**Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України»**
**Національна бібліотека України імені В. І. Вернадського**

# КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

## № 8 (серпень)

**Київ – 2021**

**Кібербезпека в інформаційному суспільстві:** Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2021.– №8 (серпень) . – 260 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.

© Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», 2021
© Національна бібліотека України імені В.І. Вернадського, 2021

# ЗМІСТ

Стан кібербезпеки в Україні ..... 4
Національна система кібербезпеки ..... 12
Правове забезпечення кібербезпеки в Україні ..... 14
Кібервійна проти України ..... 16
Боротьба з кіберзлочинністю в Україні ..... 17
Міжнародне співробітництво у галузі кібербезпеки ..... 20
Коронавірус COVID-19 та питання кібербезпеки ..... 27
Світові тенденції в галузі кібербезпеки ..... 30
Сполучені Штати Америки ..... 60
Китай ..... 69
Російська Федерація та країни ЄАЕС ..... 70
Австралія ..... 72
Інші країни ..... 73
Кібервійни та протидія зовнішній кібернетичній агресії ..... 78
Створення та функціонування кібервійськ ..... 86
Кіберзахист критичної інфраструктури ..... 86
Захист персональних даних ..... 87
Кібербезпека Інтернету речей ..... 121
Кіберзлочинність та кібертерроризм ..... 125
Діяльність хакерів та хакерські угруповування ..... 157
Вірусне та інше шкідливе програмне забезпечення ..... 162
Технічні аспекти кібербезпеки ..... 215
Виявлені вразливості технічних засобів та програмного забезпечення ..... 215
Технічні та програмні рішення для протидії кібернетичним загрозам ..... 248
Питання криптографії ..... 255

**«Компанії CyberLands та Cyber Unit Technologies, а також ряд галузевих експертів, випустили перше в Україні велике дослідження екосистеми кібербезпеки в Україні.** Обіцяють, що згодом оновлення проекту відбуватиметься щорічно…

Також упорядники дослідження готові доповнити його та удосконалити методологію, отримавши конструктивний зворотний зв'язок. Для цього можна написати на uace@cyberlands.io чи info@cyberunit.tech.

Протягом останніх 5-7 років сфера кібербезпеки сильно еволюціонувала в Україні через необхідність захищати країну від російської агресії і зайняла вагому частину поміж інших IT-секторів країни орієнтованих на експорт.

У цьому дослідженні, кібербезпека визначається як можливість витримувати кібератаки націлені на IT-інфраструктуру країни, в першу чергу забезпечуючи ефективне використання наявних контролів безпеки та впроваджуючи нові, тим самим роблячи сприяючи захищеності операційних процесів.

Операції з безпеки (cyber operations) матимуть успіх тільки за наявності широкої і продуктивної екосистеми – мережі, кадровий потенціал, капітал, технології і ефективна організація процесів. Екосистема формується інноваційними постачальниками послуг та сервісів, а також споживачами які мотивують прискорення розвитку кібербезпеки на рівні компаній і індустрії в цілому.

Наразі було виділено 96 відомих компаній, які є активними в екосистемі кібербезпеки України, є представниками освітніх інстанцій, приватного бізнесу, генераторами попиту (споживачі та донори).

Екосистема кібербезпеки була повністю перебудована за останні сім років. Зараз вона спрямована на експорт і, в основному, працює на клієнтів з США та ЄС, базується на можливостях 96 представлених суб'єктів.

Українська кіберекосисема сильна в:

Постачанні STEM (Science, Technology, Engineering and Mathematics) та кваліфікованих спеціалістів у кібербезпеці – більш ніж 2000 нових кадрів з`являється на ринку щороку.

Наданні всього спектру сервісів у кібербезпеці – пентест, консультування, постачання сервісів.

Приверненні уваги донорів поза межами країни.

Українській кіберекосисемі бракує:

Відповідного маректингового підходу та зусиль на ключових світових ринках – США, ЄС, Азіатсько-Тихоокеанський регіон, регіон Перської затоки.

Експертів з продажу та маркетингу заточених на кібербезпеку.

Об`ємного внутрішнього ринку.

Ключові тренди та фактори

Зростання внутрішнього ринку. Внутрішній ринок неухильно зростає завдяки чотирьом ключовим факторам.

По-перше, місцева економіка працює добре, щорічно демонструючи зростання або виступаючи краще, ніж очікувалося у 2020 році (під час пандемії).

По-друге, закон про децентралізацію бюджету (прийнятий у 2014 році) зміцнив міста та громади фінансово, зробивши міста вагомими споживачами у сфері кібербезпеки. Прикладом може слугувати виділення п’яти мільйонів доларів США Київської міської ради на проект реалізації SOC (Операційного центру безпеки).

