих результатах?

Часто при управлении этими устройствами возникают дополнительные сложности, которые также влияют на их защитную полезность. Дело в том, что ими управляют многие ИТ-отделы, не связанные с их защитной защитой. Это затрудняет их постоянную настройку. Я встречал сотни профессионалов в области безопасности, которые отказались от своего ИТ-отдела, а не от своих датчиков.

Выберите лучший подход

Несколько проблем снижают эффективность датчиков, которые мы развертываем в наших средах, которые могут существенно повлиять на нашу позицию в области безопасности. Однако многие SOC, возможно, используют неправильный подход к размещению и конфигурации своих датчиков, существенно снижая видимость того, что происходит в окружающей среде.

Это может включать в себя настройку датчиков, обработку ложных срабатываний одинаково независимо от контекста и разрешение ограниченного числа сигнатур, которые датчики включены для обнаружения.

Чтобы решить эти проблемы, командам SOC необходимо найти решения, которые обеспечивают видимость состояния здоровья их датчиков. Это не только повысит уровень безопасности окружающей среды, но и обеспечит признание соответствующей окупаемости инвестиций в свои датчики». **(Chris Calvert. Making Sense of the Security Sensor Landscape // Threatpost (https://threatpost.com/making-sense-security-sensor-landscape/161911/). 04.12.2020).**

***

«Сегодня компания Citrix подтвердила, что продолжающаяся «модель атаки DDoS» с использованием DTLS в качестве вектора усиления влияет на сетевые устройства Citrix Application Delivery Controller (ADC) с включенным EDT.

Datagram Transport Layer Security (DTLS) - это протокол связи для защиты чувствительных к задержкам приложений и служб, использующих транспорт дейтаграмм.

DTLS основан на протоколе Transport Layer Security (TLS) и предназначен для предотвращения подслушивания и взлома, а также для защиты конфиденциальности данных.

Сообщения об атаке начали поступать 21 декабря, а клиенты сообщают о продолжающейся DDOS-атаке с усилением по протоколу UDP / 443 на устройства Citrix (NetScaler) Gateway.

Затронуто небольшое количество клиентов

«В рамках этой атаки злоумышленник или боты могут сокрушить пропускную способность сети Citrix ADC DTLS, что может привести к исчерпанию исходящей полосы пропускания», - пояснила компания в сообщении об угрозах, опубликованном ранее сегодня.

«Эффект от этой атаки, кажется, более заметен на соединениях с ограниченной пропускной способностью».

Согласно Citrix, в настоящее время масштаб атаки ограничен только «небольшим количеством клиентов», и она затрагивает все ADC с включенным протоколом Enlighted Data Transport UDP (EDT).

Кроме того, согласно имеющимся данным, в этой продолжающейся атаке нет известных уязвимостей Citrix, которые активно используются.

Если в ходе этого расследования будет обнаружена информация о продуктах, уязвимых для DDoS-атак из-за программных ошибок, она будет опубликована группой Citrix Security Response Team в отдельном сообщении по безопасности.

Обновление для удаления вектора атаки в стадии разработки

«Citrix работает над улучшением функций DTLS, чтобы исключить уязвимость к этой атаке», - добавила компания.

«Citrix ожидает, что это усовершенствование будет доступно на странице загрузок Citrix для всех поддерживаемых версий 12 января 2021 года».

Клиенты, пострадавшие от этой DDoS-атаки, могут временно смягчить ее, временно отключив DTLS, вектор усиления, используемый злоумышленниками…

«Отключение протокола DTLS может привести к ограниченному снижению производительности приложений реального времени, использующих DTLS в вашей среде», - добавил Citrix.

«Степень деградации зависит от нескольких переменных. Если ваша среда не использует DTLS, временное отключение протокола не повлияет на производительность».

Клиентам, которые не могут немедленно отключить DTLS в своей среде, рекомендуется обратиться в службу технической поддержки Citrix». ***(Sergiu Gatlan. Citrix confirms ongoing DDoS attack impacting NetScaler ADCs // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/citrix-confirms-ongoing-ddos-attack-impacting-netscaler-adcs/). 24.12.2020).***

***

«Google заявляет, что сбой глобальной системы аутентификации, который затронул большинство сериалов, ориентированных на потребителей в понедельник, был вызван ошибкой в автоматической системе управления квотами, влияющей на службу Google User ID.

Этот всемирный сбой системы не позволил пользователям войти в свои учетные записи и пройти аутентификацию во всех облачных сервисах.

В результате пользователи не могли получить доступ к Gmail, YouTube, Google Drive, Google Maps, Google Calendar и ряду других сервисов Google в течение почти часа в понедельник, 14 декабря.

Во время отключения пользователи не могли отправлять электронные письма через мобильные приложения Gmail или получать электронную почту через POP3 для настольных клиентов, в то время как посетители YouTube видели сообщения об ошибках, в которых говорилось, что «Возникла проблема с сервером (503) - нажмите, чтобы повторить».

Воздействие сбоя и основная причина

«В понедельник, 14 декабря 2020 года, с 03:46 до 04:33 (США / Тихоокеанский регион) выдача учетных данных и поиск метаданных учетных записей для всех учетных записей пользователей Google завершились неудачно», - пояснил Google. «В результате мы не смогли проверить, были ли запросы пользователей аутентифицированы и выдавали ошибки 5xx практически для всего аутентифицированного трафика.

«Большинство аутентифицированных сервисов испытали аналогичное влияние на уровень управления: повышенный уровень ошибок во всех Google Cloud Platform и API и консолях Google Workspace».

Основная причина сбоя заключалась в снижении пропускной способности центральной системы управления идентификацией Google из-за ошибки, влияющей на автоматизированную систему управления квотами.

Это приводило к проблемам с проверкой аутентификации запросов пользователей Google, что приводило к отображению ошибок при всех попытках аутентификации.

Глобальная система управления идентификацией

Служба идентификации пользователей Google, которая была причиной крупного сбоя Google с понедельника, хранит уникальные идентификаторы для всех учетных записей Google и управляет учетными данными для аутентификации как для токенов OAuth, так и для файлов cookie.

Он также хранит данные учетных записей пользователей в распределенной базе данных, которая использует протоколы Paxos для координации обновлений во время аутентификации.

Поскольку служба User ID Service отклоняет запросы при обнаружении устаревших данных по соображениям безопасности, все клиентские службы Google, требующие доступа Google OAuth, стали недоступны сразу после того, как служба начала испытывать проблемы и начала выдавать устаревшие идентификаторы.

«Google использует развивающийся набор инструментов автоматизации для управления квотами различных ресурсов, выделяемых для услуг», - говорится в опубликованном сегодня отчете компании.

"В рамках продолжающегося перехода службы User ID Service на новую систему квот в октябре было внесено изменение, чтобы зарегистрировать службу User ID с новой системой квот, но части предыдущей системы квот остались на месте, о чем было сообщено неверно использование для службы User ID как 0.

«Существующий льготный период по введению ограничений квот отсрочил воздействие, которое в конечном итоге истекло, вызвав автоматические системы квот, чтобы уменьшить квоту, разрешенную для службы User ID, и вызвать этот инцидент».

Несмотря на то, что проверки безопасности установлены для предотвращения незапланированных изменений квот, они не смогли должным образом отреагировать на сценарий с нулевой отчетной нагрузкой одной службы.

«В результате квота для базы данных учетных записей была сокращена, что помешало лидеру Paxos писать», - добавил Google. «Вскоре после этого большинство операций чтения устарело, что привело к ошибкам при поиске аутентификации».

Google заявил, что это серьезное отключение также затронуло внутренних пользователей и инструменты компании, вызвав задержки во время расследования сбоев и отчетности об обновлениях статуса.

В Gmail произошел второй сбой в течение одного дня

В Gmail произошел второй сбой в течение примерно 7 часов после устранения проблем с аутентификацией в понедельник. Отказ затронул часть пользователей Gmail, у которых возникли проблемы с доставкой электронной почты.

«Сообщение об ошибке указывало на то, что адрес электронной почты не существует, и в результате затронутые электронные письма так и не были доставлены», - говорится в отчете Google, опубликованном сегодня. «Затронутые отправители могли получить сообщение о недоставке, созданное промежуточной службой SMTP».

«В некоторых случаях полное сообщение об ошибке SMTP цитировалось в сообщении о недоставке. Поведение этих сообщений зависело от подключения внешних клиентов SMTP к службе Google SMTP».

Причиной этого второго сбоя был текущий переход на обновление базовой системы конфигурации входящей службы SMTP Gmail.

«В результате изменения конфигурации во время этой миграции изменилось поведение форматирования опции службы, так что она неверно предоставила неверное доменное имя вместо предполагаемого доменного имени gmail.com для входящей службы Google SMTP», - сказал Google.

"В результате служба неправильно преобразовала запросы определенных адресов электронной почты, заканчивающихся на" @ gmail.com ", в несуществующие адреса электронной почты.

«Когда служба учетных записей пользователей Gmail проверила каждый из этих несуществующих адресов электронной почты, служба не смогла обнаружить действительного пользователя, что привело к ошибке SMTP с кодом 550». ***(Sergiu Gatlan. Google explains the cause of the recent YouTube, Gmail outage // Bleeping Computer® (https://www.bleepingcomputer.com/news/google/google-explains-the-cause-of-the-recent-youtube-gmail-outage/). 19.12.2020).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«По следам открытия в прошлом году серии уязвимостей Ripple20 в программном обеспечении Treck, реализующем поддержку TCP/IP, группа исследователей Forescout обнаружила ещё более масштабные проблемы с безопасностью в других открытых стеках TCP/IP.

Экспертам удалось выявить в общей сложности 33 дефекта в четырёх из семи изученных ими открытых библиотек. Это ПО — uIP, FNET, picoTCP и Nut/Net — входит в состав программной прошивки разнообразного оборудования от более полутора сотен производителей, выпускавшегося на протяжении двух десятилетий.

По самым скромным оценкам, пакет уязвимостей, получивший название Amnesia:33, ставит под угрозу безопасность миллионов потребительских и промышленных устройств: смартфонов, игровых консолей, датчиков, систем-на чипе, принтеров, маршрутизаторов, ИБП и пр.

Представительный набор уязвимостей открывает перед киберпреступниками широчайшие возможности организации атак, таких как: удалённое выполнение кода (RCE) — для захвата контроля над устройством; отказ в предоставлении сервиса (DoS) — для нарушения работы бизнеса; утечка информации (infoleak) — для кражи конфиденциальных данных; отравление кэша DNS — для перенаправления веб-запросов на мошеннические сайты.

Использовавшаяся для выявления багов Amnesia:30 комбинация методов автоматизированного (фаззинг) и ручного анализа кода не нашла никаких ошибок в библиотеках lwIP, uC/TCP-IP и CycloneTCP.

Как и с Ripple20, в случае Amnesia:33 обнаружение уязвимостей было далеко не самой сложной из связанных с ними проблем. Теперь, вендорам предстоит интегрировать исправленные библиотеки в свои продукты. Для смартфонов и сетевого оборудования задача легко решается автоматической установкой обновлений (OTA), но многие другие устройства зачастую вообще не предусматривают возможности изменения прошивки и останутся уязвимыми до конца своей службы.

Более того, Forescout указывает, что не всегда можно понять — уязвимо ли конкретное устройство: у владельцев часто нет информации даже об используемых операционных системах.

Другими словами, Amnesia:33 в очередной раз демонстрирует, что экосистема интеллектуального оборудования представляет собой головную боль для обеспечения безопасности и будет оставаться таковой ещё многие годы». ***(Amnesia:33 — комплект дыр в прошивке миллионов подключенных устройств // Компьютерное Обозрение (https://ko.com.ua/amnesia_33_komplekt_dyr_v_proshivke_millionov_podklyuchennyh_ustrojstv_135588). 09.12.2020).***

***

«Исследователи Check Point Software Technologies подтвердили, что популярные приложения в Google Play Store по-прежнему подвержены известной уязвимости CVE-2020-8913 – а значит, сотни миллионов пользователей Android подвергаются значительному риску. Впервые об этой бреши сообщили в конце августа исследователи Oversecured. Используя ее, злоумышленник может внедрить вредоносный код в уязвимые приложения, предоставляя доступ ко ресурсам хост-приложения. В итоге хакер может получить доступ к конфиденциальным данным из других приложений на устройстве.

Проблема коренится в широко используемой библиотеке Play Core, которая позволяет разработчикам загружать обновления и добавлять функциональные модули в приложения для Android. Уязвимость дает возможность добавлять исполняемые модули в любые приложения, которые используют библиотеку. Если злоумышленник получает доступ к одному вредоносному приложению на устройстве жертвы, то дальше он может украсть ее личную информацию: логины, пароли, финансовые данные, письма в почте.

Разработчикам нужно как можно быстрее обновить приложения.

Google признал и исправил ошибку 6 апреля, присвоив ей 8,8 баллов опасности из 10. Однако, чтобы полностью устранить угрозу, разработчики должны были внедрить патч в свои приложения. Исследователи Check Point случайным образом выбрали несколько известных приложений, чтобы посмотреть, кто действительно внедрил исправление, предоставленное Google.

В течение сентября 13% приложений Google Play из всех проанализированных специалистами Check Point, использовали библиотеку Play

Core. При этом у 8% из них были уязвимые версии. В их числе был Viber, Booking, Cisco Teams, Moovit и пр…». ***(Из-за устаревшей версии библиотеки Play Core множество приложений уязвимы для атак // Компьютерное Обозрение (https://ko.com.ua/iz-za_ustarevshej_versii_biblioteki_play_core_mnozhestvo_prilozhenij_uyazvimy_dlya_atak_135536). 04.12.2020).***

***

«Хакер, нанятый компанией Google для работы в составе команды Project Zero, подробно описал в блоге, как ему удалось удаленно взломать смартфон iPhone через Wi-Fi без необходимости какой-либо ошибки со стороны пользователя. Все, что ему нужно было для получения несанкционированного доступа, – это находиться недалеко от устройства-жертвы. Проблема, из-за которой можно было использовать эту дыру безопасности, была исправлена компанией Apple еще в мае.

Специальный червеобразный эксплойт позволил этому хакеру получить доступ ко всем файлам, хранящимся на взломанных устройствах, включая электронную почту, заметки, изображения, данные о местоположении и т.д. При этом от пользователям взломанных устройств вообще не требовалось совершать каких-либо действий – нажимать ссылку, посещать веб-сайт или загружать вредоносную карту. Ошибка безопасности к тому же открывала доступ к камере и микрофону взломанного устройства.

По словам Яна Бира (Ian Beer), исследователя команды Project Zero, который обнаружил проблему безопасности, ошибка, по всей видимости, не была широко использована кибер-преступниками. Однако он отметил, что люди начали реагировать на новости после того, как Apple выпустила патч, который исправил эту уязвимость. Следовательно, данная проблема могла использоваться ранее. По словам хакера из Google, обычные люди не замечают такие исправления без глубокого интереса к этому коду.

Тот факт, что дыра безопасности была исправлена еще в мае, а рядовые пользователи узнают об этом в декабре, означает, что эксплойт, возможно, существовал в течение длительного времени, прежде чем Apple смогла выпустить требуемый патч и закрыть уязвимость». ***(Найден способ удаленно взломать Apple iPhone через Wi-Fi // Компьютерное Обозрение (https://ko.com.ua/najden_sposob_udalenno_vzlomat_apple_iphone_cherez_wi-fi_135556). 07.12.2020).***

***

На этой неделе OpenSSL выпустил исправления для серьезной уязвимости отказа в обслуживании (DoS), влияющей на проект с открытым исходным кодом.

Агентство по кибербезопасности и безопасности инфраструктуры DHS США (CISA) предупредило администраторов о необходимости немедленно обновить уязвимые экземпляры OpenSSL.

Вызвано нулевыми указателями при проверке имени сертификата SSL

Уязвимость с высокой степенью серьезности, отслеживаемая как CVE-2020-1971, возникает из-за проблемы разыменования нулевого указателя.

Как указано в стандарте X.509, сертификаты SSL используют тип GeneralName в разных местах для представления разных типов имен.

Объект GeneralName может быть IP-адресом, DNS-именем, идентификатором URL-адреса или даже чем-то, что называется «EDIPartyName».

При проверке сертификатов SSL X.509 OpenSSL использует GENERAL_NAME_cmpфункция для сравнения двух полей GeneralName .

Однако, если оба сравниваемых поля содержат EDIPartyName, OpenSSL может аварийно завершить работу из-за ошибки разыменования указателя NULL.

Например, OpenSSL консультативные состояния, одно место, гдеGENERAL_NAME_cmp Функция используется, когда OpenSSL проверяет поле точки распространения сертификата CRL (Certificate Revocation List).

Большинство сертификатов SSL содержат в себе так называемое поле точки распространения CRL.

В этом поле указывается место, где издатель сертификата публикует список отозванных сертификатов, который может быть проверен клиентом, например, веб-браузером.

Как показано ниже, компания Sectigo, выдающая сертификаты SSL компании BleepingComputer, указала свою точку распространения списков отзыва сертификатов как URL-адрес.

Это означает, что когда вы посещаете https://bleepingcomputer.com, ваш веб-браузер, получающий наш сертификат, в идеале должен проверять его по списку отзыва сертификатов, предоставленному по этому URL-адресу, встроенному в сертификат…

Напомним, GenericName не обязательно должен быть URL-адресом, а также может быть указан как IP-адрес или EDIPartyName.

Если злоумышленник может создать сертификат SSL, содержащий поле EDIPartyName для указания деталей CRL, и сам вредоносный CRL, GENERAL_NAME_cmp Функция при сравнении двух полей может вызвать сбой приложения и вызвать состояние отказа в обслуживании (DoS).

Но это лишь один из способов использования этой уязвимости.

Другое место, где GENERAL_NAME_cmp Эта функция используется в OpenSSL при сравнении подписавшего маркера ответа метки времени с именем органа метки времени.

CISA призывает администраторов обновиться

Как сообщил 9 ноября 2020 г. Дэвид Бенджамин из Google, эта уязвимость затрагивает все версии OpenSSL 1.0.2 и 1.1.1 (до 1.1.1i).

После анализа ошибки Мэтт Касвелл из OpenSSL в версии 1.1.1i развернул исправление.

В 2014 году критическая уязвимость OpenSSL попала в заголовки газет после массовых эксплойтов в дикой природе.

Возможно, поэтому CISA выпустила рекомендацию по безопасности для CVE-2020-1971, предлагающую администраторам серверов немедленно обновить свои экземпляры OpenSSL.

Пользователи OpenSSL 1.1.1 могут перейти на версию 1.1.1i. Поддержка продукта OpenSSL 1.0.2 и более ранних версий подошла к концу, и поэтому исправленная версия 1.0.2x предоставляется только пользователям премиум-класса. Обычные пользователи должны перейти на версию 1.1.1i.» ***(Ax Sharma. DHS-CISA urges admins to patch OpenSSL DoS vulnerability // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/dhs-cisa-urges-admins-to-patch-openssl-dos-vulnerability/). 09.12.2020).***

***

«Взаимодействие между сервером и клиентом в некоторых версиях средства сжатия файлов WinZip небезопасно и может быть изменено для обслуживания пользователей вредоносным или мошенническим контентом.

WinZip - давняя утилита для пользователей Windows, которым требуется архивирование файлов, выходящее за рамки поддержки, встроенной в операционную систему.

Первоначально выпущенный почти 30 лет назад, инструмент теперь имеет версии для macOS, Android и iOS, а также корпоративную версию, которая добавляет функции совместной работы. Согласно его веб-сайту, приложение скачали более одного миллиарда раз.

Открытый текстовый трафик

В настоящее время WinZip имеет версию 25, но более ранние выпуски проверяют сервер на наличие обновлений через незашифрованное соединение - уязвимость, которая может быть использована злоумышленником.

Мартин Рахманов из Trustwave SpiderLabs захватил трафик от уязвимой версии инструмента, чтобы показать незашифрованную связь.

По словам Рахманова, учитывая небезопасный характер канала связи, злоумышленник в той же сети, что и пользователь WinZip, может «захватить, манипулировать или перехватить трафик».

Одним из рисков, связанных с этим действием, является отравление DNS, которое заставляет приложение получать поддельное обновление с вредоносного веб-сервера.

«В результате ничего не подозревающий пользователь может запустить произвольный код, как если бы это было действительное обновление», - отмечает Рахманов в своем сегодняшнем блоге.

В зарегистрированных версиях WinZip, которые уязвимы, злоумышленник также может получить потенциально конфиденциальную информацию, такую как имя пользователя и регистрационный код.