По-третє, з’явилася група гравців на внутрішньому ринку – структури найвпливовішої місцевої бізнес-групи (ПрАТ «Систем Кепітал Менеджмент») почали модернізувати свої системи інформаційної безпеки, генеруючи десятки робочих місць та запускаючи різні проекти з кібербезпеки.

По-четверте, USAID як ключовий донор кібербезпеки оголосило про програму на 38 мільйонів доларів США для захисту інформаційних систем критичної інфраструктури країни.

Ми очікуємо подальшого росту місцевого ринку кібербезпеки не лише за рахунок попиту від донорів та ключових споживачів, але і за зростання потреб великого сектору розробки програмного забезпечення в Україні.

Зростання зовнішнього ринку. Зовнішні ринки сприятливі для українських сервісів у кібербезпеці – сім років тому не було MSSP (managed security service provider), лише кілька компаній спеціалізованих на пентестах, відсутність донорів та мінімальна кількість експортних послуг кібербезпеки. Сприятливими факторами стали поширення хмарних технологій та пандемія – безпека віддалених робочих навантажень може бути повністю забезпечена віддаленими українськими експертами, а також зростання української індустрії розробки програмного забезпечення (показник сукупного середньорічного темпу росту 53% 2016-2019).

Ми очікуємо експоненційного зростання для всіх послуг пов’язаних із безпекою хмарних техгологій, та сервісів, що можуть бути надані віддалено та в рамках певної авторитетної правової бази (більшість українських IT-компаній мають легальні представництва в ЄС, Великобританії та США)

Підігрів ринку талантів. Місцеві компанії щосили намагаються знайти кваліфікованих спеціалістів, оскільки експортно-орієнтовані IT-компанії можуть запропонувати більш високу заробітну плату. Різниця в зарплатах становить 50-100%, і означає, що для вирішення проблеми з`явиться попит на різні керовані послуги та освітні програми.

Розриття української кіберекосистеми

Категорії кібербезпеки

Ми поділили українську кіберекосистему на 6 основних категорій:

Бізнес.

Конференції.

Споживачі.

Донори.

Освітня діяльність.

Міжнародні асоціації.

Категорія «Бізнес»

IT-підприємства – це постачальники, які надають послуги чи продукти українським споживачам або експортують за кордон. Категорія бізнесу є найбільшою і розбивається на шість менших:

VAR (Value-added reseller) / дистриб'ютор.

Компанії зі спеціалізацією на пентесті.

SOCaaS (Security Operations Center as a Service).

Постачальники програмного забезпечення.

Консультанти.

Аутстафінг-компанії.

VAR та Дистриб'ютори – являються засобами імпорту технологій кібербезпеки, які допомагають захистити сучасні мережі, кінцеві точки, бази даних, програми та навіть промислові системи управління. Вони також надають споживачам постачальницькі професійні послуги, такі як підтримка та впровадження систем Cisco. Прикладами таких компаній є Softprom, Smartnet та Octava Cyber Defense.

Компанії зі спеціалізацією на пентесті представляють протилежний спосіб захисту корпоративних систем – замість впровадження додаткових засобів безпеки вони перевіряють стан безпеки конкретних програм та систем і пропонують зміни та покращення в уже наявних елементах контролю безпеки та основних технологічних стеках (Microsoft, RedHat, VmWare, Cisco тощо). Багато з них також зареєстровані за межами України, що полегшує ведення міжнародного бізнесу, хоча у них є команди управління, продажу та реалізації проектів. Прикладами компаній по пентесту є Pakurity та Octal Security.

Аутстафінг-компанії, надають персонал насамперед західним країнам (переважно США) у таких сферах, як безпека ПЗ, DevSecOps, а іноді й операційна безпека або управління доступом. Хоча їх основний бізнес розробка програмного забезпечення, їх можливості збуту зробили їх головною силою експорту в українській кіберекосистемі. Прикладами таких є Intellias, Svitla Systems та All-Stars IT.

На відміну від організацій, що займаються аутстафінгом, консультанти в першу чергу зосереджуються на наданні проектів у фіксованому об`ємі та часових параметрах, починаючи від компаній Big4, до спеціалізованих експертів-криміналістів та акредитованих фірм, які надають послуги з сертифікації ISO 27001 (єдиний глобально визнаний стандарт інформаційної безпеки). Прикладами являються Deloitte, DQS Ukraine та 10 Guards.

Постачальники ПЗ – це коріння ланцюжка утворення вартості технологій безпеки (програмного та апаратного забезпечення). Так звані продуктові компанії – як місцеві, так і філії міжнародних, розробляють та постачають на ринок програмне забезпечення для сфери кібербезпеки. Як і компанії по пентесту, вони часто реєструються за кордоном, уникаючи бюрократії, пов'язаної з валютним контролем, залучаючи фінансування та простіше виконуючи плани виходу на ринок. Приклади постачальників ПЗ для сфери кібербезпеки включають Cossack Labs та Hideez.

Послуги операційних центрів безпеки (SOCaaS), які часто називають постачальниками керованих послуг безпеки, є центрами, які об'єднують капітал, таланти, процеси та технології в керовані сервіси безпеки, щоб збільшити економіку за рахунок масштабу та зробити кіберможливості місцевого та іноземного бізнесу безпечними. Працюючи з такими навантаженнями, ризики,

пов'язані з капітальними вкладеннями в технології кібербезпеки, вмістом виявлення та процесами реагування, потребують найму, розвитку та утримання десятків фахівців із безпеки. Прикладами таких компаній являються IT Specialist, Octava Cyber Defense та SOC Prime.

*Категорія «Споживачі»*

Категорія Споживачів є рушійною силою, яка спрямовує місцевий ринок через свій попит. Оскільки на ринку України порівняно невелика кількість малого та середнього бізнесу, він формується кількома ключовими споживачами – це найбільші місцеві організації, такі як Київська міська рада, енергетичний гігант DTEK, міжнародна гральна компанія Parimatch. Ключові споживачі можуть бути великими покупцями технологій, великими роботодавцями (мають значну команду яка відповідає за безпеку операцій або внутрішній операційний центр безпеки) або двома відразу. Для цього дослідження ми поділили споживачів на найбільших публічних споживачів (5 суб'єктів) та найважливіших комерційних суб'єктів (15).

*Категорія «Донори»*

Категорія Донорів – це набір іноземних організацій, які підтримують стабільний розвиток української економіки за рахунок фінансування ініціатив, пов'язаних із кібербезпекою. Деякі з них – Агентство США з міжнародного розвитку (USAID), Державний департамент США (U.S. Department of State) та Організація з безпеки та співробітництва в Європі (OSCE).

*Категорія «Освітня діяльність»*

Освітня діяльність – це подвійна категорія, що складається з навчальних центрів (зазвичай приватних) та університетів (переважно державних). В Україні є кілька навчальних центрів із програмами по кібербезпеці (Академія STEP, CyberSchool тощо) та 52 університети, які навчають бакалаврів кібербезпеки. Ми обрали найважливіші з них — Київський національний університет, Київський політехнічний інститут, Львівський національний університет, Дніпровський, Львівський, Харківський та Одеський політехнічні університети.

*Інші категорії*

Конференції допомагають знайти нові можливості, вакансії та проекти для місцевих та міжнародних гравців української кібер-екосистеми. Прикладами є Bsides Ukraine, OWASP Ukraine та UISG Conference.

Міжнародні асоціації впроваджують у країну міжнародно визнані найкращі практики та фреймворки управління кібербезпекою; прикладами є OWASP Ukraine, Cloud Security Alliance (Lviv) та ISACA Kyiv Chapter.

*Методологія дослідження*

Дослідження мало на меті виявити суб'єкти, які роблять внесок у кіберекосистему України – надають капітал, кваліфікованих спеціалістів, технології, найкращі практики, послуги з формування екосистеми як ключових споживачів.

Ці організації позначаються як члени кіберекосистеми України і повинні відповідати чотирьом основним критеріям, щоб вважатися такими:

Вони мають працювати в Україні.

Відповідають одній із підкатегорій кібербезпеки.

Демонструють докази надання послуг або продуктів безпеки в межах категорії.

Є добре відомими в галузі.

Що це означає — працювати в Україні?

Щоб вважатися активною в Україні, компанія повинна мати штаб-квартиру в Україні, раду директорів, що проживає в Україні, або мати українських клієнтів, здатних розмовляти українською та надавати там послуги з кібербезпеки.

Прикладами є:

● Компанія A – обслуговує внутрішній ринок з легальною реєстрацією, керівництвом та основною командою в Україні.

● Компанія B – обслуговує світовий ринок разом із керівною групою та основною командою, які проживають в Україні, штаб-квартира в інших країнах з більш зручним бізнес-кліматом (зазвичай Естонія, Нідерланди, Сінгапур чи США).

● Компанія C – глобальна компанія з офісом в Україні, яка обслуговує українських клієнтів та має команду з продаж та\або персонал з реалізації в Україні.

● Компанія D – глобальна компанія, що використовує місцевий персонал для обслуговування міжнародної клієнтської бази.

Якщо чіткого повідомлення від компанії про її походження не було отримано, тоді переглядався її вебсайт – компанії, зареєстровані на міжнародному рівні, які мають вебсайт виключно на англійській мові, вважаються міжнародними, навіть якщо їх керівництво та служби доставки проживають в Україні.