Рахманов говорит, что общение в открытом виде также используется для отображения всплывающих окон, информирующих пользователей с бесплатной пробной версией WinZip, сколько времени у них осталось на тестирование.

Содержимое всплывающего окна - это HTML, который извлекает JavaScript. Это позволяет злоумышленнику в сети подвергать пользователей произвольному контенту, который, как представляется, поступает непосредственно с серверов WinZip.

Исследователь говорит, что этот сценарий также связан с риском выполнения произвольного кода на машине жертвы, поскольку WinZip предлагает некоторые «мощные» API для JavaScript.

С выпуском WinZip 25 обмен открытым текстом больше не происходит. Пользователям рекомендуется обновить приложение до последней версии.

Однако многие пользователи могут не спешить с получением текущей версии, потому что обновления платные. Стандартный WinZip стоит 35,64 доллара, а версия Pro - 59,44 доллара.

Если обновление программного обеспечения невозможно, пользователям рекомендуется отключить проверку обновлений. Это остановит клиента от запроса сервера WinZip о наличии новой версии». ***(Ionut Ilascu. Hackers can use WinZip insecure server connection to drop malware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hackers-can-use-winzip-insecure-server-connection-to-drop-malware/). 10.12.2020).***

***

«Cisco устранила новую уязвимость удаленного выполнения кода (RCE) критической степени серьезности, затрагивающую несколько версий Cisco Jabber для Windows, macOS и мобильных платформ, после исправления связанной с ней ошибки безопасности в сентябре.

Cisco Jabber - это настольное приложение для обмена мгновенными сообщениями и веб-конференций, созданное с использованием Chromium Embedded Framework (CEF).

Приложение доставляет сообщения между пользователями с помощью протокола расширенного обмена сообщениями и присутствия (XMPP), а также предоставляет им функции присутствия и совместного использования рабочего стола.

RCE из-за недостаточного смягчения

В сентябре Cisco выпустила обновления системы безопасности для устранения критической уязвимости системы безопасности RCE, обозначенной как CVE-2020-3495, связанной с ошибкой межсайтового скриптинга (XSS) в Cisco Jabber.

С тех пор исследователи Watchcom обнаружили новую уязвимость RCE, которую можно было бы использовать для червя, и сообщили об этом в Cisco после проверки, полностью ли устраняет уязвимость сентябрьский патч CVE-2020-3495.

«В ходе этого аудита мы обнаружили, что наиболее серьезные уязвимости, включая уязвимость RCE, не были устранены должным образом, и что пользователи остаются уязвимыми», - сообщает Watchcom.

«Теперь доступны исправления, и мы настоятельно призываем всех пользователей Cisco Jabber как можно скорее выполнить обновление!»

Всего в сентябре исследователи сообщили о четырех уязвимостях клиента Cisco Jabber, и, как они обнаружили, три из них не были в достаточной мере устранены патчами Cisco.

Это позволило им обнаружить новые уязвимости, которыми можно было злоупотреблять для эксплуатации всех поддерживаемых в настоящее время версий Cisco Jabber, от 12.1 до 12.9.

Уязвимости средней и критической степени серьезности

Как и предыдущая уязвимость, недавно обнаруженная уязвимость RCE, отслеживаемая как CVE-2020-26085, является ошибкой XSS, которая может позволить злоумышленникам удаленно выполнять произвольный код, избегая изолированной программной среды Cisco Jabber CEF.

Так же, как и CVE-2020-3495, это также вызвано неправильной проверкой ввода содержимого входящих сообщений и получило почти максимальную базовую оценку 9,9 CVSS .

«Эта уязвимость не требует взаимодействия с пользователем и может быть заражена червем, поскольку полезная нагрузка доставляется через мгновенное сообщение», - заявляет Watchcom. «Это означает, что его можно использовать для автоматического распространения вредоносных программ без какого-либо взаимодействия с пользователем».

Исследователи Watchcom также обнаружили вторую ошибку (CVE-2020-27132), уязвимость, связанную с кражей хэша пароля, раскрывающую информацию, которая может позволить злоумышленникам собирать хэши паролей NTLM от целей, использующих уязвимые версии Cisco Jabber.

Третья и последняя уязвимость (CVE-2020-27127), обнаруженная во время аудита сентябрьских патчей Cisco, вызвана ошибкой внедрения команд в обработчиках настраиваемых протоколов приложения, которые могут позволить злоумышленникам захватить браузер, встроенный в клиент Cisco Jabber цели.

Червячные уязвимости

«Поскольку некоторые уязвимости могут быть подвержены червю, организациям следует рассмотреть возможность отключения связи с внешними организациями через Cisco Jabber, пока все сотрудники не установят обновление», - предупреждает Watchcom. «Это можно сделать, отключив федерацию XMPP или настроив политику для федерации XMPP».

Это можно сделать, инициировав передачу файлов, содержащих вредоносные EXE-файлы, и вынудив жертв принять их с помощью XSS-атаки.

Это также позволяет злоумышленникам запустить вредоносный файл на целевом компьютере, не требуя вмешательства пользователя.

Ниже представлено видео о том, как злоумышленники могут использовать уязвимости Cisco Jabber, исправленные в сентябре 2020 года.

Однако, что касается недавно обнаруженных уязвимостей, «код злоумышленника будет добавлен к сообщению для обмена файлами вместо обычного сообщения», как сказал BleepingComputer Олав Сортланд Торесен из Watchcom». ***(Sergiu Gatlan. Cisco fixes new critical code execution bug in Jabber for Windows // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/cisco-fixes-new-critical-code-execution-bug-in-jabber-for-windows/). 10.12.2020).***

***

«Sophos выпустила исправление для своей линейки брандмауэров и маршрутизаторов Cyberoam, чтобы исправить уязвимость SQL-инъекции.

Sophos приобрела производителя межсетевых экранов и маршрутизаторов Cyberoam Technologies в 2014 году и с 2019 года предлагает бесплатные обновления для своей ОС XG Firewall.

Сегодня компания Sophos сообщила, что в операционной системе Cyberoam (CROS) была исправлена уязвимость SQL-инъекций, которая могла удаленно добавлять учетные записи на устройство CROS.

«Уязвимость SQL-инъекции перед аутентификацией была недавно обнаружена и исправлена на устройствах с операционной системой Cyberoam (CROS). Этот тип уязвимости может позволить выполнять операторы SQL удаленно, но только если интерфейс администрирования (служба администрирования HTTPS) был открыт на Зона WAN», - поясняется в сообщении Sophos.

Sophos сообщил BleepingComputer, что в настоящее время выясняет, воспользовались ли злоумышленники этой уязвимостью.

«Небольшое подмножество устройств Cyberoam было затронуто уязвимостью SQL-инъекции перед аутентификацией, и мы быстро развернули исправление для этих устройств. Никаких дополнительных действий не требуется. Дополнительная информация доступна на странице сообщества и в KBA».

«Мы постепенно отказываемся от устройств Cyberoam с начала 2019 года и рекомендуем пользователям обновиться до XG Firewall. Доступен простой способ обновления, который позволяет пользователям Cyberoam обновлять свое программное обеспечение бесплатно», - сказал Sophos в заявлении BleepingComputer.

Эта уязвимость не затрагивает устройства Sophos XG Firewall и SG UTM.

Sophos уже развернул исправление этой уязвимости для всех поддерживаемых версий CROS, и уязвимые устройства должны быть немедленно обновлены до последней версии. Устройства CROS, использующие «Разрешить беспроводное исправление», будут автоматически получать исправление на свои устройства…

Администраторы должны сравнить полученную информацию о версии со следующей таблицей, чтобы определить, было ли добавлено исправление. Если номер версии исправления такой же или больше, чем отображается в консоли, это означает, что исправление установлено.

Sophos также советует администраторам отключить WAN-доступ к интерфейсам веб-администратора и SSH и проверить устройства на наличие подозрительных пользователей.

Владельцы Cyberoam могут узнать, как перейти на программное обеспечение XG Firewall, используя это руководство по миграции». ***(Lawrence Abrams. Sophos fixes SQL injection vulnerability in their Cyberoam OS // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/sophos-fixes-sql-injection-vulnerability-in-their-cyberoam-os/). 10.12.2020).***

***

«Уязвимость в проприетарном программном обеспечении GE Healthcare, используемом для медицинских устройств визуализации, может поставить под угрозу конфиденциальность здоровья пациентов.

Дефект получил название MDHexRay (CVE-2020-25179) и оценку серьезности 9,8 из 10. Он затрагивает более 100 моделей аппаратов КТ, рентгеновских лучей и МРТ в десятке продуктовых линеек компании.

Пострадавшие устройства в двух десятках семейств

Программное обеспечение GE для управления с закрытым исходным кодом работает поверх операционной системы на основе Unix, установленной в медицинских системах визуализации, чтобы обеспечить удаленное обслуживание и процедуры обновления.

Уязвимость MDHexRay заключается в использовании учетных данных по умолчанию при каждой установке этого программного обеспечения для аутентификации на серверах GE для задач обновления и обслуживания. Учетные данные общедоступны.

Компания CyberMDX, занимающаяся кибербезопасностью в сфере здравоохранения, обнаружила и назвала уязвимость. Исследователи сообщили о недостатке в конце мая 2020 года и помогли GE Healthcare найти решение для смягчения последствий.

При первоначальном раскрытии GE было идентифицировано несколько семейств затронутых устройств. С тех пор было обнаружено более 100 экземпляров…

Устранение проблемы

Изменение этих данных аутентификации возможно только со стороны производителя, когда клиенты запрашивают это через систему поддержки GE Healthcare.

Неясно, сколько клиентов сделали этот запрос, если таковые были. Элад Луз, руководитель отдела исследований CyberMDX, сообщил BleepingComputer, что GE недавно начала уведомлять клиентов по электронной почте и письмом, сообщая им об угрозе безопасности.

Более быстрый и простой подход, по крайней мере теоретически, для GE - инициировать сброс учетных данных и заранее проинформировать своих клиентов. Однако это легче сказать, чем сделать.

Луз сообщил нам, что одним из решений, обсуждавшихся с GE, было изменение пароля через сеансы удаленного обслуживания, использующие безопасный протокол (надежная аутентификация и поддержка шифрования).

Исследователь говорит, что этот метод нецелесообразен, потому что для него потребуется заплатка. Учитывая большое количество уязвимых устройств, это будет сложной задачей. Кроме того, по словам Лус, даже с патчем, чтобы охватить всю клиентскую базу, потребуются годы.

В случае медицинских устройств иногда требуется локальная помощь, чтобы убедиться, что все настроено правильно, особенно правила брандмауэра.

Пока пароль не будет изменен, объекты с уязвимыми устройствами должны следовать рекомендациям по управлению сетью (политикам доступа) и

безопасности. CyberMDX рекомендует ограничить следующие порты до состояния прослушивания:

FTP (порт 21) - используется модальностью для получения исполняемых файлов с сервера обслуживания

SSH (порт 22)

Telnet (порт 23) - используется сервером обслуживания для запуска команд оболочки в модальности

REXEC (порт 512) - используется сервером обслуживания для запуска команд оболочки в модальности

Луз сказал нам, что использовать MDHexRay довольно просто. Это возможно из внутренней сети больницы или клиники и дает злоумышленнику доступ для чтения и записи к уязвимой машине обработки изображений, добавил исследователь.

Злоумышленник может получить личную информацию о здоровье. Исследователь сказал нам, что в худшем случае они также смогут манипулировать данными, тем самым влияя на результаты определенной терапии. Также существует возможность отказа в обслуживании.

Стоит отметить, что данные изображений хранятся на машине только временно, поскольку их постоянное хранилище находится в системе архивации изображений и обмена данными (PACS).

В настоящее время нет никаких свидетельств того, что MDHexRay использовался в дикой природе. BleepingComputer обратилась в GE Healthcare за заявлением, и компания подтвердила, что ей не известно ни об одном инциденте, в котором использовалась эта уязвимость…

CISA опубликовал консультативное сегодня с подробной информацией о том, как больницы и клиника с уязвимыми системами визуализации GE Healthcare могут защитить от врагов, которые могут попытаться эксплуатировать MDHexRay учетных данных по умолчанию уязвимости.

Агентство по кибербезопасности сообщает, что GE разработала решение для MDHexRay и компании «и примет упреждающие меры для обеспечения правильной настройки защиты межсетевого экрана продукта и изменения паролей по умолчанию на затронутых устройствах, где это возможно».

Для затронутых организаций рекомендуется изолировать больничную / клиническую сеть и обеспечить соблюдение строгих правил доступа на основе источника подключения, IP-адреса назначения и порта (TELNET, FTP, REXEC и SSH). Еще один совет - использовать IPSec VPN и явные правила доступа на пограничных шлюзах перед пересылкой входящих подключений в локальную сеть». ***(Ionut Ilascu. Severe MDHexRay bug affects 100+ GE Healthcare imaging systems // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/severe-mdhexray-bug-affects-100-plus-ge-healthcare-imaging-systems/). 08.12.2020).***

***

«Комитет по безопасности продуктов Kubernetes предоставил советы о том, как временно заблокировать злоумышленникам использование

уязвимости, которая может позволить им перехватывать трафик из других модулей в многопользовательских кластерах Kubernetes в атаках типа «человек посередине» (MiTM).

Kubernetes (также известный как K8s), первоначально разработанный Google и теперь поддерживаемый Cloud Native Computing Foundation, представляет собой систему с открытым исходным кодом, предназначенную для автоматизации развертывания, масштабирования и управления контейнерными рабочими нагрузками, службами и приложениями в кластерах хостов.

Он делает это путем организации контейнеров приложений в поды, узлы (физические или виртуальные машины) и кластеры, при этом несколько узлов образуют кластер, управляемый мастером, который координирует связанные с кластером задачи, такие как масштабирование, планирование или обновление приложений.

Затронутые службы не получили широкого распространения

Проблема безопасности средней степени серьезности отслеживается как CVE-2020-8554, и о ней сообщил Этьен Шампетье из Anevia.

Его могут удаленно использовать злоумышленники с базовыми разрешениями клиента (например, создавать или редактировать службы и модули) без взаимодействия с пользователем в рамках атак низкой сложности.

CVE-2020-8554 - это недостаток дизайна, который влияет на все версии Kubernetes, при этом многопользовательские кластеры, позволяющие клиентам создавать и обновлять службы и модули, являются наиболее уязвимыми для атак.

«Если потенциальный злоумышленник уже может создавать или редактировать службы и модули, то он может перехватывать трафик от других модулей (или узлов) в кластере», - пояснил Тим Олклер, инженер-программист, работающий над безопасностью Kubernetes в Apple. рекомендации по безопасности, опубликованные в понедельник.

«Если вы создаете службу с произвольным внешним IP-адресом, то трафик на этот внешний IP-адрес из кластера будет перенаправлен на эту службу», - добавил Олклер. «Это позволяет злоумышленнику, имеющему разрешение на создание службы с внешним IP-адресом, перехватывать трафик на любой целевой IP-адрес».

К счастью, уязвимость должна затронуть небольшое количество развертываний Kubernetes, учитывая, что внешние IP-службы не очень широко используются в многопользовательских кластерах, и предоставление пользователям-арендаторам разрешений службы исправлений / статуса для IP-адресов LoadBalancer не рекомендуется.

Как заблокировать эксплойты CVE-2020-8554

Поскольку команда разработчиков Kubernetes еще не предоставила обновление безопасности для решения этой проблемы, администраторам рекомендуется смягчить последствия CVE-2020-8554, ограничив доступ к уязвимым функциям.

Вы можете использовать контейнер веб-перехватчика допуска для ограничения использования внешнего IP - исходный код и инструкции по развертыванию доступны здесь.

Внешние IP-адреса также можно ограничить с помощью контроллера политики Open Policy Agent Gatekeeper для Kubernetes, используя ограничения и шаблоны, доступные здесь.

Меры по снижению рисков для IP-адресов LoadBalancer не предусмотрены, поскольку рекомендуемая конфигурация не является уязвимой, но, если требуются ограничения, рекомендации по внешним IP-адресам также применяются к IP-адресам LoadBalancer.

Чтобы обнаружить атаки, пытающиеся использовать эту уязвимость, вам необходимо вручную проверить использование внешнего IP-адреса в мультитенантных кластерах с использованием уязвимых функций.

«Услуги ExternalIP широко не используются, поэтому мы рекомендуем вручную проверять любое использование внешнего IP», - сказал Олклер. «Пользователи не должны исправлять статус службы, поэтому события аудита для запросов статуса службы исправлений, аутентифицированных для пользователя, могут быть подозрительными». ***(Sergiu Gatlan. All Kubernetes versions affected by unpatched MiTM vulnerability // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/all-kubernetes-versions-affected-by-unpatched-mitm-vulnerability/). 08.12.2020).***

***

«Уязвимость в прошивке D-link, питающей несколько маршрутизаторов с функцией сквозной передачи VPN, позволяет злоумышленникам получить полный контроль над устройством.

Ошибка затрагивает модели маршрутизаторов DSR-150, DSR-250 / N, DSR-500 и DSR-1000AC с прошивкой версии 3.17 или ниже.

Запускать команды с правами root

Группа по исследованию уязвимостей Digital Defense сообщила 11 августа, что уязвимость представляет собой инъекцию корневой команды, которую можно использовать удаленно, если веб-интерфейс устройства Unified Services Router доступен через общедоступный Интернет…

Хакеры могут использовать свой доступ для перехвата трафика, его изменения или нацеливания на другие подключенные устройства в доме.

D-Link признал проблему и опубликовал некоторые подробности в информационном сообщении ранее в этом месяце, в котором говорилось, что некоторые LUA CGI доступны без аутентификации и могут использоваться для выполнения функции библиотеки LUA для передачи данных, предоставленных пользователем.

Производитель маршрутизатора объясняет, что злоумышленник может вставить вредоносные данные в команду, предназначенную для вычисления хэша, который обрабатывается функцией «os.popen ()».

После отчета Digital Defense, в котором упоминалась только модель маршрутизатора DSR-250, D-Link оценила, что уязвимая версия прошивки использовалась для других моделей (DSR-250 / N, DSR-500 и DSR-1000AC).

Для затронутых моделей маршрутизаторов компания D-Link выпустила исправление, последняя версия прошивки, устраняющая проблему, - 3.17B401C.

Еще две ошибки, одна не исправлена

Помимо этой уязвимости, Digital Defense сообщила о двух других, ни одна из которых не была такой серьезной. Один из них также является инъекцией корневой команды, которую можно использовать через открытый веб-интерфейс «Unified Services Router», но для этого требуется аутентификация.

Третий - это аутентифицированная инъекция crontab, которая позволяет планировать выполнение произвольных команд с привилегиями root.

D-Link не признал эту ошибку, классифицируя ее как неопасную после применения патча для двух других проблем. Компания поясняет:

«Для этого поколения продуктов устройство использует конфигурацию с открытым текстом, которая предназначена для непосредственного редактирования и загрузки конфигурации на те же устройства DSR соответственно. Если D-Link устраняет проблему №1 и №2, а также другие, недавно сообщенные проблемы, злонамеренный пользователь должен будет разработать способ получения доступа к устройству для загрузки файла конфигурации, поэтому мы понимаем отчет, но классифицируем отчет как не представляющий опасности, как только исправленная прошивка станет доступной»…» ***(Ionut Ilascu. D-Link VPN routers get patch for remote command injection bugs // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/d-link-vpn-routers-get-patch-for-remote-command-injection-bugs/). 08.12.2020).***

***

«Ошибки безопасности, обнаруженные в облачном игровом приложении для Windows PlayStation Now (PS Now), позволяли злоумышленникам выполнять произвольный код на устройствах Windows с уязвимыми версиями приложений.

PlayStation Now достигла более 2,2 миллиона подписчиков [PDF] в конце апреля 2020 года с момента запуска сервиса в 2014 году.

Уязвимости, обнаруженные охотником за наградами Парсией Хакимиан, затронули PS Now версии 11.0.2 и более ранних версий на компьютерах под управлением Windows 7 SP1 или более поздних версий.

Хакимиан сообщил об ошибке PS Now 13 мая 2020 года через официальную программу вознаграждения за ошибки PlayStation на HackerOne. PlayStation устранила ошибку и пометила отчет об ошибке как «Решенный» месяц спустя, 25 июня 2020 года.