Збір інформації та перевірка фактів

Було використано такі джерела для збору та перевірки інформації:

Найбільша у світі соціальна мережа для професіоналів LinkedIn.

Довідник постачальників з посиланнями Clutch.

Веб-сайти компаній.

Плани закупівель державних суб`єктів.

Інтерв'ю з членами спільноти кібербезпеки». ***(Илья Кабачинский. Як виглядає екосистема кібербезпеки України — перше велике дослідження // ain.ua (https://ain.ua/2021/08/10/yak-viglyada%d1%94-ekosistema-kiberbezpeki-ukra%d1%97ni/). 10.08.2021).***

***

**«В Україні діють продуктові та сервісні стартапи у галузі кібербезпеки. Десятьом з них вдалось потрапити до першої в Україні акселераційної програми від SocialBoost. AIN.UA розповідає, чим займаються стартапи і що таке «Кібеpакселератор».**

*Що таке «Кібеpакселератор»*

«Кібеpакселератор» — одна зі складових проекту USAID «Кібербезпека критично важливої інфраструктури України».

Випускникам програми обіцяють можливість доступу до Seed Grant Fund від USAID, загальний обсяг якого становить близько $3 млн, плюс допомогу в залученні інвестицій від партнерських фондів.

Найуспішніших випускників організатори також рекомендують до участі у Cyber Mentor / Protégé Program, яку проводить американська компанія VFI.

За словами представників акселератора, в межах програми українські технологічні МСБ компанії отримають наставництво від великих IT-компаній.

*Хто потрапив до «Кібераксеператора»*

Cyberlands B.V. – пропонує компаніям і корпораціям тиражовані і масштабовані пентести та аудити з кібербезпеки, формує і навчає команди, здатні проводити аудити безпеки. Спеціалізується на API & Mobile Security Assessment (iOS, Android), Kubernetes.

H-X Technologies – проводить аудити, впроваджує стандарти інформаційної безпеки, допомагає підтримувати їх виконання, працюючи з повним циклом процесу для промислової безпеки. Компанія пропонує своїм клієнтам Security Operations Services (SOC) по моделі SaaS.

Intelli Group – вибудовують та підтримують всі процеси в компанії клієнта, пов'язані з IT-складовою, звільняючи від потреби наймати в штат кількох фахівців з різною експертизою. Фокусується на роботі з малим та середнім бізнесом.

ITEXE – вихідці з фінансового сектору та fintech-бізнесу, тож пропонують безпекові послуги банкам, кредитним установам, страховим, брокерським компаніям, фондовим біржам, платіжним сервісам.

once.REST – працює над інструментами анонімізації даних та шифрування. Серед рішень, які пропонує команда, є зокрема протидія небажаним втручанням, доступна для клієнтів без спеціальної підготовки. Команда працює і в сегменті B2C.

Radar – відслідковує появу персональних даних користувача у даркнеті, аби якнайшвидше попередити про витік. Компанія сповіщає юзера, що дані скомпрометовано, та дає рекомендації щодо захисту: зміни паролів, блокування банківських карток тощо.

Sekurno — сервісна IT-компанія, яка працює з пентестами, security аудитом процесів та комплаєнсом з впровадженням міжнародних стандартів GDPR, ISO27001, ISO9001, SOC2, проводить консультацію та імплементацію процесів кібербезпеки у процес розробки, security operations support.

Security Steps – сервіс автоматизованого навчання, перевірки і моніторингу знань в сфері захисту від інформаційних атак.

Ukrainian Interbank Payment Systems Members Association EMA (Українська міжбанківська Асоціація членів платіжних систем ЄМА) – розвиває в межах акселераційної програми онлайн-сервіс відслідковування несанкціонованих платежів з web та API-інтерфейсами на базі Anti-Fraud HUB.

Unlink VR Inc. — інтегрована постквантова система шифрування. Будує захищені канали обміну інформації з використанням постквантової криптографії та принципів квантової фізики.

Наразі відібрані команди працюють над партнерствами, покращенням операційної ефективності та залученням додаткових ресурсів. Деталі про відбір на другу когорту учасників «Кіберакселарора» обіцяють повідомити згодом». ***(Татьяна Грицык. Що таке «Кібераксеператор» і хто у першому наборі // ain.ua (https://ain.ua/2021/08/03/kiberakselerator-pershyi-nabir/). 03.08.2021).***

***

**«З 24 серпня українські органи державної влади входять у режим paperless. Однак поступовий перехід на «безпаперову» робота почався ще 20 років тому.** Про те, як розвивається тенденція в Україні та світі, чи загрожує paperless персональним даним та як їх захистити, в ефірі Українського радіо розповів експерт з кібербезпеки Ігор Мальченюк.

«Ми, насправді, з Вами всі, користуємось різноманітними електронними послугами і маємо розуміти, що супроводження будь-якої електронної послуги чи електронної покупки, це – якийсь електронний документ. Питання в тому – наскільки активно і ефективно використовуються ці електронні документи наші державні агенції і органи влади», — відзначив експерт.

За його словами електронний документ юридично прирівняний до будь-якого паперового документа вже 20 років, що визначено законами "Про платіжні системи" 2001 року "Про електронні документи та електронний документообіг" 2004.

«Власне електронний документ має таку ж саму юридичну силу, як паперовий», - зазначив Мальченюк.

*Як paperless запроваджується у світі*

Він зазначив, що згідно з рейтингом ООН, яка вже 20 років досліджує стан використання різноманітних інструментів електронного врядування в різних країнах, за результатами 2020 року Україна на 69 місці.

«В лідерах є Данія, Південна Корея та Естонія. І, безперечно, на досвід цих країн можна і варто дивитись. Мені особисто імпонує Данія. Я особисто був в цій країні, там дуже цікава і тривала історія використання різноманітних електронних документів. Ще в 1972 році вони задумались як ефективніше використовувати інформаційно-комунікаційні технології, і створили муніципальну компанію, яка зараз надає, по суті, державні послуги, реалізовує цифрову адміністрацію, через «хмарні» послуги - компанія «КМД». Послугами користуються понад 75% муніципалітетів. І це – надзвичайно цікавий досвід. Сказати, що ми є попереду всього світу, то – так, в чомусь наші напрацювання є цікавими, але, нам є до чого рівнятись і куди розвиватись», — розповів експерт.

*Чи загрожує paperless особистим даним*

Що ж до захисту персональних даних, Мальченюк зазначив, що варто приділяти значну увагу питанню приватності.

«Це те, що не часто згадується і те, чому варто приділяти увагу. Ми, починаючи використовувати ці сервіси, мали б давати згоду на використання наших персональних даних і свідомо вибирати», — зазначив він.

Для порівняння, у західних країнах створені великі програми із захисту персональних даних та контролю їхнього використання.

«Слід розуміти, що якщо ще минулого року 10% населення мешкало в країнах, де є хоча б якесь законодавство, що захищає персональні дані, то до 2023 року вже 65% громадян будуть захищені, так чи інакше, законодавством, яке захищає персональні дані. Зразком у всьому світі є Європейська Директива щодо захисту персональних даних», — пояснив експерт.

Мальченюк підкреслив, що не можна говорити лише про державу як основного гравця в цій сфері. «В будь-якому випадку ми говоримо про державно-приватне партнерство - каже він, - саме в цій взаємодії, ми з вами можемо хоч щось зробити».

*Рекомендації щодо захисту персональних даних*

«Що стосується захисту, особливо в контексті в режимі «без паперових документів», це – електронні підписи. Іноді їх називають «кваліфікованими електронними підписами", саме в залежності від носія», — пояснив Мальченюк

За його словами, є різні типи носіїв для підпису. Зокрема, ключ або сертифікат свого можете зберігати на файловому носієві – звичайному USB-накопичувачі; на захищеному носієві – так званому «електронному ключі»; на сім-карті, наприклад, при використанні сервісу «Mobile ID» і на носієві в складі сервісу.

«Я особисто рекомендую використовувати різні захищені носії», — наголосив експерт». ***(Олександра Комісарова. Україна входить в режим "без паперових документів". Експерт пояснив, як захистити свої дані // АТ «НСТУ» (https://suspilne.media/154596-ukraina-vhodit-v-rezim-bez-paperovih-dokumentiv-ekspert-poasniv-ak-zahistiti-svoi-dani/). 10.08.2021).***

***

**«Міністерство цифрової трансформації презентувало освітній серіал «Обережно! Кібершахраї».**

Як повідомляє кореспондент Укрінформу, презентація серіалу відбулася 12 серпня.

Заступик міністра цифрової трансформації з питань євроінтеграції Валерія Іонан під час презентації розповіла, що в серіалі викладені чіткі алгоритми дій при втраті банківських даних або пристроїв, на яких така інформація зберігалася.

«Наші експерти моделюють ситуації, в яких відбувається втрата службової та приватної інформації, і розповідають, як діяти в кожній з них. Глядач дізнається, як діяти у разі крадіжки фінансового номера, втрати мобільного пристрою чи цілеспрямованого викрадення інформації», - додала вона.

У серіалі також ідеться про те, як встановити місцезнаходження гаджета, як уберегтися від витоку інформації та як протидіяти фішингу та вішингу.