Он был награжден наградой за свой отчет в размере 15000 долларов, даже несмотря на то, что его представление не входило в сферу охвата - то есть оно затрагивало приложение Windows, а не один из целевых активов, включенных в программу вознаграждения за ошибки (системы PlayStation 4 и PlayStation 5, операционные системы, аксессуары или PlayStation Network.)

Небезопасное приложение Electron подвергает пользователей атакам RCE

Хакимиан обнаружил, что в цепочке критические проблемы безопасности позволяют злоумышленникам, не прошедшим проверку подлинности, запускать атаки удаленного выполнения кода (RCE), злоупотребляя уязвимостью внедрения кода.

«Любой веб-сайт, загруженный в любом браузере на той же машине, может запускать произвольный код на машине через уязвимое соединение через веб-сокет», - сказал Хакимиан.

Злоумышленники могут запустить вредоносный код на компьютере пользователя PS NOW через локальный сервер WebSocket, запущенный psnowlauncher.exe на порту 1235, с помощью приложения AGL Electron, которое оно запускает после запуска.

«JavaScript, загруженный AGL, сможет запускать процессы на машине», - пояснил исследователь. «Это может привести к выполнению произвольного кода. Приложение AGL не проверяет, какие URL-адреса загружаются».

Это возможно, потому что сервер websocket, запущенный на целевом устройстве, не выполняет никаких проверок заголовка Origin или проверки происхождения запроса.

Чтобы успешно воспользоваться ошибкой RCE, злоумышленники должны убедить пользователя PS NOW, чье устройство они хотят взломать, открыть специально созданный сайт, используя вредоносную ссылку, предоставленную через фишинговые письма, форумы, каналы Discord и т. Д.

После открытия его в любом веб-браузере на своем компьютере вредоносные сценарии на веб-сайте подключатся к локальному серверу WebSocket и попросят AGL загрузить вредоносный код узла с другого сайта и запустить его на целевом устройстве.

Программы поощрения ошибок Sony

Sony объявила о запуске своей публичной программы вознаграждений за обнаружение ошибок HackerOne PlayStation в июне 2020 года, программы, которая платит исследователям безопасности и игрокам за сообщение о проблемах безопасности, обнаруженных в системах PlayStation 4 и 5, операционных системах, аксессуарах и сети PlayStation Network.

Квалифицированные сообщения об ошибках PlayStation имеют право на вознаграждение в размере от 100 долларов за уязвимость PlayStation Network низкой степени серьезности до 50 000 долларов за критическую ошибку PlayStation 4.

Эта программа поощрения ошибок уже работала в частном порядке с некоторыми исследователями безопасности, когда она была запущена в июне, что объясняет представления Хакимиана за месяц до запуска программы.

С октября 2017 года компания также запускает отдельную Программу раскрытия уязвимостей на HackerOne, которая позволяет охотникам за ошибками сообщать о соответствующих уязвимостях безопасности в продуктах Sony или на веб-сайтах, на которые не распространяется программа PlayStation.

PlayStation Now - не единственный облачный сервис потоковой передачи игр, который в этом году исправил критическую проблему безопасности.

NVIDIA также выпустила обновление для системы безопасности, устраняющее уязвимость в приложении Windows для облачных игр GeForce Now, которая позволяла злоумышленникам выполнять произвольный код или повышать привилегии в системах, на которых запущено неустановленное программное обеспечение». ***(Sergiu Gatlan. PlayStation Now bugs let sites run malicious code on***

Windows PCs // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/playstation-now-bugs-let-sites-run-malicious-code-on-windows-pcs/). 07.12.2020).

***

«Cisco выпустила обновления безопасности для устранения нескольких уязвимостей предварительной аутентификации с помощью общедоступных эксплойтов, влияющих на Cisco Security Manager, которые могут позволить удаленное выполнение кода после успешной эксплуатации.

Cisco Security Manager помогает управлять политиками безопасности на большом количестве устройств безопасности и сетевых устройств Cisco, а также предоставляет сводные отчеты и возможности устранения неполадок в событиях безопасности.

Этот продукт работает с широким спектром устройств безопасности Cisco, включая, помимо прочего, устройства Cisco ASA, коммутаторы Cisco Catalyst серии 6000, маршрутизаторы с интегрированными сервисами (ISR) и модули служб межсетевого экрана.

Эксплойты Proof-of-Concept доступны с ноября

«Группе реагирования на инциденты, связанные с безопасностью продуктов Cisco (PSIRT), известно о публичных объявлениях об этих уязвимостях», - говорится в сообщении.

Эти уязвимости влияют на Cisco Security Manager версий 4.22 и более ранних, и они были обнаружены Cisco 16 ноября после того, как в августе о них сообщил исследователь безопасности Code White Флориан Хаузер.

Хаузер поделился экспериментальными эксплойтами для всех 12 уязвимостей Cisco Security Manager, о которых он сообщил после того, как Cisco PSIRT перестала отвечать.

К счастью, на данный момент Cisco заявляет, что им неизвестно о каких-либо продолжающихся атаках, использующих исправленные сегодня уязвимости.

«Cisco PSIRT не знает о злонамеренном использовании уязвимостей, описанных в этом информационном сообщении», - добавляет Cisco.

Доступны обновления безопасности

Cisco устранила две из 12 уязвимостей (CVE-2020-27125 и CVE-2020-27130), но не предоставила никаких обновлений безопасности для исправления нескольких ошибок безопасности, которые в совокупности отслеживаются как CVE-2020-27131.

Уязвимости были обнаружены Хаузером в функции десериализации Java в Cisco Security Manager и вызваны «небезопасной десериализацией предоставленного пользователем контента уязвимым программным обеспечением».

После успешной эксплуатации они могут позволить злоумышленникам, не прошедшим проверку подлинности, удаленно выполнять произвольные команды на уязвимых устройствах.

«Злоумышленник может воспользоваться этими уязвимостями, отправив вредоносный сериализованный объект Java определенному слушателю в уязвимой системе», - объясняет Cisco.

«Успешный эксплойт может позволить злоумышленнику выполнять произвольные команды на устройстве с привилегиями NT AUTHORITY \ SYSTEM на целевом хосте Windows».

Cisco устранила эти уязвимости в Cisco Security Manager Release 4.22 Service Pack 1.

Администраторы должны немедленно развернуть обновление безопасности как можно скорее, учитывая, что нет обходных путей, которые устраняют эти ошибки безопасности.

В ноябре Cisco также раскрыла ошибку нулевого дня AnyConnect VPN с общедоступными эксплойтами, влияющими на программное обеспечение с нестандартными конфигурациями». ***(Sergiu Gatlan. Cisco fixes Security Manager vulnerabilities with public exploits // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/cisco-fixes-security-manager-vulnerabilities-with-public-exploits/). 07.12.2020).***

***

«Агентство национальной безопасности (АНБ) предупреждает, что спонсируемые государством российские злоумышленники используют недавно исправленную уязвимость VMware для кражи конфиденциальной информации после развертывания веб-шеллов на уязвимых серверах.

«АНБ призывает администраторов сети Национальной системы безопасности (NSS), Министерства обороны (DoD) и оборонной промышленной базы (DIB) уделять приоритетное внимание устранению уязвимости на уязвимых серверах», - заявили в разведывательном агентстве Министерства обороны США.

На просьбу предоставить дополнительную информацию о целях, скомпрометированных в этих атаках, АНБ заявило BleepingComputer, что «не раскрывает публично подробности о жертвах злонамеренной киберактивности из-за рубежа».

«Любая организация, использующая затронутые продукты, должна незамедлительно применить исправление, выпущенное поставщиком», - настаивает АНБ.

АНБ также воздержалось от предоставления дополнительной информации о дате начала этих атак, заявив, что «[мы] не предоставляем конкретных сведений об источнике какой-либо конкретной информации, чтобы мы могли продолжать выполнять нашу жизненно важную роль для страны, включая развитие и обмен техническими рекомендациями, подобными этому отчету ".

Доступны обновления безопасности и обходные пути

VMware выпустила обновления безопасности для устранения ошибки безопасности 3 декабря после публичного раскрытия уязвимости две недели назад и предоставления временного обходного пути, который полностью удаляет вектор атаки и предотвращает эксплуатацию.

CVE-2020-4006 изначально была оценена как уязвимость с критической степенью серьезности, но VMware снизила ее максимальную степень серьезности до «Важно» после выпуска исправления и совместного использования этой уязвимости, требующей «действительного пароля для учетной записи администратора конфигуратора».

«Эта учетная запись является внутренней для затронутых продуктов, и пароль устанавливается во время развертывания. Злоумышленник должен обладать этим паролем, чтобы попытаться использовать CVE-2020-4006», - поясняет VMware.

Полный список версий продуктов VMware, на которые распространяется действие нулевого дня, включает:

VMware Workspace One Access 20.01, 20.10 (Linux)

VMware Identity Manager (vIDM) от 3.3.1 до 3.3.3 (Linux)

Коннектор VMware Identity Manager (коннектор vIDM) 3.3.1, 3.3.2 (Linux)

Коннектор VMware Identity Manager (коннектор vIDM) 3.3.1, 3.3.2, 3.3.3 / 19.03.0.0, 19.03.0.1 (Windows)

VMware Cloud Foundation 6 4.x

VMware vRealize Suite Lifecycle Manager 7 8.x

Администраторы, которые не могут немедленно развернуть исправление, могут использовать временный обходной путь для предотвращения эксплуатации CVE-2020-4006…

«Этот обходной путь должен быть временным, пока не удастся полностью исправить систему», - заявили в АНБ. «Кроме того, проверьте и укрепите конфигурации и мониторинг поставщиков федеративной аутентификации».

Эксплуатация позволяет развертывать веб-оболочку и кражу данных

В атаках с использованием CVE-2020-4006 АНБ наблюдало, как злоумышленники подключались к открытому веб-интерфейсу управления устройствами, на которых запущены уязвимые продукты VMware, и проникали в сети организаций для установки веб-шеллов с помощью внедрения команд.

После развертывания веб-оболочек злоумышленники крадут конфиденциальные данные, используя учетные данные SAML, чтобы получить доступ к серверам Microsoft Active Directory Federation Services (ADFS).

Успешное использование уязвимости, обозначенной как CVE-2020-4006, также позволяет злоумышленникам выполнять команды Linux на скомпрометированных устройствах, что может помочь им добиться устойчивости.

«При использовании продуктов, выполняющих аутентификацию, критически важно, чтобы сервер и все сервисы, которые от него зависели, были правильно настроены для безопасной работы и интеграции», - поясняет АНБ.

«В противном случае утверждения SAML могут быть сфальсифицированы, предоставляя доступ к многочисленным ресурсам. При интеграции серверов аутентификации с ADFS, NSA рекомендует следовать передовым методам Microsoft, особенно для защиты утверждений SAML и требования многофакторной аутентификации».

Обнаружить эти атаки с помощью сетевых индикаторов невозможно, поскольку вредоносная деятельность осуществляется после подключения к веб-интерфейсу управления через зашифрованные туннели TLS.

Однако операторы «exit», за которыми следуют трехзначные числа, такие как «exit 123», найденные в /opt/vmware/horizon/workspace/logs/configurator.log на серверах, указывают на то, что на устройстве могли иметь место действия по эксплуатации.

«Могут присутствовать и другие команды вместе с закодированными сценариями. Если такие журналы обнаружены, следует выполнить действия по реагированию на инциденты», - добавило АНБ. «Рекомендуется дополнительное исследование сервера, особенно на предмет вредоносных программ веб-оболочки».

Снижение риска успешных атак

Риск безопасности этой уязвимости снижается за счет того, что этот пароль должен быть установлен во время развертывания - выбор уникального и надежного пароля настоятельно рекомендуется

Ограничение доступа к веб-интерфейсу управления для затронутых продуктов дополнительно снижает риск успешной атаки.

Агентство рекомендует в сообщении [PDF], что «сетевые администраторы NSS, DoD и DIB ограничивают доступность интерфейса управления на серверах только небольшим набором известных систем и блокируют прямой доступ в Интернет».

При подозрении на компрометацию АНБ рекомендует проверять журналы сервера на наличие признаков эксплуатации, проверять и обновлять конфигурации служб аутентификации и внедрять многофакторную аутентификацию для служб учетных данных безопасности.

Не указывая пальцами

АНБ не назвало поддерживаемую Россией группу APT, которая использует уязвимость внедрения команд VMware в текущих атаках.

Однако, по крайней мере, одна такая хакерская группа в течение последних нескольких месяцев активно атакует сети государственных, местных, территориальных и племенных (SLTT) государственных организаций США.

ФБР и DHS-CISA заявили в совместном сообщении, опубликованном в октябре, что спонсируемая государством российская хакерская группа Energetic Bear взломала и похитила данные из правительственных сетей США, начиная с сентября 2020 года.

DHS-CISA предоставляет более подробную информацию об исторической злонамеренной кибер-активности в России, нацеленной на организации США (отслеживается как GRIZZLY STEPPE)». ***(Sergiu Gatlan. NSA: Russian state hackers exploit new VMware vulnerability to steal data // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/nsa-russian-state-hackers-exploit-new-vmware-vulnerability-to-steal-data/). 07.12.2020).***

***

«Компания QNAP, производитель сетевых хранилищ (NAS), сегодня выпустила обновления безопасности для устранения уязвимостей, которые

могут позволить злоумышленникам получить контроль над незащищенными устройствами NAS после успешного использования.

Восемь уязвимостей, исправленных сегодня QNAP, затрагивают все устройства QNAP NAS, на которых работает уязвимое программное обеспечение.

Эти ошибки безопасности, связанные с внедрением команд и межсайтовым скриптингом (XSS), оцениваются компанией как проблемы безопасности средней и высокой степени серьезности.

Уязвимости XSS могут позволить удаленным злоумышленникам внедрить вредоносный код в уязвимые версии приложений.

Использование ошибок внедрения команд позволяет им повышать привилегии, выполнять произвольные команды на скомпрометированном устройстве или приложении и управлять базовой операционной системой.

Внедрение команд ОС и межсайтовый скриптинг

Список программного обеспечения, к которому применяются некоторые из сегодняшних обновлений безопасности, включает высокопроизводительную операционную систему QNAP QuTS hero на основе ZFS и ОС QTS NAS.

QNAP исправил ошибки XSS CVE-2020-2495, CVE-2020-2496, CVE-2020-2497 и CVE-2020-2498, а также ошибку внедрения команды CVE-2019-7198 в этих версиях QTS и QuTS…

Производитель NAS настоятельно рекомендует клиентам обновить свои системы до последней версии, чтобы предотвратить будущие атаки на их устройства…

Хотя устройства NAS обычно не используются в качестве контроллеров домена Windows, некоторые организации могут включать эту функцию для управления учетными записями пользователей, аутентификации и обеспечения безопасности домена». ***(Sergiu Gatlan. QNAP patches QTS vulnerabilities allowing NAS device takeover // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/qnap-patches-qts-vulnerabilities-allowing-nas-device-takeover/). 07.12.2020).***

***

«Это лишь один из симптомов: у 83% из 30 крупнейших розничных продавцов США есть уязвимости, которые представляют «неминуемую» киберугрозу, включая Amazon, Costco, Kroger и Walmart.

2020 год обещает стать знаменательным годом для уязвимостей программного обеспечения, оставив профессионалов в области безопасности тонуть в настоящем море исправлений, отчетов и надвигающихся атак, многие из которых они даже не видят.

Три последних отчета об отслеживании уязвимостей программного обеспечения за последний год подчеркивают проблемы управления исправлениями и предотвращения атак.

«Судя по данным об уязвимостях, состояние безопасности программного обеспечения остается довольно плачевным, - сказал Threatpost Брайан Мартин, вице-президент по анализу уязвимостей компании Risk Based Security (RBS).

Год начался не так. Команда VulnDB в RBS заметила резкое сокращение раскрытия информации в течение первых трех кварталов 2020 года. Затем ударил COVID-19, создав прекрасную возможность для злоумышленников использовать хаос.

«В конце первого квартала этого года мы увидели резкое сокращение числа раскрываемых уязвимостей по сравнению с 2019 годом - на 19,2 процента», - написал Мартин в отчете за третий квартал. «По статистике, это огромно. Однако по мере продолжения 2020 года мы начинаем видеть, насколько большое влияние пандемия оказала на раскрытие информации об уязвимостях ».

Программное обеспечение Vuln Perfect Storm

Теперь RBS сообщил, что количество раскрытых уязвимостей, возможно, превысит показатели 2019 года, но по мере того, как год подходит к концу, все еще существует большая неопределенность в отношении воздействия COVID на 2021 год.

«Поскольку пандемия возобновляется в большей части мира, даже когда мы вступаем в сезон отпусков, трудно предсказать точное влияние COVID-19 на ситуацию раскрытия уязвимостей», - заключил отчет RBS.

До пандемии ИТ-команды уже находились под огромным давлением, чтобы не отставать от исправлений из-за того, что RBS окрестило «событиями уязвимости Фудзивары». Термин «Фудзивара», согласно исследователям RBS, описывает слияние двух ураганов, которые они сравнивают с такими днями, как 14 января, 14 апреля и 14 июля этого года, когда 13 основных поставщиков, включая Microsoft и Oracle, выпустили исправления для в то же время. RBS заявило, что эти три события, связанные с уязвимостью Fujiwara в 2020 году, создают серьезную нагрузку на службы безопасности.

Между тем, регулярные мероприятия, проводимые некоторыми крупными поставщиками по вторникам патчей, начинают создавать своего рода повторяющийся эффект Фудзивара уязвимости круглый год, добавил RBS, поскольку количество патчей для каждого из них увеличилось. Например, с декабрьским вторником патчей Microsoft насчитывает 1250 патчей за год - намного больше, чем 840 в 2019 году.

Фактически, согласно последнему анализу Comparitech, Microsoft и Oracle возглавляют 50 ведущих поставщиков по количеству обнаруженных уязвимостей безопасности.

Исследователи безопасности изучили детали CVE у 50 ведущих поставщиков программного обеспечения и обнаружили, что с 1999 года безоговорочным лидером является Microsoft с 6700 отчетами, за ней следует Oracle с 5500 и IBM с 4600.

«Новое программное обеспечение выпускается более быстрыми темпами, чем устаревшее программное обеспечение или прекращение его поддержки», - сказал Threatpost из Comparitech Пол Бишофф. «Учитывая это, я думаю, что новые уязвимости программного обеспечения неизбежны. Большинство этих уязвимостей выявляются и исправляются еще до того, как они когда-либо эксплуатируются в дикой природе, но неизбежны и другие нулевые дни. Нулевые дни - гораздо большее беспокойство, чем уязвимости в целом».

Уязвимости программного обеспечения в Интернете и для настольных компьютеров

По словам Cyberpion, реальный рост недостатков безопасности программного обеспечения пришелся на стороннее онлайн-программное обеспечение, которое разработало инструмент для оценки дыр в безопасности во всех онлайн-экосистемах. Их выводы включают поразительную статистику, согласно которой 83 процента из 30 крупнейших розничных продавцов США имеют уязвимости, которые создают «неминуемую» киберугрозу, включая Amazon, Costco, Kroger и Walmart.

«Программное обеспечение, разработанное для настольных компьютеров, в корне отличается от программного обеспечения, разработанного для онлайн-приложений, - сказал Threatpost технический директор Cyberpion Ран Нахмиас. «Программный код настольного компьютера должен быть защищен от вируса, который переписывает код (а атака происходит на одном компьютере за раз). Онлайн-программное обеспечение сильно зависит от инфраструктуры, в которой оно размещается, управляется и распространяется.

Это создает массивную поверхность атаки, включая не только сам код, но и стоящую за ним инфраструктуру.

«Эти онлайн-инфраструктуры могут стать сложными, и одна неправильная конфигурация в любом месте может привести к взлому или изменению кода», - сказал Нахмиас. «Кроме того, поскольку программное обеспечение централизованно расположено и обслуживает множество клиентов, одно нарушение может затронуть многие компании и людей (в отличие от программного обеспечения для настольных компьютеров, зараженного вирусом, который затронет одного пользователя)».

Что действительно нужно организациям для надлежащей защиты своих систем, так это хорошо обученные профессионалы. К сожалению, как добавил Бишофф, их становится все меньше.

«Помимо растущего объема программного обеспечения, отсутствие квалифицированного персонала по кибербезопасности способствует увеличению уязвимостей программного обеспечения», - сказал он. «Практически в каждом секторе экономики персонал, занимающийся кибербезопасностью, пользуется большим спросом».

Между тем программные ошибки никуда не денутся.