Серіал складається з чотирьох серій і доступний для перегляду на порталі «Дія.Цифрова освіта».

Курс розроблено Міністерством цифрової трансформації України за підтримки проєкту Агентства з міжнародного розвитку США - USAID Україна «Кібербезпека критично важливої інфраструктури України» за участі Кіберполіції, НБУ, Держспецзв’язку, CERT-UA та Комітету ВР із цифрової трансформації…». ***(Мінцифри презентувало серіал про захист від кібершахраїв // Укрінформ (https://www.ukrinform.ua/rubric-society/3296717-v-ukraini-prezentuvali-serial-pro-zahist-vid-kibersahraiv.html). 12.08.2021).***

***

**«Національний банк України розробляє методичні рекомендації з посилення безпеки операцій в онлайн-банкінгу, онлайн-операцій з використанням карток, мобільних застосунків та чатботів у месенджерах.**

Про це під час брифінгу в Укрінформі сказав заступник голови Національного банку України Олексій Шабан.

Він зазначив, що інформація, вказана на платіжних картках, досить часто використовується зловмисниками в шахрайських схемах.

«Для того щоб громадяни були впевнені в тому, що їх банк доволі захищений від шахрайських атак, ми розробляємо і скоро опублікуємо методичні рекомендації для банків з безпеки та моніторингу операцій, в тому числі з використанням платіжних карток, побудови мобільних застосунків, інтернет-банкінгу та чатботів», - розповів Шабан.

Він додав, що рекомендації будуть базуватися на принципах побудови та організації кібербезпеки. Зокрема, вони міститимуть вимоги до мобільних застосунків, механізми запобігання використання втрачених даних, заходи з відновлення доступу до застосунку (аккаунта), вимоги до процедури зміни фінансового номера та вимоги до захисту операцій з платіжними картками…». ***(НБУ розробляє рекомендації з посилення безпеки онлайн-банкінгу // Укрінформ (https://www.ukrinform.ua/rubric-economy/3295522-nbu-rozroblae-rekomendacii-z-posilenna-bezpeki-onlajnbankingu.html). 10.08.2021).***

***

**«Сьогодні, 19 серпня, начальник Департаменту кіберполіції Олександр Гринчак та директор Департаменту безпеки Національного банку України Ігор Коновалов підписали меморандум про співпрацю.**

Згідно з положеннями меморандуму, сторони координуватимуть свої дії відповідно до законодавства України у разі виявлення кіберзагроз, кіберзлочинів у фінансових установах. Кіберполіція та Нацбанк також планують превентивну роботу з підвищення поінформованості громадян щодо безпеки в кіберпросторі.

Начальник Департаменту кіберполіції Олександр Гринчак зазначив, що кіберзахист у банківській системі України та у сфері переказу коштів у час диджиталізації є надважливим завданням.

«Таке завдання можливо виконати лише за умови тісної співпраці та обміну інформацією. Спільно з фахівцями Нацбанку ми зможемо оперативно реагувати на кіберінциденти в даній сфері та вчасно повідомляти про нові форми загроз», - зазначив Олександр Гринчак.

Директор Департаменту безпеки Національного банку України Ігор Коновалов зазначив, що цей підрозділ НБУ завжди перебуває у конструктивному діалозі з колегами з кіберполіції.

«Ми активно співпрацюємо у напрямі забезпечення кібербезпеки у фінансовій сфері. Водночас я упевнений, що підписання Меморандуму та тісніша координація наших спільних зусиль, спрямованих на підвищення ефективності протидії кіберзлочинності, дозволять піднести на якісно новий рівень нашу

співпрацю у сфері кіберзахисту фінансової системи», - сказав Ігор Коновалов». ***(Кіберполіція співпрацюватиме з Національним банком України для ефективнішої протидії злочинам у банківській сфері // Офіційний сайт Національної поліції (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-spivpraczyuvatime-z-naczionalnim-bankom-ukrajini-dlya-efektivnishoji-protidiji-zlochinam-u-bankivskij-sferi). 19.08.2021).***

***

**«Держспецзв'язку спільно із Міністерством освіти та науки України розглядають можливість створення академічної команди реагування на кіберінциденти, до складу якої входитимуть студенти закладів вищої освіти Києва.** Таку можливість обговорили під час зустрічі заступник Голови Держспецзв'язку Олександр Потій та заступник Міністра освіти та науки Ігор Гарбарук.

Заступник Міністра зазначив, що утворення цієї спільноти можливе в рамках Президентського університету.

Олександр Потій наголосив: «Наразі в Києві працює 9 закладів вищої освіти, в яких студенти навчаються за спеціальністю «Кібербезпека». На цій базі цілком можливо сформувати повноцінну академічну команду реагування, яка займатиметься питаннями виявлення кіберінцидентів, їх усунення та проведення розслідувань».