«Несмотря на то, что все больше организаций относятся к безопасной разработке более серьезно, и несмотря на то, что доступно больше инструментов, помогающих находить и устранять уязвимости, количество обнаруженных уязвимостей говорит о том, что они еще не перевернулись», - добавил Мартин. «Мы надеемся, что по мере того, как все больше и больше новостей о взломанных организациях воспринимается всерьез, а организации и разработчики лучше понимают серьезность уязвимого кода, они приложат дополнительные усилия для обеспечения большего количества проверок перед выпуском [программного обеспечения].» ***(Becky Bracken. Record Levels of Software Bugs Plague Short-Staffed IT Teams in 2020 // Threatpost (https://threatpost.com/record-levels-software-bugs-it-teams-2020/162095/). 09.12.2020).***

***

«VMware выпустила полный патч и изменила уровень серьезности уязвимости, о которой сообщило АНБ, на «важный».

VMware исправила ошибку нулевого дня, которая была обнаружена в конце ноября, - недостаток повышения привилегий, который влияет на Workspace One и другие платформы как для операционных систем Windows, так и для Linux.

VMware также изменила рейтинг серьезности ошибки CVSS с критического на «важный».

Агентство по кибербезопасности и безопасности инфраструктуры США (CISA) изначально отметило незащищенную уязвимость безопасности 23 ноября, которая затрагивает 12 версий VMware в его портфелях Cloud Foundation, Identity Manager, vRealize Suite Lifecycle Manager и Workspace One. Об этом компании сообщили в Агентстве национальной безопасности (АНБ).

В соответствии с рекомендациями компании, ошибка, отслеживаемая как CVE-2020-4006, допускает внедрение команд.

«Злоумышленник с сетевым доступом к административному конфигуратору через порт 8443 и действующим паролем для учетной записи администратора конфигуратора может выполнять команды с неограниченными привилегиями в базовой операционной системе», - написала VMware в обновленном информационном сообщении в четверг.

Первоначально ошибка была оценена в 9,1 из 10 по шкале серьезности CVSS, но дальнейшее расследование показало, что любому злоумышленнику потребуется пароль, указанный в обновлении, что значительно затрудняет эффективное использование. Его рейтинг сейчас 7,2, что делает его «важным», а не «критическим».

«Эта учетная запись является внутренней для затронутых продуктов, и пароль устанавливается во время развертывания», - говорится в сообщении. «Злоумышленник должен обладать этим паролем, чтобы попытаться использовать CVE-2020-4006».

Он добавил, что пароль необходимо будет получить с помощью таких приемов, как фишинг или брутфорс / заполнение учетных данных.

Когда в ноябре была обнаружена уязвимость, компания выпустила обходные пути «временного решения для предотвращения эксплуатации CVE-2020-4006», с учетом того, что изменения настроек, управляемые конфигуратором, возможны, пока существует обходной путь. Однако теперь доступен полный патч.

Уязвимость затронула следующие продукты:

VMware Workspace One Access (Доступ)

Коннектор доступа к VMware Workspace One (коннектор доступа)

VMware Identity Manager (vIDM)

Коннектор VMware Identity Manager (коннектор vIDM)

VMware Cloud Foundation

vRealize Suite Lifecycle Manager

Затронутые версии:

VMware Workspace One Access 20.01, 20.10 (Linux)

VMware Identity Manager 3.3.3, 3.3.2, 3.3.1 (Linux)
Коннектор VMware Identity Manager 3.3.2, 3.3.1 (Linux)
Коннектор VMware Identity Manager 3.3.3, 3.3.2, 3.3.1 (Windows)
VMware Cloud Foundation 4.x (Linux и Windows)
vRealize Suite Lifecycle Manager 8.x (Linux и Windows)

Сообщений об эксплуатации в дикой природе не поступало». ***(Tara Seals. VMware Rolls a Fix for Formerly Critical Zero-Day Bug // Threatpost (https://threatpost.com/vmware-fix-critical-zero-day-bug/161896/). 04.12.2020).***

***

«CISA предупреждает, что ведущая платформа управления корпоративной документацией открыта для атак, и призывает компании применять исправления.

Xerox выпустила исправление для двух уязвимостей, влияющих на лидирующую на рынке платформу управления корпоративными документами DocuShare. В случае использования этих ошибок пользователи DocuShare могут подвергнуться атаке, которая приведет к потере конфиденциальных данных.

В среду Агентство по кибербезопасности и безопасности инфраструктуры (CISA) выпустило бюллетень по безопасности, призывающий пользователей и администраторов применить патч, закрывающий две дыры в безопасности в недавно выпущенных версиях (6.6.1, 7.0 и 7.5) DocuShare от Xerox. Уязвимость оценена как важная.

Xerox заявила, что уязвимости, обозначенные как CVE-2020-27177, открывают для пользователей Solaris, Linux и Windows DucuShare как атаку подделки запросов на стороне сервера (SSRF), так и атаку с внедрением неаутентифицированного внешнего XML-объекта (XXE). 30 ноября Xerox выпустила уведомление по безопасности (XRX20W). Компания

Xerox не сообщила подробностей об ошибках или возможных сценариях атак. В своем «Мини-бюллетене» он предлагает ссылки на ссылки на исправления к файлам tarball, устраняющие ошибки в уязвимых версиях Solaris, Linux и Windows DocuShare.

Однако исправление для версии DocuShare 7.5 для Solaris недоступно. Xerox не ответила на запросы прессы перед публикацией этой новостной статьи.

Возможные векторы угроз

Уязвимость SSRF позволяет злоумышленнику злоупотреблять функциональностью на сервере, на котором размещается программное обеспечение как услуга (SaaS) DocuShare. Успешная атака SSRF обычно позволяет злоумышленнику читать или обновлять внутренние ресурсы.

«Злоумышленник может предоставить или изменить URL-адрес, по которому код, запущенный на сервере, будет читать или отправлять данные, и, тщательно выбирая URL-адреса, злоумышленник может иметь возможность читать конфигурацию сервера, такую как метаданные AWS, подключаться к внутренним службам, таким как http включены базы данных или выполнять почтовые запросы к внутренним службам, которые не предназначены для раскрытия», - говорится в описании атаки SSRF в OWASP Foundation.

XXE - это тип атаки на приложение, которое анализирует ввод XML. «Эта атака происходит, когда ввод XML, содержащий ссылку на внешний объект, обрабатывается плохо настроенным анализатором XML», - описывает OWASP.

Успешная атака XXE позволит киберпреступникам получить доступ к конфиденциальным данным, а также может облегчить атаки, которые включают: «отказ в обслуживании, подделку запросов на стороне сервера и сканирование портов с точки зрения машины, на которой расположен анализатор», согласно OWASP.

Охотнику за ошибками Жюльену Аренсу (@MrTuxracer) приписывают то, что он обнаружил ошибку и обратил на нее внимание Xerox…». ***(Tom Spring. Xerox DocuShare Bugs Allow Data Leaks // Threatpost (https://threatpost.com/xerox-docushare-bugs/161791/). 02.12.2020).***

***

«Согласно отчету аналитиков Juniper Threat Labs, основанном на данных Shodan, почти 3000 серверов Oracle WebLogic доступны через интернет и по-прежнему позволяют неаутентифицированным злоумышленникам удаленно выполнять произвольный код. Дело в том, что все они по-прежнему уязвимы перед RCE-багом CVE-2020-14882, который был исправлен два месяца назад.

Хакеры, разумеется, не могли оставить такую возможность без внимания и атакуют серверы WebLogic, используя как минимум пять различных пейлоадов. Но эксперты Juniper Threat Labs пишут, что наибольший интерес в данном случае представляет малварь DarkIRC, «которая в настоящее время продается на хак-форумах за 75 долларов».

Злоумышленник, занимающийся распространением DarkIRC, носит псевдоним Freak_OG и начал его рекламировать свою малварь в августе 2020 года. Исследователи не сообщают, этот ли злоумышленник стоит за продолжающимися атаками DarkICE, хотя имя файла в одном из недавно обнаруженных пейлодов крайне похоже на имя файла в FUD (Fully Undetected) Crypter, который тоже недавно рекламировался Freak_OG.

«Мы не уверены, что оператор, атаковавший нашу приманку, — это тот же человек, который рекламирует эту вредоносную программу на Hack Forum, или один из его клиентов», — говорят исследователи.

Аналитики рассказывают, что DarkIRC проникает на непропатченные серверы с помощью PowerShell-скрипта, выполняемого через HTTP-запрос GET в форме вредоносного бинрника, который имеет как функции обхода анализа, так и работы в песочнице. Так, перед распаковкой малварь проверяет, работает ли она на виртуальной машине VMware, VirtualBox, VBox, QEMU или Xen, и останавливает процесс заражения, если обнаруживает среду песочницы.

После распаковки бот DarkIRC установится в %APPDATA% \Chrome\Chrome.exe и закрепится на взломанном устройстве, прописавшись в автозапуск.

Эксперты отмечают, что DarkIRC обладает множеством функций, включая кейлоггинг, хищение файлов и выполнение команд на зараженном сервере, кражу

учетных данных, распространение на другие устройства через MSSQL и RDP (посредством брутфорса), SMB или USB, а также организацию DDoS-атак.

Злоумышленники даже могут использовать бота в качестве биткоин-клиппера, который позволяет в реальном времени подменять адреса биткоин-кошельков в буфер обмена на адреса, контролируемые хакерам». ***(Мария Нефёдова. Критический баг в Oracle WebLogic активно используется малварью DarkIRC // Xakep (https://xakep.ru/2020/12/02/weblogic-darkirc/). 02.12.2020).***

***

«Специалисты по кибербезопасности из Positive Technologies сообщили, что в протоколах 5G есть уязвимости, позволяющие атаковать смартфоны.

По словам экспертов, стеки 5G-протоколов HTTP/2 и PFCP потенциально предоставляют злоумышленникам возможность проводить атаки на абонентов и сети оператора.

Также отмечается, что соответствующие атаки злоумышленники смогут проводить из партнёрских сетей, предоставляющих доступ к услугам, или даже в роуминге.

Речь идет об атаках типа «отказ в обслуживании» для пользователей. Они позволят злоумышленникам полностью отключить сеть на устройстве или перехватить трафик». ***(В сетях 5G есть уязвимости, позволяющие атаковать смартфоны // iLenta.com (https://ilenta.com/news/internet/news_31199.html). 20.12.2020).***

***

«Компания Hewlett Packard Enterprise (HPE) обнаружила ошибку нулевого дня в последних версиях своего проприетарного программного обеспечения HPE Systems Insight Manager (SIM) для Windows и Linux.

Хотя обновления безопасности для этой уязвимости удаленного выполнения кода (RCE) пока недоступны, HPE предоставила сведения о смягчении последствий для Windows и работает над устранением уязвимости нулевого дня.

Zero-days - это публично раскрытые уязвимости, которые еще не исправлены поставщиком, которые в некоторых случаях также активно используются в дикой природе или имеют общедоступные экспериментальные эксплойты.

HPE SIM - это решение для автоматизации управления и удаленной поддержки для нескольких серверов, систем хранения и сетевых продуктов HPE, включая, помимо прочего, серверы HPE ProLiant Gen10 и HPE ProLiant Gen9.

Уязвимость RCE критической степени серьезности

Уязвимость, о которой Харрисон Нил сообщил в рамках программы Trend Micro Zero Day Initiative, отслеживается как CVE-2020-7200 и затрагивает HPE Systems Insight Manager (SIM) 7.6.x.

CVE-2020-7200 был оценен HPE как недостаток безопасности критической степени серьезности (9,8 / 10), который позволяет злоумышленникам без каких-либо прав использовать его в рамках атак низкой сложности, не требующих взаимодействия с пользователем.

Уязвимость возникает из-за отсутствия надлежащей проверки данных, предоставленных пользователем, что может привести к десериализации ненадежных данных, что позволяет злоумышленнику использовать их для выполнения кода на серверах, на которых запущено уязвимое программное обеспечение.

HPE не сообщила в рекомендациях по безопасности, если ошибка нулевого дня также используется в дикой природе.

В то время как HPE SIM поддерживает операционные системы Linux и Windows, HPE выпустила информацию о смягчении последствий только для блокирования атак на системы Windows.

Представитель HPE не был немедленно доступен для комментариев, когда сегодня BleepingComputer связался с ним для получения дополнительной информации о затронутых платформах и о продолжающейся эксплуатации.

Доступные меры смягчения

Компания Hewlett Packard Enterprise включила информацию о смягчении последствий в рекомендацию по безопасности CVE-2020-7200, которая требует отключения функций «Федеративный поиск» и «Конфигурация федеративного CMS», которые позволили использовать уязвимость.

«Полное исправление, предотвращающее уязвимость удаленного выполнения кода, будет доступно в будущем выпуске», - говорится в сообщении безопасности .

Системные администраторы, использующие программное обеспечение для управления SIM-картами HPE, должны использовать следующую процедуру для блокировки атак CVE-2020-7200:

Остановить службу HPE SIM

Удалите файл C: \ Program Files \ HP \ Systems Insight Manager \ jboss \ server \ hpsim \ deploy \ simsearch.war из установленного сим-пути del / Q / FC: \ Program Files \ HP \ Systems Insight Manager \ jboss \ server \ hpsim \ развертывание \ simsearch.war

Перезапустите службу HPE SIM

Подождите, пока откроется веб-страница HPE SIM «https: // SIM_IP: 50000», и выполните следующую команду из командной строки. mxtool -r -f tools \ multi-cms-search.xml 1> nul 2> nul

Согласно HPE, после принятия мер по снижению риска пользователи HPE SIM больше не смогут использовать функцию федеративного поиска». ***(Sergiu Gatlan. HPE discloses critical zero-day in server management software // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hpe-discloses-critical-zero-day-in-server-management-software/). 16.12.2020).***

***

«Количество сообщений об уязвимостях увеличилось за последние 12 месяцев как минимум на одной краудсорсинговой платформе безопасности, при этом в отчетах о критических проблемах зафиксирован скачок на 65%.

Данные поступают с платформы Bugcrowd и также отражают рост выплат, поскольку этические хакеры выявляют более критические уязвимости, связывая ошибки и разрабатывая проверочный код эксплойта.

Время ожидания отчета о критической ошибке

Bugcrowd сообщает, что компании, предлагающие потребительские услуги и работающие в медиаиндустрии, получают критические отчеты о критических проблемах менее чем за день.

Для организаций государственного и автомобильного секторов сообщения об ошибках с высоким риском отправляются в течение нескольких дней и часто представляют собой «гораздо более высокие ставки».

Больше представлений, лучшие награды

В этом году количество сообщений об уязвимостях через Bugcrowd увеличилось на 50%, в то время как для отчетов с приоритетом 1 (наиболее критичных) рост составил 65%.

Веб-приложения остаются в числе основных предпочтений хакеров, хотя они диверсифицируют цели, чтобы оставаться конкурентоспособными…

В период с января по октябрь 2020 года организации, работающие в сфере финансовых услуг, получили больше заявок, чем за весь 2019 год. Выплаты за уязвимости P1 в этом секторе удвоились во втором квартале этого года.

Злоумышленники также активизировали свои атаки, заставляя компании увеличивать выплаты в случае серьезных проблем. В целом выплаты за критические уязвимости (P1) выросли на 31% с первого по второй квартал. То же самое произошло с ошибками P2 между Q2 и Q3.

Сообщается о тенденциях в количестве ошибок

В верхней части списка уязвимостей, наиболее часто обнаруживаемых через Bugcrowd, находится управляемый человеком нарушенный контроль доступа, блокирующий межсайтовый скриптинг (XSS).

Захват поддоменов также подскочил на две позиции в списке, с шести до четырех, причиной скачка стало более активное использование хакерами автоматизации для своих сессий поиска ошибок.

Одна из тенденций, предвосхищающая поиск ошибок, - это подход «снаружи внутрь», который открывает область вознаграждения для скрытых или забытых активов (теневые ИТ), которые увеличивают кибер-риски компании.

Bugcrowd наблюдала эту тенденцию в компаниях, имеющих развитую программу кибербезопасности, признавая, что поверхность их атак менялась так часто, что это приводило к игнорированию активов.

Компании, соответствующие этому профилю, добавили управление поверхностью атаки (ASM) к своему краудсорсинговому решению безопасности, чтобы позволить охотникам за ошибками вести разведку и обнаруживать принадлежащие им неизвестные активы, которые могут представлять опасность.

Хотя уязвимости нулевого дня привлекают все внимание, поскольку они обычно связаны с атаками со стороны продвинутой постоянной угрозы (APT - обычно поддерживаемые государством хакеры), большую часть времени эти злоумышленники полагаются на известные эксплойты…

Один из примеров в отчете относится к уязвимостям удаленного выполнения кода в решениях F5 BIG-IP (CVE-2020-5902). Bugcrowd сообщает, что охотники за головами сообщили о проблеме на платформе до того, как о ней было объявлено.

Bugcrowd отмечает, что изменения, зафиксированные в этом году, созвучны проблемам удаленной работы, вызванным пандемией. Проводя больше времени дома, «охотники за ошибками» могли быть более активными и находить более серьезные ошибки, а также отправлять более качественные отчеты». ***(Ionut Ilascu. Pandemic year increases bug bounties and report submissions // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/pandemic-year-increases-bug-bounties-and-report-submissions/). 15.12.2020).***

***

«На этой неделе Mattermost в сотрудничестве с Golang обнаружил 3 критические уязвимости в синтаксическом анализаторе XML языка Go.

В случае эксплуатации эти уязвимости, которые также влияют на несколько реализаций SAML на основе Go, могут привести к полному обходу аутентификации SAML, которая используется сегодня в известных веб-приложениях.

Парсер XML не гарантирует целостность

Перечисленные ниже уязвимости двустороннего обмена XML скрываются в синтаксическом анализаторе языка XML Golang encoding / xml, который не возвращает надежных результатов при кодировании и декодировании входных XML-данных.

Это означает, что разметка XML при кодировании и декодировании с помощью анализатора может возвращать противоречивые и неожиданные результаты.

CVE-2020-29509: нестабильность атрибутов XML в кодировке Go / xml

CVE-2020-29510: нестабильность директивы XML в кодировке / xml Go

CVE-2020-29511: нестабильность XML-элемента в кодировке Go / xml

«Как видно из названий, уязвимости тесно связаны. Основная проблема во всех трех случаях одинакова: злонамеренно созданная разметка XML мутирует во время циклических переходов через реализации декодера и кодировщика Go», - сказал Юхо Нурминен, инженер по безопасности продуктов в Mattermost.

Нурминен объяснил, что это означает, что если приложение использует синтаксический анализатор XML, кодировщик и декодер не сохранят семантику исходной разметки.

"Если ваше приложение обрабатывает XML и, обрабатывая его, анализирует разметку, которая является выводом по крайней мере одного предыдущего цикла синтаксического анализа и сериализации, вы больше не можете предполагать, что вывод этого синтаксического анализа совпадает с выводом предыдущего цикла. Другими словами, передача XML через декодер и кодировщик Go не сохраняет его семантику», - пояснил Нурминен.

Одно из частичных исправлений уязвимостей демонстрирует несоответствия, которые могут возникать во время синтаксического анализа XML из-за этих недостатков.

Например, у `<: name>` будет удалено двоеточие, и аналогично, тег XML с атрибутом, содержащим пустое значение (""), будет отображаться без атрибута вообще во время сериализации.

Возможен полный обход аутентификации SAML

Хотя на первый взгляд это может показаться тривиальной ошибкой, Mattermost подчеркивает, что несколько приложений ожидают семантической целостности, и эти уязвимости могут иметь серьезные последствия.

Например, различные реализации SAML, использующие упомянутый синтаксический анализатор XML, могут быть обмануты злоумышленниками, чтобы полностью обойти аутентификацию SAML.

Язык разметки утверждения безопасности (SAML) - это стандарт веб-аутентификации, используемый несколькими известными веб-сайтами и службами для облегчения онлайн-входа с использованием XML.

«Из-за этих уязвимостей реализации SAML на основе Go во многих случаях открыты для взлома злоумышленником: путем внедрения вредоносной разметки в правильно подписанное сообщение SAML можно сделать так, чтобы оно по-прежнему выглядело правильно подписанным, но изменив его семантику, чтобы передать ", - предупредил Маттермост.

Если критически важное приложение использует синтаксический анализатор XML, влияние на систему SSO SAML может заключаться в повышении привилегий или обходе аутентификации, в зависимости от того, как приложение использует уязвимый синтаксический анализатор XML.

Нет патча для самого парсера

Стоит отметить, что на данный момент команда безопасности Go сообщила, что патча для исправления этих уязвимостей не существует.

Фиксация исправления, описанная выше, также указывает, что стабильность приема-передачи не является поддерживаемым свойством безопасности для encoding / xml, что делает одно исправление недостаточным для обеспечения надежности синтаксического анализа XML.

Однако для некоторых отдельных проектов SAML на основе Go были выпущены исправленные версии, например:

Dex IDP версии 2.27.0

github.com/crewjam/saml версия 0.4.3

github.com/russellhaering/gosaml2 версия 0.6.0

Кроме того, Mattermost предоставил инструмент « xml-roundtrip-validator », который можно использовать в качестве обходного пути при включении проверки XML в ваше приложение.

Полные выводы исследователей Mattermost и сроки раскрытия информации представлены в их сообщении в блоге». ***(Ax Sharma. Critical Golang XML parser bugs can cause SAML authentication bypass // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/critical-golang-xml-parser-bugs-can-cause-saml-authentication-bypass/). 14.12.2020).***

***

«Команда Check Point обнаружила уязвимости в игровой платформе Steam от компании Valve. Корень проблем крылся в библиотеке Game Networking Sockets (GNS или Steam Sockets). GNS является основной сетевой библиотекой,

используемой в самых разных играх, включая собственные игры Valve (такие как CS: GO, Dota2, Team Fortress 2), а также сторонние тайтлы (например, Destiny 2).

Исследователи обнаружили сразу несколько уязвимостей в имплементации GNS от Valve. Они рассказывают, что библиотека может поддерживать связь как в P2P-режиме, так и так и в централизованном режиме клиент-сервер. Именно этот фактор стал ключевым, поскольку так злоумышленники могут получить контроль над компьютером, подключенным к стороннему игровому серверу.

Используя уязвимости в GNS, хакеры могли проводить множество различных атак, которые могли повлечь за собой серьезные последствия. Например, злоумышленник мог вывести из строя игровой клиент противника, чтобы победить в матче, или даже обеспечить «эффектный» rage quit, полностью выведя из строя игровой сервер Valve и убедившись, что нормально играть не будет никто.

Наиболее опасной специалисты называют ситуацию, когда пользователи играют в игру, созданную сторонними разработчиками. В этом случае хакер мог удаленно скомпрометировать игровой сервер, чтобы выполнить на нем произвольный код. В итоге же злоумышленник получал доступ к личным данным и персональной информации других игроков.

Опираясь на статистические данные от Steam, эксперты делают вывод, что уязвимости в GNS каждый день ставили под угрозу сотни тысяч игроков, ведь в 2019 году Steam пользовались более 95 миллионов геймеров в месяц, которые получали доступ более чем к 34 000 игр. И если раньше пользователи подвергались атакам, кликая на ссылку или скачивая файл с малварью, то в данном случае стать потенциальной жертвой злоумышленников можно было просто войдя в игру.

В общей сложности специалисты Check Point уведомили компанию Valve о четырех уязвимостях в GNS (CVE-2020-6016, CVE-2020-6017, CVE-2020-6018 и CVE-2020-6019), и еще в сентябре 2020 года инженеры Valve своевременно устранили все баги.

«Мы рекомендуем пользователям обновить игры сторонних разработчиков. Особое внимание стоит уделить играм, скачанным до 4 сентября 2020 года — именно в этот день Valve выпустила патч для библиотеки Steam», — рассказывает Василий Василий Дягилев, глава представительства Check Point Software Technologies в России и СНГ». ***(Мария Нефёдова. Баги в Steam позволяли хакерам влиять на онлайн-игры Valve // Xakep (https://xakep.ru/2020/12/15/gns-bugs/). 15.12.2020).***

***

«В 2020 году Компьютерная команда экстренной готовности США (US-CERT) внесла в Национальную базу уязвимостей 17 447 новых уязвимостей – четвертый подряд рекордный показатель за год (предыдущий рекорд был зафиксирован в 2019 году – 17 306).

По данным Национального института стандартов и технологий США (NIST), в нынешнем году было зафиксировано 4168 высокоопасных, 10 710 среднееопасных и 2569 малоопасных уязвимостей. Для сравнения, в 2019 году было зафиксировано 4337 высокоопасных, 10 956 среднееопасных и 2013 малоопасных уязвимостей.

Рост из года в год числа обнаруживаемых уязвимостей наталкивает на мысль: стали ли разработчики использовать больше уязвимого кода, или исследователи безопасности улучшили свои навыки по поиску уязвимостей? Учитывая текущие обстоятельства и растущую популярность программ bug bounty, эксперты считают, что оба фактора сыграли свою роль.

В нынешнем году также зафиксирован существенный рост в сфере краудсорсинговой кибербезопасности. Как сообщает краудсорсинговая ИБ-платформа Bugcrowd, за последние 12 месяцев количество отчетов исследователей безопасности об обнаруженных уязвимостях увеличилось на 50%. Число сообщений о критических уязвимостях, являющихся приоритетными для исправления, возросло на 65%.

Платформа HackerOne также подтвердила рост числа отчетов об уязвимостях. Более трети всех 180 тыс. уязвимостей, внесенных через HackerOne, были обнаружены в нынешнем году. В течение первого месяца карантина, введенного из-за пандемии коронавируса, количество сообщений об уязвимостях выросло на 28%, а сумма вознаграждений, выплаченных компаниями в рамках программ bug bounty за этот период, увеличилась на 29%.

В 2020 году Microsoft и Oracle трижды выпускали обновления безопасности в один и тот же день. В течение восьми месяцев в рамках «вторника исправлений» Microsoft исправляла более 110 уязвимостей каждый месяц. В июне и сентябре число патчей достигало 129». ***(В 2020 году US-CERT задокументировала рекордные 17 447 уязвимостей // SecurityLab.ru (https://www.securitylab.ru/news/514959.php). 18.12.2020).***

***

«Плохо настроенный файл открывает пользователям возможность захвата сайта.

Исследователи заявили, что Easy WP SMTP, плагин WordPress для управления электронной почтой, имеющий более 500 000 установок, имеет уязвимость, которая может привести к захвату сайта.

Easy WP SMTP позволяет пользователям настраивать и отправлять все исходящие электронные письма через SMTP-сервер, чтобы они не попадали в папку нежелательной почты / спама получателя. По словам исследователей GBHackers, версия 1.4.2 и ниже содержит ошибку в файле отладки, которая обнаруживается из-за фундаментальной ошибки в том, как плагин поддерживает папку.

«[Уязвимость] позволит неаутентифицированному пользователю сбросить пароль администратора, что позволит хакеру получить полный контроль над веб-сайтом», - говорится в сообщении в понедельник.

В этот необязательный журнал отладки плагин записывает все сообщения электронной почты (заголовки и тело), отправленные веб-сайтом. Он находится в папке установки плагина, «/ wp-content / plugins / easy-wp-smtp /», - сказали исследователи.

Журнал представляет собой простой текстовый файл; а в папке плагина нет файла index.html, так что на серверах, на которых включен список каталогов,

хакеры могут находить и просматривать журнал, открывая путь для сканирования с перечислением имен пользователей. Это может позволить злоумышленникам найти логин администратора.

«Хакеры также могут выполнять ту же задачу, используя сканирование авторских достижений (/? Author = 1)», - пояснили исследователи. «Они заходят на страницу входа и просят сбросить пароль администратора. Затем они снова обращаются к журналу отладки Easy WP SMTP, чтобы скопировать ссылку сброса, отправленную WordPress. После получения ссылки они сбрасывают пароль администратора».

По словам исследователей, вход в панель управления администратора дает злоумышленникам возможность запускать сайт, в том числе устанавливать мошеннические плагины.

Чтобы исправить проблему, пользователям следует выполнить обновление до текущей версии 1.4.4.

Проблемные плагины

Плагины WordPress продолжают предоставлять киберпреступникам удобный способ атаковать.

В ноябре в плагине электронной коммерции Welcart была обнаружена уязвимость системы безопасности, открывающая веб-сайты для внедрения кода. По словам исследователей, это может привести к установке скиммеров платежей, сбою сайта или поиску информации с помощью SQL-инъекции.

В октябре в Post Grid, плагине WordPress, установленном более 60 000 экземпляров, были обнаружены две уязвимости высокой степени опасности, что открыло путь к захвату сайтов. А в сентябре было обнаружено, что серьезная ошибка в плагине Email Subscribers & Newsletters от Icegram затронула более 100 000 веб-сайтов WordPress…». ***(Tara Seals. Easy WP SMTP Security Bug Can Reveal Admin Credentials // Threatpost (https://threatpost.com/easy-wp-smtp-security-bug/162301/). 15.12.2020).***

***

«Mozilla Foundation выпускает браузер Firefox 84, в котором исправлено несколько недостатков и обеспечено повышение производительности и поддержка процессоров Apple.

Обновление Mozilla Foundation для веб-браузера Firefox, выпущенное во вторник, устраняет одну критическую уязвимость и несколько серьезных ошибок. Обновление, выпущенное как Firefox версии 84, также объявлено Mozilla как повышение производительности браузера и добавление встроенной поддержки оборудования MacOS, работающего на его собственных процессорах Apple.

В общей сложности было исправлено шесть серьезных недостатков, помимо критической ошибки, отслеживаемой как CVE-2020-16042. Конкретная критическая ошибка в Firefox также была отмечена ранее в этом месяце в обновлении безопасности браузера Google Chrome, где она была оценена как серьезная ошибка.

Рассматриваемая ошибка Firefox и Chrome (CVE-2020-16042) до сих пор не полностью описана ни одним из производителей браузеров и указана только как ошибка памяти.

Загадочная ошибка также влияет на веб-браузер Google Chrome

В рекомендациях по безопасности Mozilla CVE-2020-16042 описывается как недостаток в компоненте JavaScript под названием BigInt, который «мог привести к раскрытию неинициализированной памяти».

BigInt - это компонент JavaScript, используемый для представления «произвольно больших целых чисел» в контексте процесса JavaScript в браузере, согласно описанию Mozilla.

Google по-разному описывает тот же недостаток. Он называет это ошибкой «неинициализированного использования», влияющей на движок JavaScript V8 Chrome. Из бюллетеня Google также неясна точная природа недостатка. Но исследователи кибербезопасности описали эти типы ошибок, связанных с неинициализированным использованием, как «в значительной степени упускаемые из виду» и часто «рассматриваемые как незначительные ошибки памяти».

«[Они] на самом деле являются критическим вектором атаки, который может быть надежно использован хакерами для запуска атак с повышением привилегий в ядре Linux», - говорится в исследовании 2017 года, опубликованном Технологическим институтом Джорджии.

На прошлой неделе Microsoft также сослалась на CVE в своем декабрьском списке ошибок во вторник, касающемся браузера Edge версии 87.0.664.57. Браузер Microsoft Edge, выпущенный в январе 2020 года, основан на проекте программного обеспечения с открытым исходным кодом Google Chromium. Исходный код Chromium используется в браузере Google Chrome и браузере Microsoft Edge 2020.

Движок JavaScript V8 и WebAssembly

Движок JavaScript с открытым исходным кодом V8 был разработан Chromium Project для веб-браузеров Google Chrome и Chromium. Движок JavaScript V8 не поддерживается Firefox, но компонент WebAssembly, часто связанный с V8, поддерживает.

WebAssembly, или сокращенно WASM, - это открытый стандарт, который определяет переносимый формат двоичного кода для исполняемых программ в соответствии с проектом WebAssembly. «WebAssembly описывает безопасную для памяти изолированную среду выполнения, которая может быть реализована даже внутри существующих виртуальных машин JavaScript», - говорится на веб-сайте проекта.

Браузер Mozilla Firefox не основан на Chromium. WASM поддерживается в Mozilla Firefox и Apple Safari, хотя оба они не используют Google V8. Некоторые подсказки относительно природы ошибки могут быть получены из того факта, что ошибка затрагивает как браузер Firefox, так и браузер Chrome - общим знаменателем является WASM. Кроме того, анализ ошибок WASM и V8 за 2018 год предупредил о возможных проблемах безопасности.

В 2018 году Google Project Zero опубликовал исследование под названием «Проблемы и перспективы WebAssembly » и выявил три уязвимости, которые были

устранены. Одна из будущих угроз WASM, как предупреждает Google, связана с функцией сборщика мусора (GC) WebAssembly.

WebAssembly виноват?

Сборщик мусора - важный процесс, связанный с движками JavaScript. «Приложения Java получают объекты в памяти по мере необходимости. Задача GC в виртуальной машине Java (JVM) - автоматически определять, какая память больше не используется Java-приложением, и повторно использовать эту память для других целей», - описывает Джон Уортингтон в сообщении о важности GC.

Что касается Google, то в 2018 году он предупреждал:

«WebAssembly GC - еще одна потенциальная возможность WebAssembly, которая может привести к проблемам с безопасностью. В настоящее время некоторые виды использования WebAssembly имеют проблемы с производительностью из-за отсутствия управления памятью более высокого уровня в WebAssembly. Например, сложно реализовать высокопроизводительную виртуальную машину Java в WebAssembly. Если будет реализован сборщик мусора WebAssembly, это увеличит количество приложений, для которых можно использовать WebAssembly, но также повысит вероятность того, что уязвимости, связанные с управлением памятью, возникнут как в механизмах WebAssembly, так и в приложениях, написанных на WebAssembly».

В обоих национальных репозиториях баз данных уязвимостей, MITER и NIST, технические особенности CVE еще не раскрыты публично. В декабрьском бюллетене по безопасности Google отмечалось, что детали, связанные с CVE-2020-16042, и другие ошибки не разглашались, «до тех пор, пока большинство пользователей не обновят исправление». Он также отметил, что, когда и если ошибки существуют в сторонних библиотеках кода, используемых на других устройствах или платформах, технические детали ошибок ограничены.

За обнаружение ошибки приписывается охотник за ошибками Андре Баргулл, который первоначально сообщил об ошибке 23 ноября, согласно Google.

Шесть серьезных ошибок Firefox

Проблемы с памятью преобладали в списке серьезных ошибок, исправленных Mozilla Tuesday. Были исправлены две «ошибки безопасности памяти» (CVE-2020-35114 и CVE-2020-35113). Оба CVE исправляли ошибки в Firefox 84 и его браузере с расширенной поддержкой Firefox (ESR) 78.6 для крупных предприятий.

«Некоторые из этих ошибок свидетельствовали о повреждении памяти, и мы предполагаем, что при достаточных усилиях некоторые из них могли быть использованы для запуска произвольного кода», - написала Mozilla об обеих ошибках.

Также к памяти браузера связаны ошибки, отслеживаемые как CVE-2020-26971, CVE-2020-26972 и CVE-2020-26973, которые включают переполнение буфера кучи в WebGL, использование после освобождения в WebGL и выполнение дезинфицирующего средства CSS. некорректная санация». ***(Tom Spring. Firefox Patches Critical Mystery Bug, Also Impacting Google Chrome // Threatpost (https://threatpost.com/firefox-patches-critical-mystery-bug-also-impacting-google-chrome/162294/). 15.12.2020).***

***

«Разработчики Dell выпустили обновления для некоторых моделей Wyse Thin Client. Патчи исправляют ряд критических уязвимостей, которые можно использовать удаленно и без аутентификации.

Уязвимости были обнаружены специалистами CyberMDX, которая специализируется на кибербезопасности в сфере здравоохранения. По данным компании, только в США эти продукты Dell используют более 6000 организаций, включая многих поставщиков медицинских услуг.

Исследователи CyberMDX заметили, что локальный FTP-сервер, используемый Dell Wyse Thin Client для получения новых прошивок, пакетов и конфигураций, доступен по умолчанию без учетных данных, что позволяет получить к нему доступ любому желающему. По сути, хакер мог получить доступ к файлу INI, хранящемуся на сервере, и внести изменения в этот файл.

«Файлы INI содержат длинный список настраиваемых параметров, подробно описанный на более чем 100 страницах официальной документации Dell. Чтение или изменение этих параметров открывает двери для множества различных атак. Настройка и включение VNC для полного удаленного управления, слив учетных данных удаленного рабочего стола и манипулирование результатами DNS — вот лишь некоторые из сценариев атак, о которых следует знать», — пишут исследователи.

Подобные атаки стали возможны из-за двух уязвимостей: CVE-2020-29491, которая позволяет неаутентифицированному злоумышленнику получить доступ к файлу конфигурации, и CVE-2020-29492, которая позволяет вносить изменения в файл.

Dell сообщила своим клиентам, что уязвимости влияют на тонкие клиенты Wyse 3040, 5010, 5040, 5060, 5070, 5470 и 7010 под управлением ThinOS 8.6 и более ранних версий. Уязвимости были исправлены с выпуском ThinOS версии 8.6 MR8». ***(Мария Нефёдова. Две опасные уязвимости исправлены в Dell Wyse Thin Client // Xakep (https://xakep.ru/2020/12/22/wyse-thin-client-flaws/). 22.12.2020).***

***

«Представители HackerOne сообщили, что румынский ИБ-специалист Космин Иордач (@inhibitor181) стал первым в истории проекта исследователем, который заработал на bug bounty более 2 000 000 долларов. Также он седьмой исследователь, получивший более миллиона долларов всего за два года: этой отметки он достиг, получив более 300 000 долларов всего за 90 дней.

Иордач рассказал HackerOne, что последние шесть лет он живет в Германии, с женой и двумя собаками. Интерес к взлому и уязвимостям проснулся в нем после семинара HackAttack, прошедшего в Гамбурге в середине 2016 года. Тогда эксперт еще учился в университете, но в конце 2017 года он уже серьезно занялся охотой за багами, продолжая работать в качестве full-stack разработчика.

Вскоре исследователь получил высший ранг The Assassin на сингапурском хакерском ивенте h1-65, а в 2019 году он отстоял свой титул в Лондоне, в ходе h1-4420.

В общей сложности на счету Космина Иордача 468 найденных уязвимостей, в том числе в продуктах Verizon Media, PayPal, Dropbox, Facebook, Spotify, AT&T, TikTok, Twitter, Uber и GitHub, а также ряд ошибок в системах Министерства обороны США.

Напомню, что в настоящее время на HackerOne есть всего девять багхантеров, заработавших более 1 000 000 долларов. Два первых миллионера появились на HackerOne весной прошлого года. Первым рекордсменом стал Сантьяго Лопес (@try_to_hack) из Аргентины. Он был самоучкой, когда зарегистрировался на HackerOne в 2015 году, в возрасте шестнадцати лет. За прошедшие годы он нашел более 1600 уязвимостей, в том числе в решениях Twitter и Verizon Media.

Второй миллионер HackerOne — британец Марк Личфилд (@mlitchfield). Он уже помог исправить более 900 багов в продуктах таких компаний, как Dropbox, Yelp, Venmo, Starbucks, Shopify и Rockstar Games.

По словам главы HackerOne, за все время существования проекта исследователи уже обнаружили порядка 170 000 уязвимостей, а платформу сейчас используют более 700 000 этичных хакеров». ***(Мария Нефёдова. Исследователь заработал на HackerOne более 2 000 000 долларов // Хакер (https://xakep.ru/2020/12/25/hackerone-achievement/). 25.12.2020).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Компания Fortinet, мировой лидер в области глобальных интегрированных и автоматизированных решений для обеспечения кибербезопасности, сообщает о вхождении в список лидеров исследования Gartner Magic Quadrant 2020 for Network Firewall. Это уже 11 раз когда компания была отмечена исследованием Gartner 2020 Magic Quadrant, посвященным межсетевым экранам, в категориях «Ability to Execute» (Способность Реализации) и «Further in Completeness of Vision» (Полнота Видения).

«Мы уверены, что Fortinet предоставляет самую широкую и целостную платформу безопасности в отрасли. Мы первыми внедрили сетевой подход, основанный на безопасности, интегрировав элементы защиты в каждый сегмент сети и позволив клиентам обезопасить любую периферию в любом масштабе.

Fortinet снова вошла в список лидеров по результатам исследования Gartner Magic Quadrant 2020 for Network Firewall. Ранее мы также были названы в числе лидеров по результатам исследования Gartner 2020 Magic Quadrant, посвященного инфраструктуре WAN Edge. Мы считаем, что наш успех обусловлен неизменной приверженностью инновациям, уникальной и гибкой платформой безопасности и подходу, заключающемуся в защите всей поверхности атаки – от локальной сети до облака» – Джон Мэддисон, первый вице-президент отдела маркетинга продуктов и решений компании Fortinet.