У рамках реалізації ініціативи зі створення академічної команди реагування Держспецзв'язку забезпечуватиме організаційно-методичну допомогу, підготовку, навчання фахівців та координаційну підтримку майбутньої команди…». ***(Планується створення академічної команди реагування на кіберінциденти // Компьютерное Обозрение(https://ko.com.ua/planuyetsya_stvorennya_akademichnoyi_komandi_reaguvannya_na_kiberincidenti_138422). 18.08.2021).***

***

**«У Міністерстві цифрової трансформації вважають, що для боротьби з кібершахрайством треба застосовувати комплексний підхід, зокрема підвищувати кіберграмотність населення.**

Про це під час брифінгу в Укрінформі заявив перший заступник міністра цифрової трансформації Олексій Вискуб.

«Схеми незаконного оформлення кредитів на громадян в Україні… стають більш цифровими та націленими на крадіжку цифрової ідентичності громадян... Вирішення цієї ситуації, безумовно, потребує комплексного підходу», - сказав Вискуб.

За його словами, у Мінцифри окреслюють два напрямки боротьби з кібершахрайством в Україні. Перший - підвищення кіберграмотності та покращення навичок з кібергігієни громадян, для чого відомство готує комунікаційну компанію. Зокрема, цього тижня буде презентовано освітній серіал про основи кіберграмотності та кібергігієни за участю кіберполіції.

Другий напрям боротьби з кібершахрайством, указав Вискуб, - це посилення відповідальності за порушення процедур, пов'язаних з наданням доступу до особистої інформації громадян.

Заступник міністра навів приклад одного з видів шахрайства, коли зловмисники переоформлюють номер телефону на іншу сім-картку і отримують доступ до онлайн-банкінгу, пошти та інших застосунків, зареєстрованих на такий номер. За словами Вискуба, Мінцифри спільно з кіберполіцією проведе перевірку регламенту відновлення номерів телефонів у всіх мобільних операторів. Він додав, що міністерство планує посилювати правила виконання такої процедури і запроваджувати відповідальність за їх порушення.

Як повідомляв Укрінформ, у Дніпропетровській області правоохоронці викрили місцеву жительку, яка незаконно оформляла онлайн-кредити на громадян. За попередніми даними, фігурантка ошукала близько 40 осіб більш ніж на 300 тис. грн. Зокрема, через підбір пароля зловмисниця отримала доступ до електронної скриньки однієї з потерпілих, де зберігалися копії документів та особисті фото. З використанням цих даних правопорушниця отримала доступ до онлайн-банкінгу та увійшла до мобільного застосунку «Дія».

Правоохоронці наголосили, що розкриття цієї схеми підтвердило неможливість отримання онлайн-кредиту з використанням цифрових документів у «Дії». ***(У Мінцифри назвали два напрями боротьби з кібершахрайством // Укрінформ (https://www.ukrinform.ua/rubric-society/3295662-u-mincifri-nazvali-dva-naprami-borotbi-z-kibersahrajstvom.html). 11.08.2021).***

***

## *Правове забезпечення кібербезпеки в Україні*

---

**«Кабмін на засіданні 4 серпня схвалив Стратегію енергетичної безпеки України, у ній визначаються основні загрози та пріоритети в енергетиці.**

Про це відомо з документів до засідання, трансляція засідання.

Міністр енергетики Герман Галущенко назвав стратегію "ключовим документом енергобезпеки України". Вона дає визначення основні поняттям: енергобезпеці, загрозі енергобезпеці та стійкості функціонування енергетичного сектору.

Стратегія налічує 29 загроз енергетичній безпеці, основними з яких є кіберзагрози, російська агресія, незавершена інтеґрація з енергетичними та газовими системами Євросоюзу, зношеність основних фондів, питання конкуренції на ринку та "поглиблення енергетичної бідності".

На основі цього Міненерго створило три сценарія: базовий (змін не відбувається), «недружнього впливу» (за умови зростання зовнішнього впливу РФ) та «позитивної трансформації» (за умови незворотности європейського курсу України).

Серед стратегічних цілей визначено доступність енергоресурсів всіх видів для споживачів, стійкість функціонування енергосектору, ефективність

використання ресурсів, "екологічно прийнятний" вплив енергетики на довкілля, євроінтеґрація та незалежність України у формуванні енергетичної політики.

У результаті стратегії у Міненерго очікують створити систему енергобезпеки та умови забезпечення енергостійкости, запровадити щорічний моніторинг загроз». ***(Уряд схвалив Стратегію енергетичної безпеки: кібератаки є однією з основних загроз // Економічна правда (https://www.epravda.com.ua/news/2021/08/4/676569/). 04.08.2021).***

***

**«Президент України Володимир Зеленський затвердив Стратегію кібербезпеки України та ввів у дію рішення Ради національної безпеки та оборони про створення умов для формування у системі Міністерства оборони України кібервійськ.**

Про це йдеться в указах президента №446 та 447 від 26 серпня 2021 року.