Межсетевые экраны следующего поколения FortiGate (NGFW) являются неотъемлемым компонентом платформы Fortinet Security Fabric, которая обеспечивает широкую видимость и защиту на всей поверхности атаки. FortiGate NGFW защищают любую периферию и в любом масштабе, поскольку они оснащены специализированными блоками обработки безопасности (SPU), что обеспечивает наивысший в отрасли Security Compute Rating. Fortinet продолжает внедрять инновации, предлагая безопасный SD-WAN с расширенной маршрутизацией и наиболее гибкими в отрасли опциями безопасности, благодаря интегрированной облачной безопасности на основе NGFW или SASE.

Мы считаем, что место в квадранте лидеров во многом связано с постоянным стремлением компании предлагать сетевой подход, основанный на безопасности, который интегрирует защиту во все элементы сети и позволяет клиентам.

Управлять операционными рисками и рисками безопасности, обеспечивая непрерывность бизнес-процессов. Цифровая трансформация предлагает компаниям огромные возможности для формирования ценности и повышения эффективности. Однако это также создает новые риски для безопасности, такие как расширение поверхности атаки в фокусе потенциальных киберпреступников. С помощью Fortinet NGFW клиенты могут полностью контролировать свои сети, приложения и потенциальные угрозы. Fortinet предлагает наивысший в отрасли рейтинг безопасности вычислений благодаря мощности специально созданных блоков обработки безопасности (SPU, например NP7) для обеспечения оптимального взаимодействия с пользователем в любом масштабе.

Сокращение расходов и сложности системы. По мере расширения поверхности цифровых атак группы безопасности также должны расширять свои возможности защиты. NGFW от Fortinet позволяют клиентам выстраивать глубокую защиту с помощью сегментации, динамического доверия и расширенной инспекции безопасности для обеспечения бесперебойности операций. FortiGate NGFW защищает бизнес-приложения с помощью сервисов FortiGuard на базе искусственного интеллекта и машинного обучения, устраняя необходимость в специализированных продуктах и обеспечивая оптимальную совокупную стоимость владения (TCO).

Повышение эффективности работы. Единая консоль управления в Fabric Management Center обеспечивает полное и консолидированное представление о различных границах сети, локальных или в облачных. Fabric Management Center обеспечивает автоматизацию и оркестровку Security Fabric, охватывающую более 400 элементов экосистемы. Это упрощает рабочие процессы в FortiGate, FortiManager, FortiAnalyzer и партнерской экосистеме в масштабе предприятия.

Благодаря эффективности сетевого подхода, основанного на безопасности, и ведущих в отрасли межсетевых экранов следующего поколения FortiGate NGFW, Fortinet предлагает самые гибкие и гипермасштабируемые решения безопасности для удовлетворения растущих и часто непредсказуемых потребностей в производительности, которые могут быстро превзойти возможности организации.

Помимо получения звания лидера по результатам исследования Gartner Magic Quadrant 2020 for Network Firewalls, компания Fortinet была также отмечена как «Выбор клиентов Gartner Peer Insights for Network Firewall». Мы считаем, что это

дополнительное признание со стороны клиентов еще раз подчеркивает, что подход Fortinet к платформе, базирующийся на принципах простоты, безопасности и масштабируемости находит отклик у клиентов во всех отраслях.

Компания Gartner не одобряет никаких поставщиков, продуктов или услуг, упомянутых в ее исследовательских публикациях, и не советует пользователям технологий выбирать только тех поставщиков, которые имеют наивысший рейтинг или другое обозначение. Исследовательские публикации Gartner основаны на оценках организации и не должны быть истолкованы как непреложный факт. Компания Gartner отказывается от всех гарантий, выраженных или подразумеваемых, в отношении данного исследования, включая любые гарантии товарного состояния или пригодности для определенной цели». ***(Fortinet среди лидеров Gartner Magic Quadrant 2020 по межсетевым экраном // AMC Ukraine (https://channel4it.com/publications/fortinet-sredi-liderov-gartner-magic-quadrant-2020-po-mezhsetevym-ekranom.html). 04.12.2020).***

***

«Компания IT-Solutions сообщает о подписании партнерского соглашения с Qualys, в рамках которого сможет предоставить заказчикам доступ к решениям вендора в области ИТ и информационной безопасности.

Как отмечается, Qualys – мировой лидер в сегменте решений по управлению уязвимостями и контролю соответствия требованиям. С помощью облачной платформы Qualys, клиенты IT-Solutions смогут консолидировать решения ИБ и соответствия требованиям в рамках одной платформы и встроить безопасность в инициативы по цифровой трансформации для обеспечения большей гибкости, выгоды для бизнеса и существенной экономии средств.

Облачная платформа Qualys и ее интегрированные приложения непрерывно предоставляют организациям доступ к критически важной информации по безопасности, позволяя им автоматизировать полный спектр задач по аудиту, обеспечению соответствия требованиям и защиты ИТ-систем и веб-приложений внутри организаций, на мобильных клиентах и в облаках.

Для платформы Qualys не важно, где находятся ИТ-активы (локально, на периметре, в облаках или у сотрудников дома, и пр.) и к какому типу они принадлежат (рабочие станции, сервера, веб-приложения, контейнеры, АСУ ТП, и пр.), а для ее использования не нужна никакая вспомогательная инфраструктура в виде VPN. Платформа динамически масштабируется под клиента и решает задачи независимо от внешних условий без дополнительных затрат.

«Информационная безопасность сегодня глобальный тренд рынка. Поэтому ее обеспечение становится основным вопросом удержания бизнеса на плаву. В то же время наша цель – сделать бизнес клиентов не только более простым и управляемым, но и защищенным. Сотрудничество с Qualys позволит нам создавать инновационные проекты в области кибер-безопасности и повысить уровень информационной защиты наших заказчиков», – отметил Иван Зимин, технический директор IT-Solutions». ***(IT-Solutions будет продвигать решения Qualys в области ИБ // Компьютерное Обозрение (https://ko.com.ua/it-solutions_budet_prodvigat_resheniya_qualys_v_oblasti_ib_135585). 09.12.2020).***

***

«Компания Group-IB сообщила о соответствии рекомендациям Министерства юстиции США в области кибербезопасности и кибербезопасности и киберразведки высокотехнологичной системы Group-IB Threat Intelligence & Attribution. Основанная на инновационных технологиях, подтвержденных более чем 30 патентами в разных странах мира, Group-IB TI&A предназначена для сбора данных об угрозах и атакующих, релевантных для конкретной организации, с целью исследования, проактивной охоты за хакерами и защиты сетевой инфраструктуры. Проверка технологий Group-IB TI&A проводилась одной из компаний «Большой четверки» (Big Four), которая подтвердила их соответствие отраслевым рекомендациям в области сбора данных киберразведки. Group-IB является первым вендором в сфере кибербезопасности, предложившим рынку высокотехнологичное решение, разработанное командой инженеров компании и способное создавать динамическую карту угроз под каждую компанию, ее клиентов и партнеров. Group-IB TI&A соединяет разрозненные события вокруг атаки, обеспечивая возможность атрибутировать угрозы, анализировать вредоносный код и немедленно реагировать на инцидент. Каждый специалист, использующий TI&A, получает доступ к крупнейшей коллекции данных даркнета, продвинутой модели профилирования хакерских групп, а также полностью автоматизированному графовому анализу, который за секунды помогает провести корреляцию данных и атрибутировать угрозы до конкретной преступной группы. Рекомендации Департамента Юстиции США (Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources (Version 1.0, February 2020)) на текущий момент являются первым в мире сводом правил, описывающим принципы частных компаний в сфере сбора данных киберразведки. Цель документа — регламентировать этот процесс, чтобы снизить правовые риски для организаций, занимающихся изучением угроз на даркнет-форумах. В ходе проверки независимые эксперты одной из компаний-аудиторов «Большой четверки» проанализировали, каким образом Group-IB получает доступ к закрытым веб-ресурсам и собирает информацию на них, а также политики, внедренные компанией для регулирования перечисленных процедур. Продукты Group-IB представлены на рынках более 60 стран мира. Работая в разных юрисдикциях, Group-IB уделяет особое внимание соблюдению технических отраслевых стандартов, чтобы обеспечить наилучшее качество взаимодействия с клиентами. Успешно пройденная проверка системы Group-IB Threat Intelligence & Attribution, осуществленная одной из крупнейших международных аудиторских компаний, подтверждает стремление компании следовать ведущим мировым практикам в сфере кибербезопасности. «Group-IB стремится обеспечивать защиту своих клиентов на самом высоком уровне, — отмечает Дмитрий Волков, технический директор и глава киберразведки Group-IB. — Соответствие Group-IB рекомендациям американского регулятора в области сбора данных киберразведки является важным показателем зрелости внутреннего контроля компании и ее приверженности принципам, признанным в профессиональном сообществе». Group-IB Threat Intelligence & Attribution является частью экосистемы

высокотехнологичных продуктов для исследования киберугроз и охоты за атакующими Group-IB, которая была представлена на международной конференции CyberCrimeCon в конце ноября 2020 г. В центре внимания Group-IB TI&A — атакующие. Вокруг них выстроена вся идеология системы: выявить не только угрозу, но и того, кто за ней стоит. Массивы данных, которыми она оперирует, помогают оперативно связывать атаку с группировкой или конкретными персоналиями. TI&A «умеет» анализировать и атрибутировать угрозы, с которыми уже столкнулась компания, обнаруживать утечки и компрометацию пользователей, идентифицировать инсайдеров, торгующих данными компании на андеграудных ресурсах, выявлять и блокировать атаки, нацеленные на компанию и ее клиентов, независимо от отрасли. Таким образом, TI&A позволяет обнаруживать атаки, не покрываемые традиционными средствами защиты, глубже понимать методы работы продвинутых атакующих, а также оценивать, может ли им противостоять защищаемая инфраструктура. Такой подход помогает мотивировать и совершенствовать внутренние команды кибербезопасности, а также усиливать их экспертизу за счет глубокого понимания ландшафта угроз для защищаемой инфраструктуры». ***(Екатерина Быстрова. Group-IB TI&A соответствует рекомендациям Минюста США // ООО «АМ-МЕДИА» (https://www.anti-malware.ru/news/2020-12-09-111332/34457). 09.12.2020).***

***

«Incydr позволяет отслеживать пользователей из группы высокого риска, не мешая их текущей работе.

Суть проблемы инсайдерской угрозы в том, что рисковать может каждый. Вот почему большинство групп безопасности сосредотачиваются на получении более широкой и глубокой видимости всей файловой активности, особенно всплеска удаленной активности вне сети. Но это не означает, что службы безопасности должны сбрасывать со счетов свой с трудом заработанный опыт и знания о том, где наиболее вероятно обнаружение рисков. Например, все мы знаем, что увольняющиеся сотрудники представляют собой концентрированный риск. Но в типичной организации есть несколько других категорий сотрудников с высоким уровнем риска:

Риски бегства: сотрудники, которые выразили неудовлетворенность работой, недавно пропустили повышение по службе или задокументировали конфликты с коллегами.

Проблемы с производительностью: сотрудники с недавними отрицательными отзывами о производительности, пониженные в должности или включенные в план повышения производительности.

Путешествующие сотрудники: сотрудники, которые путешествуют по работе, особенно в регион, который может считаться высокорисковым, например, в Китай.

Угрозы безопасности: сотрудники, которые неоднократно нарушают протоколы безопасности (намеренно или иным образом), например, переходят по фишинговым ссылкам, или не проходят обучение по вопросам безопасности.

Привилегированный доступ: сотрудники с учетными данными / авторизованным доступом к интеллектуальной собственности или работающие над

важными и важными проектами и файлами - такими как сделка M&A, разработка новых продуктов или другие передовые инновации.

Не упускайте из виду высшее руководство

Высшее руководство почти всегда попадает в категорию «привилегированного доступа», включая ОГО и других руководителей службы безопасности. Дело не только в том, что эти высокопоставленные сотрудники имеют доступ к ценной информации - они часто с большей вероятностью будут делать то, что подвергает себя риску: Отчет Code42 о раскрытии данных за 2019 год показал, что 65% руководителей признались, что нажимали опасную ссылку - и более 3 из 4 ОГО признались, что нажимали на ссылку, которой у них быть не должно.

Установите тесные связи с лидерами отдела кадров и бизнес-направлений

Многие из вышеперечисленных категорий высокого риска являются динамическими - они меняются от недели к неделе или даже изо дня в день. Команды безопасности должны быть тесно связаны с руководителями отделов кадров и направлений бизнеса (LOB), чтобы контролировать эти группы пользователей с высоким уровнем риска. Например, руководитель службы безопасности должен быть частью рабочего процесса отдела кадров, когда сотрудники ставят планы повышения производительности или отмечают другие кадровые проблемы. Code42 даже работает над автоматизированными рабочими процессами, которые интегрируются с системой управления персоналом, такой как ADP или Workday, чтобы сделать это соединение беспроблемным и автоматическим в будущем. Точно так же командам безопасности важно знать, когда сотрудники едут в регионы с высоким уровнем риска. И им необходимо постоянно общаться с руководителями бизнес-подразделений, чтобы они знали о критически важных для бизнеса проектах, связанных с высокочувствительным контентом и новыми IP.

Code42 предоставляет гибкий объектив, позволяющий сосредоточиться на пользователях из группы повышенного риска

Выявление пользователей с высоким уровнем риска - это первый шаг, а эффективный мониторинг их - уникальная задача. Code42 разработала нашу платформу обнаружения и реагирования Incydr для решения этой проблемы. Incydr позволяет отслеживать пользователей из группы высокого риска, не мешая их текущей работе. И он использует оповещения на основе искусственного интеллекта, чтобы дать вам точный сигнал о риске, которому вы можете доверять. Вот краткий пример того, как Incydr может помочь развлекательной компании нацеливаться на пользователей с высоким риском, работающих над финальным эпизодом долгожданного сериала:

Администратор безопасности добавляет производственную группу, работающую над финальным эпизодом, в объектив Incydr для сотрудников с высоким уровнем риска.

Incydr обнаруживает совместное использование файлов и их утечку через компьютеры, облако и электронную почту через агента и прямую интеграцию с облаком и электронной почтой.

Служба безопасности получает уведомление, когда сотрудники с высоким уровнем риска перемещают файлы или обмениваются ими в ненадежные места, или когда активность соответствует другим индикаторам риска, например, когда сотрудник перемещает файлы в периоды, когда они обычно не работают. Это позволяет быстро расставить приоритеты, какие действия рассматривать в первую очередь.

Если рискованная деятельность требует расследования, Incydr позволяет вам быстро получить доступ ко всему, что вам нужно: просмотреть исторические тенденции активности пользователя, подробный контекст файлов, векторов и пользователей, и даже просмотреть содержимое файла, о котором идет речь.

В этом примере группа безопасности получает предупреждение о том, что видеофайл был загружен членом производственной группы. Аналитик сразу же может открыть файл, о котором идет речь, и подтвердить, что это почти финальная версия финального эпизода. Аналитик также может увидеть точное время загрузки, а также вектор (даже марку и серийный номер внешнего накопителя). Вооружившись этими доказательствами, группа безопасности может быстро повысить риск и соответствующим образом отреагировать - будь то автоматическое действие SOAR, дружеская беседа с сотрудниками отдела кадров или судебный иск.

Вот как выглядит интеллектуальная программа инсайдерского риска: сочетание опыта профессионалов в области безопасности с целенаправленными возможностями технологий следующего поколения». ***(Code42 Incydr Series: Honing in on High-Risk Users with Code42 Incydr // Threatpost (https://threatpost.com/code42-incydr-series-honing-in-on-high-risk-users-with-code42-incydr/161626/). 03.12.2020).***

***

«Австралийская кибер-мегамикс CyberCX совершила еще одно приобретение, на этот раз приобретя Foresight с прицелом на свой правительственный портфель.

CyberCX, группа компаний по обеспечению безопасности, возглавляемая двумя наиболее опытными австралийскими ветеранами технологий и кибернетической безопасностью, заявила, что специализированная консалтинговая компания Foresight укрепит свое присутствие в Канберре и укрепит ее возможности и репутацию «ведущей австралийской организации по кибербезопасности».

«Благодаря обширному опыту работы с правительственными агентствами Австралии, добавление Foresight расширит существенные возможности CyberCX по предоставлению решений кибербезопасности для крупных государственных клиентов», - заявила CyberCX.

Foresight - это независимая консалтинговая компания по вопросам кибербезопасности, основанная более десяти лет назад, которая занимается вопросами соответствия техническим требованиям и гарантиями безопасности для предприятий и правительства. CyberCX заявила, что Foresight обладает обширным опытом в предоставлении решений безопасности ведущим австралийским и

глобальным организациям, работая с австралийскими правительственными учреждениями при оценке больших и очень сложных систем.

Консультации также имеют особенно сильную практику облачной безопасности и работают с поставщиками облачных услуг, государственными учреждениями и крупными предприятиями.

«Мы создали Foresight как 100% австралийскую компанию, предоставляющую независимые консультации по кибербезопасности в качестве надежного советника для наших клиентов. CyberCX усиливает эту миссию», - сказал управляющий директор Foresight Питер Баусманн.

«Команда CyberCX быстро зарекомендовала себя как грозная сила в Австралии и Новой Зеландии. Мы надеемся и дальше обслуживать наших клиентов на самом высоком уровне и предлагать им полный набор возможностей и опыта, которые может предложить CyberCX».

CyberCX при поддержке частной инвестиционной компании BGH Capital была создана чуть более года назад, когда объединила 12 независимых австралийских брендов кибербезопасности: Alcorn, Assurance, Asterisk, CQR, Diamond, Enosys, Klein & Co, Phriendly Phishing, Sense of Security, Буревестник, TSS и YellIT.

Его возглавляет Аластер МакГиббон, бывший глава Австралийского центра кибербезопасности и когда-то специальный советник по кибербезопасности бывшего премьер-министра Малкольма Тернбулла, а также генеральный директор Джон Пайтаридис, который ранее был управляющим директором Optus Business.

С момента запуска CyberCX начала активно расширяться, одновременно создав несколько местных стартапов в области кибербезопасности.

В прошлом месяце он объявил о планах продвижения в Квинсленд, а в конце октября CyberCX возобновил операции в Западной Австралии после приобретения двух местных киберфирм, Asterisk Information Security и Diamond Cyber Security.

Фирма по управлению идентификацией Decipher Works и специалисты по облачной безопасности CloudTen также присоединились к организации в октябре; и два стартапа из Мельбурна, Basis Networks и Identity Solutions, были добавлены в CyberCX в июле.

CyberCX также продвинулась на рынок Новой Зеландии в августе, добавив свое первое приобретение Kiwi в Insomnia Security месяц спустя». ***(Asha Barbaschow. CyberCX eyes Australian government with Foresight acquisition // ZDNet (https://www.zdnet.com/article/cybercx-eyes-australian-government-with-foresight-acquisition/). 09.12.2020).***

***

«Google создал новый сайт для отслеживания межсайтовых утечек, предупреждая, что эти типы недостатков используются некоторыми сайтами для кражи информации о пользователе или его данных в других веб-приложениях.

Новая вики включает информацию о принципах межсайтовых утечек, распространенных атаках и предлагает механизмы защиты, чтобы остановить эти атаки.

«Все чаще проблемы безопасности, обнаруживаемые в современных веб-приложениях, зависят от неправильного использования давних моделей поведения веб-платформ, что позволяет сомнительным сайтам раскрывать информацию о пользователе или их данных в других веб-приложениях. Этот класс проблем, широко называемый перекрестным "утечки сайтов" (XS-Leaks) создают интересные проблемы для инженеров безопасности и разработчиков веб-браузеров из-за разнообразия атак и сложности построения комплексной защиты", - сказал Google.

В вики объясняется, что XSLeaks «представляют собой класс уязвимостей, производных от побочных каналов, встроенных в веб-платформу».

«Они пользуются преимуществом основного принципа веб-компоновки, который позволяет веб-сайтам взаимодействовать друг с другом, и злоупотребляют законными механизмами для получения информации о пользователе», - поясняет вики.

«Принцип XS-Leak заключается в использовании таких побочных каналов, доступных в Интернете, для раскрытия конфиденциальной информации о пользователях, такой как их данные в других веб-приложениях, сведения об их локальной среде или внутренних сетях, к которым они подключены».

Хотя такие уязвимости обычно не рассматриваются как серьезные недостатки, они также очень распространены и могут использоваться в качестве стартовой площадки для более сложных и вредоносных атак.

Google работает над XSS-уязвимостями вместе с внешними исследователями безопасности с 2010 года, предоставляя вознаграждение за обнаружение ошибок для веб-сайтов Google, включая Google и YouTube. Раньше у Google была функция в Chrome под названием XSS Auditor, которая сканировала исходный код веб-сайта на наличие признаков атак с использованием межсайтовых сценариев в браузере пользователя. Однако в прошлом году он удалил XSS Auditor, обнаружив, что сам внес слишком много утечек XS.

В вики рассматриваются типы атак и предлагается обзор функций безопасности, которые могут предотвратить или смягчить их.

В нем также подробно описывается, как разработчики веб-браузеров могут использовать новые функции безопасности браузера, такие как получение заголовков запросов метаданных, отправляемых браузерами с запросами HTTPS, чтобы предоставить контекст о том, как был инициирован запрос. Это позволяет приложениям принимать более обоснованные решения о том, как на них реагировать.

Другие средства защиты включают в себя кросс-Origin открывалка политики, Cross-Origin Policy Resource и SameSite печенье». ***(Liam Tung. Google: These new data-leaking website attacks are a growing menace // ZDNet (https://www.zdnet.com/article/google-these-new-data-leaking-website-attacks-are-a-growing-menace/). 07.12.2020).***

***

«Евгений Касперский объявил о предстоящем в 2021 году выпуске смартфонов под собственным брендом. Гаджеты будут оснащены новой ОС, которая обеспечит пользователей защитой от хакерских атак.

Установкой "операционки" и производством будет заниматься китайская корпорация. Глава "Лаборатории Касперского" отметил, что новая ОС не является конкурентом для Apple и Google. Специальная операционная система будет необходима для предприятий и государственных служащих. Основной задачей компании является создание телефона, который невозможно будет "взломать". "Лаборатория Касперского" уже имеет 20-30 "пилотов" не только в России, но и в Азии, Европе и странах СНГ. Система будет полностью готова для смартфонов в 2021 году.

В связи с таким назначением смартфона, на нем не будет каких-либо дополнительных функций, кроме стандартных приложений ии браузера. По признанию Касперского, он мечтает, чтобы гаджет использовался даже для управления турбиной электростанции.

Наличие магазина приложений на такой ОС пока не предполагается. "Пока мы не предполагаем, что у нас будет какой-либо AppStore, но в будущем должно появиться нечто похожее. Скорее всего, сначала мы сделаем свой, а потом готовы будем привлекать и другие магазины приложений. Мы понимаем, что без большой экосистемы этот проект не взлетит, поэтому мы готовы будем привлекать партнеров", - добавил он.» ***(«Лаборатории Касперского» готовит к выходу новые смартфоны с антихакерской операционной системой // SecurityLab.ru (https://www.securitylab.ru/news/514644.php). 08.12.2020).***

***

«Джерела повідомили про плани Microsoft відмовитися від паролів в своїх продуктах. Компанія вже давно говорить про небезпеку такого виду аутентифікації.

Якщо вірити ЗМІ, клієнти Microsoft зможуть перестати використовувати паролі вже в 2021 році. За інформацією джерела, компанія працює над створенням нових API і призначеного для користувача інтерфейсу. Вони будуть використовуватися для управління особливими ключами безпеки на основі стандарту FIDO2.

Також Microsoft розробляє такий собі «конвергентний портал реєстрації», який клієнти використовували б для контролю цих ключів безпеки. Для користувача такий спосіб аутентифікації повинен бути навіть простіше – не потрібно вводити ім’я користувача або пароль.

У Microsoft говорять, що майже 80% кібератак на меті мають крадіжку пароля. Тому потрібно щось з цим робити». ***(Митник Михайло. Microsoft планує відмовитися від паролів в своїх програмах // TechnoPortal.com.ua (https://technoportal.com.ua/smartfony/56984). 19.12.2020).***

***

«Компания Darktrace, занимающаяся кибербезопасностью, лучше других разбирается в методах цифровых атак. Его уникальный подход,

основанный на искусственном интеллекте, возник в результате работы бывших шпионов правительственных спецслужб и математиков из Кембриджского университета.

Благодаря 4000 организаций, полагающихся на ее технологии, Darktrace смогла выявить некоторые заметные закономерности в современном ландшафте угроз. Невозможно игнорировать одну тенденцию: злоумышленники все чаще атакуют компании через их самый непредсказуемый актив: их людей. В частности, они обращаются к электронной почте, чтобы получить первую ногу в дверь. Действительно, 94% кибератак исходят из почтовых ящиков. Приняв образ мышления злоумышленника, мы можем начать понимать, почему электронная почта предлагает самый простой путь проникновения и почему они будут продолжать использовать папку «Входящие» в качестве плацдарма для своих атак в 2021 году.

Мотив

По мнению экспертов Darktrace, злоумышленники будут штурмовать вашу защиту по ряду причин. Хакеры стремятся обыскать вашу цифровую среду в поисках секретов. Промышленный шпионаж - это быстро развивающийся бизнес, и талантливые хакеры всегда ищут интеллектуальную собственность. ИС - это лишь одна из форм экономической выгоды. Организованные киберпреступники часто используют более прямой подход: либо воруют активы, которые они могут конвертировать в наличные, либо просто крадут деньги напрямую.

Данные кредитной карты клиента приносят значительную прибыль онлайн, как и учетные данные. В качестве альтернативы мошенники, занимающиеся компрометацией корпоративной электронной почты (BEC), ведут здоровый бизнес, убеждая тех, кто отвечает за кошельки компании, отправлять деньги на мошеннические счета.

Некоторые награды носят чисто эгоистический характер. Взлом компаний исключительно для лулзов - это постоянный цифровой спорт для некоторых, в то время как некоторые выбирают более идеологический путь. Хактивисты по-прежнему регулярно разоряют сети.

Все началось с фишинга, никогда не думал, что до этого дойдет. Как многие из этих людей проникают в свои цели? Обычно он начинается с фишинг-атаки, целью которой является кража учетных данных получателя, чтобы хакер мог взломать его учетную запись.

Получение доступа к чьим-либо учетным данным предлагает точку опоры в инфраструктуре компании, наряду с большим количеством конфиденциальных данных, скрытых в учетной записи электронной почты жертвы. Контракты, бизнес-планы, данные о ценах и списки контактов - все это богатые ресурсы для воров.

Эти учетные данные также могут разблокировать общие корпоративные ресурсы. Сотрудники, использующие одни и те же учетные данные для нескольких систем, увеличивают ущерб. Поскольку только треть всех компаний применяет многофакторную аутентификацию, риски высоки.

Злоумышленники часто наносят вторичные удары, отправляя фишинговые письма из захваченных почтовых ящиков. Кто бы не поверил электронному письму, пришедшему из аккаунта доверенного коллеги? Этот этап позволяет

злоумышленникам украсть еще больше учетных данных у других жертв, установить программы-вымогатели или запустить особенно убедительную атаку BEC.

Подпитываемое страхом мошенничество

Для злоумышленника все зависит от того, первая жертва откроет это электронное письмо и воспользуется приманкой. Большинство людей считают себя рациональными игроками, которые никогда бы не попались на фишинговую аферу - пока они этого не сделают.

Причина тут ни при чем. Хорошие злоумышленники - это эксперты в методах социальной инженерии, отточенные, чтобы полностью обойти ваш рациональный мозг. Они используют общие психологические триггеры, которые напрямую обращаются к эмоциям жертвы.

Преступники хорошо разбираются в атаках социальной инженерии. Они годами извлекают выгоду из стихийных бедствий в новостях, эксплуатируя сочувствие и заботу людей в поддельных благотворительных акциях.

Страх - еще один распространенный эмоциональный триггер, потому что он очень хорошо работает. Киберпреступники используют его в качестве основы для успешных кампаний в концепции, которую Darktrace называет программным обеспечением страха. Вот почему пандемия COVID-19 была такой находкой для злоумышленников.

Когда пандемия только разразилась, дезинформация была распространена. Люди были неуверены и боялись последствий болезни. Преступники предлагали утешение через сайты, которые собирали учетные данные в обмен на поддельную информацию о вирусе. Когда люди начали лучше справляться с пандемией, эти сайты превратились в предложения фальшивых стимулирующих фондов и информацию об экономическом восстановлении.

Воры делают домашнее задание

Интернет-преступники обостряют свои атаки с помощью исследований, часто через социальные сети, но также с использованием публичных записей и веб-сайтов компаний. Злоумышленники используют эту информацию, чтобы узнать, с кем общаются жертвы, как они разговаривают, каково их чувство юмора и какой информацией они делятся. Эти идеи могут иметь неоценимое значение при нацеливании на друзей и коллег человека с помощью надежных электронных писем, имитирующих голос человека в сети.

Этот вид исследования требует больше усилий (хотя текущие разработки методов разведки ИИ могут это изменить). Злоумышленники часто хеджируют свои ставки, заходя как широко, так и глубоко. Они дополняют свои вложения в особо ценные цели массовым фишингом.

В первые дни фишинга масштабные злоумышленники были сплошь и рядом, но злоумышленники совершенствуют свои методы, используя те же инструменты и методы, которые профессиональные маркетологи электронной почты используют для увеличения открываемости писем. A / B-тестирование больше не предназначено только для маркетинговых агентств.

Игра в доменную игру

Для масштабного фишинга злоумышленники также используют метод, известный как массовая регистрация доменов. В этой доменной игре преступники могут регистрировать дешевые домены, заказывая их оптом. Это дает им большой выбор доменов на выбор, что делает их кампании более гибкими. Они регистрируют домены, относящиеся к определенной теме, переключая их в ответ на появляющиеся новости. Отчасти поэтому мы увидели, что покупка новых доменов, связанных с COVID, резко возросла на ранней стадии пандемии. Поскольку злоумышленники становятся все более изощренными, пришло время изменить наши представления о защите самих себя. Обучение осведомленности о кибербезопасности всегда будет полезно, но одного его недостаточно, чтобы предотвратить все атаки социальной инженерии.

Компаниям нужны дополнительные уровни защиты, чтобы увеличить свои шансы остановить атаки, но обычные средства защиты от фишинга не работают. Например, во время одной из недавних атак на электронную почту, которую обнаружил Darktrace, фишинговое письмо незаметно прошло через шлюз безопасности электронной почты Mimecast.

Электронное письмо перенаправляло получателей на поддельную страницу входа в Microsoft 365. Злоумышленник использовал сайт, чтобы собрать учетные данные жертвы и получить доступ к их учетной записи. Затем злоумышленник использовал захваченную учетную запись, чтобы сделать несколько закрытых ресурсов, включая файлы паролей и информацию о кредитных картах, общедоступными. Получив эти данные, они продолжили атаку, используя украденную учетную запись, чтобы отправить более 1600 фишинговых писем за 25 минут.

Antigena Email от Darktrace выявляет подобные атаки, выходя за рамки традиционных цифровых подписей и черных списков доменов, которые так часто не работают в устаревших инструментах. Вместо этого он использовал сочетание контролируемых и неконтролируемых методов машинного обучения для анализа более широкого контекста электронной почты. Он смог обнаружить необычные шаблоны общения, а также ссылку, к которой раньше никто в компании не переходил.

Обещание ИИ

Сканируя одновременно сотни точек данных, ИИ составляет «оценку аномалий» для электронного письма. Эти точки данных содержат нюансы, охватывающие все: от того, содержит ли электронное письмо файлы (и как они выглядят), до истории сообщений отправителя и получателя. Antigena даже улавливает попытки вымогательства и выявляет «скрытые ссылки», содержащиеся в электронных письмах за кнопками или изображениями.

Этот инструмент воплощает в себе три ключевых принципа ИИ как технологии киберзащиты:

AI имеет нюансы

Обычные инструменты классифицируют электронные письма как хорошие или плохие. Этот бинарный подход слишком упрощен. ИИ идет глубже, используя свое широкое контекстное понимание для оценки различных проблем с электронной почтой и принятия соответствующих мер.

Хотя Antigena может удерживать одно электронное письмо, содержащее известные вредоносные ссылки, оно может пропускать другое электронное письмо, отключая макрос во вложенном файле или запрещая гиперссылку. В других случаях он пропустит письмо, но пометит его как потенциальную подделку. Это обеспечивает точную и надежную защиту, позволяя бизнесу работать в обычном режиме.

ИИ постоянно уточняет свое понимание

Даже если бы люди могли сформулировать нормы общения, эти тенденции со временем меняются по мере того, как сотрудники приходят и уходят. ИИ поддерживает актуальную картину того, как люди обычно общаются, постоянно отслеживая и извлекая уроки из новых писем.

ИИ создан для облака

Antigena поддерживает этот детализированный, самообучающийся подход с архитектурой, которая отслеживает электронную почту без изменения существующей инфраструктуры электронной почты. Вместо использования записей MX он использует ведение журнала для чтения электронных писем и API для принятия мер. Это позволяет ему защищать пользователей, не изменяя поток электронной почты и не превращаясь в единую точку отказа. Этот режим работы также упрощает установку Antigena. Настройка правила ведения журнала API занимает пять минут, а системе требуется от семи до 10 дней, чтобы узнать контекст из электронной почты организации.

Преступники расширили свои операции, чтобы воспользоваться пандемией, и маловероятно, что они сократятся. По мере того, как улучшаются их методы, растет и их прибыль. Крупномасштабные атаки и хирургический целевой фишинг приносят значительные финансовые выгоды. Организации должны адаптироваться, чтобы справиться с этой трансформирующейся угрозой. Это означает принятие новых сценариев, новых технологий и новых инструментов…» ***(Robin Birtstone. How cyber-attackers are coming after you in 2021// The Register (https://www.theregister.com/2020/12/17/attackers_are_coming_in_2021/). 17.12.2020).***

***

«Лаборатория Касперского» представила решение Kaspersky Threat Attribution Engine. Это новый защитный продукт, предназначенный для корпораций и государственных ведомств, которые хотели бы понять, кто стоит за атаками на их ресурсы. Инструмент помогает аналитикам SOC-команд и сотрудникам отделов по реагированию на киберинциденты сопоставлять новые вредоносные операции с уже известными, эффективно определять источники и организаторов.

Чтобы выяснить, от какой именно кибергруппы исходит угроза, решение Kaspersky Threat Attribution Engine разбирает обнаруженный образец вредоносного кода на отдельные фрагменты, а затем ищет сходства в базе «Лаборатории Касперского». Эта информация помогает экспертам по кибербезопасности приоритизировать угрозы по степени риска, выделять наиболее серьезные из них и вовремя принимать защитные меры.

Зная, кто и с какой целью атакует компанию, сотрудники отделов по кибербезопасности могут быстро разработать и запустить план по реагированию на киберинцидент. Однако определение авторства — это сложная задача, для решения которой требуется не только большой объем информации о ранее происходивших инцидентах, но и умение ее интерпретировать. Новый инструмент позволяет автоматизировать процесс классификации и распознавания сложного вредоносного ПО.

В зависимости от того, насколько анализируемый файл похож на образцы, хранящиеся в базе, решение Kaspersky Threat Attribution Engine определяет возможное происхождение и кибергруппу, стоящую за атакой, дает короткое описание и ссылки на частные и публичные ресурсы с информацией о кампаниях, где был задействован сходный код. Подписчикам Kaspersky APT Intelligence Reporting доступен также подробный отчет о тактиках, техниках и процедурах, используемых кибергруппой, и инструкция, как действовать дальше.

В основу решения лег внутренний инструмент, используемый командой GReAT. В частности, с его помощью изучались iOS-имплант LightSpy, TajMahal, ShadowHammer и Dtrack. Одно из наиболее свежих расследований, для которого применялся Kaspersky Threat Attribution Engine, — кампания кибершпионажа CactusPete, направленная на финансовые и военные организации в Восточной Европе. В период с марта 2019 г. по апрель 2020 г. эксперты обнаружили 300 относящихся к ней вредоносных образцов.

Решение Kaspersky Threat Attribution Engine может быть развернуто в сети клиента, также в 2021 г. станет доступно развертывание в сторонней облачной сети. Кроме того, оно может быть использовано для создания собственной базы и заполнения ее вредоносными образцами, которые находят аналитики компании-заказчика.

«Есть разные способы определять, кто именно стоит за атакой. Например, аналитики могут находить во вредоносном коде некие артефакты, которые указывают на язык, на котором говорят атакующие, или IP-адреса, позволяющие предположить их местонахождение. Однако продвинутые кибергруппы могут подделывать такого рода данные и направлять исследователя по ложному следу — это происходит довольно часто. Наш опыт показывает, что лучший способ — искать сходные фрагменты кода с теми, что использовались ранее в других кампаниях. К сожалению, если делать это вручную, то на это могут уходить дни и даже месяцы. Чтобы автоматизировать и ускорить процесс, мы создали Kaspersky Threat Attribution Engine», — сказал Сергей Новиков, заместитель руководителя глобального центра исследований и анализа угроз». ***(«Лаборатория Касперского» выпустила инструмент для определения авторов кибератак // CNews (https://safe.cnews.ru/news/line/2020-12-14_laboratoriya_kasperskogo). 14.12.2020).***

***

«Европол и Европейская комиссия запустили новую платформу дешифрования, которая поможет расширить возможности Европола по получению доступа к информации, хранящейся на зашифрованных носителях, собранной в ходе уголовных расследований.

Новая платформа дешифрования, управляемая Европейским центром киберпреступности (EC3) Европола, была разработана в сотрудничестве со службой науки и знаний Объединенного исследовательского центра Европейской комиссии.

Это знаменует собой «веху в борьбе с организованной преступностью и терроризмом в Европе», согласно Агентству ЕС по сотрудничеству в правоохранительной сфере.

Европейский центр киберпреступности (EC3) Европола - орган Управления полиции ЕС, занимающийся киберпреступлениями, совершаемыми организованными преступными группами, - это организация, которая будет управлять этой платформой и будет оказывать поддержку и экспертные знания национальным расследованиям государств-членов.

«Сегодня знаменует конец трехлетнего пути», - заявила исполнительный директор Европола Катрин Де Болле в опубликованном сегодня пресс-релизе.

«Мы сделали значительный шаг вперед в борьбе с преступным злоупотреблением шифрованием с целью обеспечения безопасности нашего общества и граждан при полном соблюдении основных прав».

Несмотря на то, что в сегодняшнем пресс-релизе не содержится никаких подробностей о новой платформе дешифрования, отчет Совета Европейского Союза [PDF] затемняет.

Согласно отчету, платформа дешифрования Европола включает в себя как программные, так и аппаратные средства, которые должны помочь правоохранительным органам расшифровать информацию, законно полученную в ходе уголовных расследований.

Как поясняется в отчете:

Государства-члены должны инвестировать в специализированное оборудование и программное обеспечение с адекватными вычислительными возможностями и в персонал, прошедший соответствующую подготовку, чтобы обеспечить дешифрование даже в сложных случаях зашифрованных файлов и сообщений.

Государства-члены должны обеспечить сотрудничество между всеми соответствующими заинтересованными сторонами, включая, где это уместно, частные компании, с целью повышения возможностей дешифрования компетентных органов.

Государства-члены должны активизировать исследования и разработки с целью разработки новых и более эффективных методов дешифрования и использовать возможности Европола, а именно платформу дешифрования European Cybercrime Center (EC-3) для более сложных случаев шифрования.

«При полном соблюдении основных прав и без ограничения или ослабления шифрования, эта инициатива будет доступна национальным правоохранительным органам всех государств-членов, чтобы помочь обеспечить безопасность общества и граждан», - добавил Европол.

В понедельник Совет издал необязательную в юридическом отношении резолюцию «Безопасность посредством шифрования и безопасность несмотря на шифрование».

В резолюции подчеркивается поддержка Советом «разработки, внедрения и использования надежного шифрования как необходимого средства защиты основных прав и цифровой безопасности граждан, правительств, промышленности и общества».

В нем также подчеркивается «необходимость обеспечения того, чтобы компетентные правоохранительные и судебные органы могли осуществлять свои законные полномочия, как онлайн, так и офлайн, для защиты наших обществ и граждан».

«Возможные технические решения должны будут уважать неприкосновенность частной жизни и основные права, а также сохранять ценность, которую технологический прогресс приносит обществу», - добавил Совет». ***(Sergiu Gatlan. Europol launches new decryption platform for law enforcement // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/europol-launches-new-decryption-platform-for-law-enforcement/). 18.12.2020).***

***

«Агентство по кибербезопасности и безопасности инфраструктуры (CISA) выпустило инструмент на основе PowerShell, который помогает обнаруживать потенциально скомпрометированные приложения и учетные записи в средах Azure / Microsoft 365.

Это произошло после того, как Microsoft раскрыла, как украденные учетные данные и токены доступа активно используются злоумышленниками для нацеливания на клиентов Azure .

Администраторам Azure настоятельно рекомендуется просмотреть обе эти статьи, чтобы узнать больше об этих атаках и узнать, как определить аномальное поведение в своих клиентах.

«CISA создала бесплатный инструмент для обнаружения необычной и потенциально вредоносной активности, которая угрожает пользователям и приложениям в среде Azure / Microsoft O365», - заявило федеральное агентство США .

«Инструмент предназначен для использования специалистами по реагированию на инциденты и в узком смысле сосредоточен на деятельности, которая характерна для недавних атак на основе идентификации и аутентификации, наблюдаемых во многих секторах».

Как работает инструмент CISA

Инструмент на основе PowerShell, созданный командой CISA Cloud Forensics и получивший название Sparrow, может использоваться для сужения больших наборов модулей расследования и телеметрии «до тех, которые относятся к недавним атакам на источники федеративной идентификации и приложения».

Sparrow проверяет единый журнал аудита Azure / M365 на наличие индикаторов взлома (IoC), перечисляет домены Azure AD и проверяет субъектов-служб Azure и их разрешения Microsoft Graph API, чтобы обнаружить потенциальную вредоносную активность.

Полный список проверок, которые он выполняет после запуска на анализирующей машине, включает:

Выполняет поиск любых изменений в настройках домена и федерации в домене клиента.

Выполняет поиск любых модификаций или изменений учетных данных в приложении

Выполняет поиск любых модификаций или изменений учетных данных субъекта-службы.

Выполняет поиск любых назначений ролей приложения для субъектов-служб, пользователей и групп.

Поиск любых разрешений OAuth или приложений

Выполняет поиск аномалии использования токена SAML (UserAuthenticationValue of 16457) в единых журналах аудита.

Ищет логины PowerShell в почтовых ящиках

Ищет известный AppID для Exchange Online PowerShell

Ищет известный AppID для PowerShell

Ищет AppID, чтобы узнать, получал ли он доступ к почтовым сообщениям

Ищет AppID, чтобы узнать, получил ли он доступ к элементам Sharepoint или OneDrive

Ищет строку агента пользователя WinRM у пользователя, вошедшего в систему, и неудачные операции входа пользователя

Бесплатный инструмент безопасности Azure также выпущен CrowdStrike

Фирма по кибербезопасности CrowdStrike выпустила аналогичный инструмент обнаружения после расследования неудавшегося взлома после получения предупреждения от Microsoft о том, что скомпрометированная учетная запись реселлера Microsoft Azure попыталась прочитать электронные письма компании с использованием скомпрометированных учетных данных Azure.

После анализа внутренней и производственной среды после взлома SolarWinds, CrowdStrike заявила на прошлой неделе, что не обнаружила никаких доказательств того, что на нее повлияла атака на цепочку поставок.

Тем не менее, второе расследование было начато после предупреждения Microsoft, которое поступило, когда Crowdstrike искал IOC, связанные с хакерами SolarWinds в их среде.

Проанализировав среду Azure и не обнаружив никаких доказательств компрометации, Crowdstrike также обнаружил, что инструменты администрирования Azure «особенно сложны» в использовании.

Чтобы помочь администраторам проанализировать свои среды Azure и получить более простой обзор того, какие права предоставлены сторонним торговым посредникам и партнерам, CrowdStrike выпустила бесплатный инструмент CrowdStrike Reporting Tool для Azure (CRT).» ***(Sergiu Gatlan. CISA releases Azure, Microsoft 365 malicious activity detection tool // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/cisa-releases-azure-microsoft-365-malicious-activity-detection-tool/). 28.12.2020).***

***

«Запечатанная нацистская машина будет реставрирована.

Немецкие водолазы из экологической группы Всемирного фонда дикой природы искали на дне океана брошенные сети, угрожающие морской дикой природе. Вместо этого они обнаружили бесценный образец компьютерной истории, немецкую крипто-машину Enigma времен Второй мировой войны, затонувшую на дно Балтийского моря, чтобы защитить свою драгоценную технологию от войск союзников.

Разработка машины Enigma Cipher и гонка не на жизнь, а на смерть за взлом ее кода не только важны для решения исхода Второй мировой войны; он возвестил о наступлении современной компьютерной эры. И поскольку секретный код Энигмы был охраняемым немецким секретом, когда к нам подошли силы союзников, вооруженным силам было приказано уничтожить их, оставив в живых только 320 из них из более чем 25000, построенных для немецкой армии с 1929 года до конца прошлого года. Вторая мировая война, по словам Дэна Переры, директора музея Enigma.

Ценность загадки

Сегодня эти машины пользуются большим спросом у правительств, музеев и частных коллекционеров, сказал Перера Threatpost. Он добавил, что машины Enigma были проданы на аукционе по цене от 190 000 до 270 000 долларов.

Команда дайверов WWF обыскивала залив Мерин в Балтийском море между Германией и Данией в поисках того, что они называют «призрачными сетями», рыболовным устройством, которое зацепляется за что-то на морском дне, нанося вред морской жизни, объяснила компания Sophos Security. Одна сеть-призрак, которую они нашли, была зацеплена чем-то, что ведущий ныряльщик Флориан Хубер назвал своим коллегой «старой пишущей машинкой».

Хубер сказал, что Enigma, вероятно, находилась на борту одной из 40 подводных лодок, затопленных в бухте ВМС Германии в конце Второй мировой войны. «Мы предполагаем, что наша Enigma вышла за борт в ходе событий», - сказал он Sophos.

Энигма была передана Государственному археологическому бюро в земле Шлезвиг-Гольштейн, где она будет реставрирована. В отчете Naked Security говорится, что его первая остановка - еще один год под водой в дистиллированной воде, чтобы смыть соль с устройства.

«Историки в целом согласны с тем, что чтение секретных сообщений, отправленных немцами с помощью машин Enigma, сократило войну как минимум на два года, спасло тысячи жизней и лишило немцев времени, необходимого для разработки атомной бомбы», - сказал Перера.

Союзники, пытаясь взломать секретный код Энигмы, также раздвинули технологические границы.

«Машина Enigma помогла зародить компьютерную эру», - сказал Перера. «Первые работающие компьютеры были разработаны в рамках усилий союзников по взлому кодов Enigma и кодов других немецких шифровальных машин во время Второй мировой войны».

Наследие кибербезопасности Тьюринга

Алан Тьюринг, отец современных вычислений, изобрел компьютер для взлома кода Enigma в 1942 году и вдохновил поколения криптографов взяться за его работу.

«Эта недавно обнаруженная Enigma - захватывающая часть военной и разведывательной истории», - сказал Threatpost Рок Холланд, офицер безопасности и вице-президент по стратегии Digital Shadows. «Необходимость взломать код Enigma привела к криптоанализу и, в конечном итоге, к современному анализу сигналов. Алан Тьюринг и его коллеги в историческом Блетчли-парке помогли переломить ход Второй мировой войны. Штаб-квартира правительства Великобритании по связям с общественностью (GCHQ) и происхождение Агентства национальной безопасности (АНБ) можно проследить до этих шифровальных устройств ».

Тернинг и его команда взломщиков кодов в Блетчли-Парке тайно работали над взломом кода Enigma, опираясь на ранние работы польских математиков. Вооружившись кодом, Тьюринг в конечном итоге разработал свой собственный компьютер Bombe. . По данным British Times, в разгар войны было построено 211 бомбардировщиков, способных обрабатывать 3000 немецких сообщений в день.

Бомба была электромеханическим устройством, состоящим из 36 отдельных машин Энигмы. Каждую отдельную Enigma можно запрограммировать так, чтобы она принимала назначенные буквы и имитировала 17 500 переменных позиций шифратора до тех пор, пока не будет найдено совпадение, сообщает BT.

«За последние два столетия редко встречаются истории, которые оказали большее влияние на современные технологии и на то, как общество воспринимает их и их главных героев, чем эта», - сказал Threatpost Дик Шрейдер, глобальный вице-президент New Net Technologies, о наследии Тьюринга. что нынешние профессионалы в области безопасности все еще ведут те же битвы за шифрование, как Тьюринг против Enigma во время войны.

«Использование программируемого устройства для выполнения тяжелой работы с математическими операциями, несомненно, можно рассматривать как первую отличительную черту вычислений в современной истории», - сказал Шредер. «Сегодня кибербезопасность часто сталкивается с теми же проблемами, просто нашими противниками обычно являются не страны (и войны нет), но мы здесь и прилагаем все усилия для поиска технологических решений проблем, вызванных тем же самым технология, используемая злоумышленниками». **(Becky Bracken. Divers Pull Rare Surviving WWII Enigma Cipher Machine from Bottom of the Baltic // Threatpost (https://threatpost.com/divers-wwii-enigma-cipher-baltic/162045/). 08.12.2020).**

***

«По мере того, как криптология - изучение кодов - продолжает развиваться, а отрасль разрабатывает все более инновационные способы защиты связи, люди редко спрашивают: «Откуда все это взялось?» Как человек, увлеченный криптологией более 30 лет, я хотел бы поделиться своим

историческим взглядом на то, как развивалась криптология. И да, это началось с египетских монахов.

Криптология - это одновременно и наука, и искусство. Я определяю это как изучение кодов. Слово «криптология» происходит от греческих слов «криптос» (что означает скрытый) и «логос» (означает слово). На практике существует 2 подгруппы криптологии: криптография и криптоанализ. Криптография относится к созданию кода, а криптоанализ - к взлому кода.

Начало криптографии

Криптография - это метод использования кодов для обеспечения конфиденциальности сообщений. С самого начала письменного слова у человечества было желание хранить секреты. Самые ранние записанные секреты принадлежали египетским монахам примерно с 1900 года до нашей эры. Эти монахи разработали фотокриптографическую систему с использованием нестандартных иероглифов, чтобы никто за пределами их ближайшего окружения не понимал, что передается.

Если вы не понимали иероглифические изображения, вы не могли понять сообщение. Однако, как и в случае с большинством примитивных методов, посторонние вскоре смогли взломать код, глядя на контекст отдельных изображений, и нестандартные иероглифы стало относительно легко расшифровать.

Введите шифр скитейлов

Следующая итерация древней криптографии произошла около 500 г. до н.э. с изобретением греческой скиталии. Это было ближе к настоящей криптологии, чем использование нестандартных иероглифов, потому что есть настоящий ключ. В скитале использовалось цилиндрическое основание, такое как палка или дубинка, обернутое по спирали кожаной или пергаментной полоской. Сообщение будет написано вдоль полосы. При отмотке от основания цилиндра полоска, казалось, не содержала ничего, кроме цепочки букв.

Для расшифровки сообщения потребовалось заново обернуть полоску вокруг основания цилиндра с точно таким же диаметром, что и диаметр, который использовался для создания сообщения, что позволило буквам выровняться в читаемое сообщение. Итак, с точки зрения криптографии, ключевым моментом был диаметр основания цилиндра.

Влияние розеттского камня

Примерно в 196 г. до н. Э. На свет появился Розеттский камень. Царь Птолемей V Епифан издал указ, который он хотел, чтобы все поняли. Он написал его на трех языках - древнеегипетских иероглифах, демотических письмах и древнегреческом - и положил все три на камень рядом друг с другом. Хотя Розеттский камень не был истинной криптологией, он предоставил ключ для перевода. Если бы вы знали один из языков, вы могли бы вернуться к пониманию двух других, ранее не поддающихся расшифровке языков.

Приветствую Шифр Цезаря

Около 50 г. до н.э. римский диктатор Юлий Цезарь хотел безопасный способ общения со своими полевыми генералами, поэтому он разработал буквенный сдвиг или шифр замены, который часто носит его имя. Шифр подстановки использует

сдвиг букв - сдвиг на 3 буквы так, чтобы «A» превратилось в «D», а «B» превратилось в «E», и так далее. Чтобы расшифровать сообщение, генералам нужно знать ключ или количество букв, которые нужно сдвинуть назад, чтобы получить текстовую версию сообщения. Итак, как Цезарь отправил ключ? Ходят слухи, что он вытатуировал ключ на бритой голове курьера. Затем, когда волосы посланника отрастут, ключа не будет видно.

Тем не менее, у этого типа шифрования были серьезные недостатки - учитывая 24 буквы греческого алфавита, можно было просто угадать до 25 раз, чтобы расшифровать сообщение. Кроме того, учитывая, что структура сообщения остается прежней, можно было бы сделать предположения на основе часто используемых букв (например, E - наиболее часто используемая буква в английском языке) и структуры слов, чтобы выявить шаблоны, позволяющие легко взломать код.

Геометрический шифр замещения - ранняя современная криптология

Шифр масонов, также называемый шифром свиной пены, появился примерно в 1700 году нашей эры. Он был назван шифром геометрической подстановки, потому что он сопоставлял геометрические формы с буквами в качестве ключа для кодирования и декодирования сообщения. Тамплиеры использовали вариант, основанный на геометрических фигурах Мальтийского креста, для передачи сообщений. Но этот метод криптологии также было довольно легко расшифровать, и ключ все равно необходимо было передать предполагаемым получателям.

Одноразовый блокнот обеспечивает настоящую секретность

Одноразовый блокнот (OTP) был изобретен примерно в 1882 году н.э. и стал популярен среди шпионов к концу Первой мировой войны в 1917 году. Были созданы два идентичных блокнота: один для человека, отправившего сообщение, а другой - для предполагаемого получателя. Блокноты содержали действительно случайные символы и использовали буквенный сдвиг на основе каждого символа в блокноте.

OTP по-прежнему остается единственным процессом шифрования, обеспечивающим настоящую секретность, но только при применении пяти правил. Он должен состоять из действительно случайных символов и иметь ту же или большую длину, что и открытый текст. Может быть только две копии OTP, и их можно использовать только один раз - обе копии должны быть уничтожены сразу после использования.

Даже при полной секретности одноразовые пароли создают уникальные проблемы. Как я только что упомянул, длина блокнота должна быть такой же или больше, чем длина зашифрованного сообщения. И OTP должен быть действительно случайными цифрами. Создание, распространение и хранение планшетов создает значительную нагрузку и накладные расходы, поэтому их внедрение в настоящее время не имеет смысла.

Электромеханическая криптология Enigma

Один из самых интригующих методов реализации криптографии в начале 1900-х годов назывался Enigma. Enigma была шифровальной машиной на основе ротора, которая берет свое начало в изобретениях из США, Швеции, Нидерландов и Германии. Это была первая система электромеханической криптографии, которая

широко использовалась Германией во время Второй мировой войны для шифрования сообщений для отправки своим военным.

В машине использовались роторы (колеса) и электрические контакты на правой и левой сторонах каждого ротора, которые создавали электрические цепи, используемые для передачи сообщений с буквенным шифрованием. Когда буква была напечатана, электрический ток проходил через ряд роторов, и на ламповой панели над клавиатурой загорелся свет. Оператор набирал сообщение, по одной букве за раз, и записывал светящуюся букву с панели лампы для зашифрованного сообщения. Некоторые модели Engima отделили панель лампы от клавиатуры, что сделало процесс шифрования и дешифрования задачей двух человек (один вводил сообщение, а другой, сидящий на противоположной стороне машины Engima, записывал указанные буквы с панели лампы).

Сложность заключалась в том, что пользователи должны были знать некоторые очень специфические настройки, чтобы сконфигурировать свою машину Engima для расшифровки сообщений: какие шифровальные колеса использовались, в каком порядке шифровальные колеса были вставлены на шпиндель, какова была начальная позиция для роторов, и какая конфигурация проводки коммутационной панели и отражателя. Тот факт, что эти детали приходилось доставлять каждый день, наряду с человеческими ошибками, привели к возможному взлому Engima, приписываемого работе Алана Тьюринга, одного из взломщиков кодов, работающего на британское правительство в Блетчли-парке. Тем не менее, по моему скромному мнению, это было одно из самых гениальных устройств механической криптологии, когда-либо созданных.

Хорошая конфиденциальность - начало современной криптологии

Pretty Good Privacy (PGP) возникла примерно в 1991 году как часть группы социальных / политических активистов, желающих конфиденциально общаться с единомышленниками в различных географических регионах. PGP использовала комбинацию симметричного шифрования (один ключ для шифрования и дешифрования) для шифрования сообщения и асимметричного шифрования (открытый ключ для шифрования и закрытый ключ для дешифрования) для защиты симметричного ключа. У пользователей были собственные связки ключей, содержащие открытые ключи людей, с которыми они хотели общаться. Со временем люди начали размещать свои связки ключей на общедоступных серверах и позволяли другим людям добавлять свои собственные открытые ключи в общие связки ключей.

Были созданы открытые ключи, и связки ключей стали общими для всех в группе. Если у кого-то есть свой открытый ключ, введенный в связку ключей, и у него есть свой закрытый ключ, он может расшифровать любые сообщения, зашифрованные с помощью своего открытого ключа из набора ключей. Но недостаток PGP обнаружился у ненадежных разработчиков, поскольку добавлялось больше людей и слоев без централизованного управления для определения доверия. К тому же PGP несовместим с развивающимся конкурирующим стандартом: S / MIME.

S / MIME для шифрования электронной почты и цифровой подписи

Конфиденциальность - это лишь один из вариантов использования криптографии. Как я уже говорил, шифрование позволяет нам гарантировать, что только те, у кого есть правильный ключ, смогут расшифровать сообщение. Но что, если вы хотите сделать больше, чем просто обеспечить конфиденциальность? Используя криптографию, мы также можем реализовать цифровые подписи. Это очень специфические криптографические функции, которые служат для подтверждения происхождения подписанного сообщения и подтверждения того, что сообщение сохранило свою целостность. Это просто причудливый способ сказать, что никто не изменил содержимое после применения цифровой подписи. Если мы объединим эти концепции, шифрование и цифровую подпись, у нас теперь есть основа для обеспечения защиты сообщений, которые могут быть доставлены в электронном виде другим людям.

Примерно в 1998 году S / MIME (RFC2311) стал стандартом для шифрования и цифровой подписи. Его встроенная интеграция с Microsoft и другими почтовыми клиентами, а не произвольная PGP, сделала его гораздо более привлекательным. Однако даже сегодня большинство организаций не шифруют свою электронную почту, хотя это относительно легко реализовать с помощью легко доступных решений. Тем не менее, существует более высокий уровень внедрения в таких отраслях, как здравоохранение и финансовые услуги, а также на некоторых государственных предприятиях, которым требуется строгая безопасность.

Подпись кода и мобильная аутентификация

Подпись кода вошла в мир в начале 2000-х годов, чтобы гарантировать целостность и происхождение драйверов и исполняемого кода. Подпись кода, как и подпись электронной почты, позволяет нам гарантировать, что программное обеспечение, которое мы запускаем на наших компьютерах и других подключенных устройствах, действительно принадлежит издателю, от которого мы ожидали, и что никто не менял программное обеспечение с момента его публикации.

Что касается использования криптографии для аутентификации, даже наши сотовые телефоны обладают достаточными криптографическими возможностями, чтобы они стали формой аутентификации. Благодаря цифровым сертификатам на основе криптографии на мобильных телефонах и другим формам аутентификации - отпечаткам пальцев, пин-кодам или паролям - наши мобильные устройства теперь являются средством аутентификации пользователей в системах.

Что ждет криптологию дальше?

Хотя криптология начиналась с очень примитивных средств защиты сообщений, прогресс, достигнутый нами с древних времен до наших дней, основывался на каждом нововведении. Новые темы криптологии включают Интернет вещей (IoT) с использованием долговечных встроенных сертификатов, распределенные реестры Blockchain и влияние квантовых вычислений на криптографические системы.

Я верю, что Интернет вещей и квантовые вычисления станут следующим этапом развития криптологии. Обеспечение безопасности по мере того, как к IoT подключается все больше устройств, будет иметь решающее значение для предотвращения мошенничества и кражи личных данных. Что касается квантовых

вычислений, предсказывается, что в течение следующих семи-десяти лет мы достигнем точки квантового превосходства. Это не очень долго. Пришло время приступить к разработке планов и подходов, чтобы определить, как мы будем передавать данные, зашифрованные с помощью старых алгоритмов, и ключевые материалы от старого к новому - или же нам следует начинать с нуля…» ***(Neal Fuerst. Who Should We Thank For Modern Cryptography? The Egyptian Monks // Entrust Corporation (https://blog.entrust.com/2020/12/who-should-we-thank-for-modern-cryptography-the-egyptian-monks/). 14.12.2020).***

***