"Затвердити Стратегію кібербезпеки України", — написано в указі.

Про що йдеться в стратегії

Забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України.

Будуть не тільки забезпечувати захист критичної інформаційної інфраструктури від кібератак, а й "превентивні наступальні операції у кіберпросторі". Це включає "виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами".

Росія залишається одним з основних джерел загроз національній та міжнародній кібербезпеці.

Згідно документу, прогнозують зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі. Крім того, глобального масштабу набуває використання кіберпростору терористичними організаціями.

Пандемія COVID-19 посилить роль електронних комунікацій у повсякденному спілкуванні та роботі. Це змушує державу і бізнес впроваджувати додаткові механізми захисту інформаційних систем.

Зеленський також увів у дію рішення РНБО "Про невідкладні заходи з кібероборони держави". Цим рішенням Кабінету Міністрів, зокрема, доручено у двомісячний строк розробити та внести на розгляд Верховної Ради законопроєкт щодо створення та функціонування у системі Міністерства оборони України кібервійськ.

Також у документі Зеленський визнав такою, що втратила чинність попередня Стратегія кібербезпеки, яка була затверджена указом президента України 15 березня 2016 року». ***(Катерина Крупенко. Зеленський затвердив Стратегію кібербезпеки України та ввів у дію рішення РНБО про кібервійська // АТ «НСТУ» (https://suspilne.media/159568-gerasenko-stav-radnikom-glavi-mvs/). 26.08.2021).***

***

**«Президент Володимир Зеленський увів у дію рішення Ради національної безпеки і оборони від 14 травня «Про невідкладні заходи з кібероборони держави»…**

Згідно з документом, указ набирає чинності з дня його опублікування.

Контроль за виконанням рішення РНБО покладено на секретаря Ради національної безпеки і оборони України Олексія Данілова.

Згідно з рішенням РНБО, уряду доручено:

«Невідкладно з метою створення у системі Міністерства оборони України кібервійськ та набуття ними відповідних спроможностей здійснити розрахунки потреб щодо: обсягу матеріально-технічних та фінансових ресурсів, необхідних для створення та забезпечення належного функціонування кібервійськ; комплектування особового складу кібервійськ з урахуванням оптимального співвідношення військовослужбовців, працівників Міністерства оборони України, а також зарахованих у запас, резервістів та інших категорій осіб", - ідеться у документі.

Крім того, за результатами розрахунків у двомісячний строк розробити та внести на розгляд Верховної Ради України законопроєкт щодо створення та функціонування у системі Міністерства оборони України кібервійськ.

Як повідомляв Укрінформ, 14 травня на засіданні РНБО ухвалила Стратегію розвитку кібербезпеки на наступні п'ять років». ***(Зеленський увів у дію рішення РНБО про кібероборону держави // Укрінформ (https://www.ukrinform.ua/rubric-polytics/3304767-zelenskij-uviv-u-diu-risenna-rnbo-pro-kiberoboronu-derzavi.html). 26.08.2021).***

***

## ***Кібервійна проти України***

---

**«Киберспециалисты СБУ предотвратили новые попытки информационно-подрывной деятельности спецслужб РФ против Украины: в Киеве разоблачили мощную ботоферму.**

Вражеская интернет-агентура использовала ее для дискредитации нашего государства перед международным сообществом, заявили в пресс-центре Службы безопасности Украины.

По заданию своих «кураторов» злоумышленники распространяли через соцсети антиукраинские лозунги и дезинформацию о результатах проведения «Крымской платформы». Основная деятельность злоумышленников была в сетях Facebook, Instagram и Tik-Tok.

Для распространения дезинформации они администрировали более 15 тыс. анонимных аккаунтов. Свои сообщения публиковали от имени «рядовых граждан».

Установлено, что среди организаторов противоправной деятельности - четверо жителей Киева. Для "работы" они переоборудовали помещение одного из офисов в центральном районе столицы.

Деньги за «публикации» злоумышленники получали с территории РФ на запрещеные в Украине электронные платежные системы.

Во время обысков в помещениях ботофермы правоохранители обнаружили 300 модемов для доступа в интернет, несколько тысяч сим-карт различных операторов мобильной связи, десятки мобильных терминалов и компьютерную технику с доказательствами противоправной деятельности.

В рамках уголовного производства по ст. 361 (несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи) Уголовного кодекса Украины продолжаются следственные действия для установления всех обстоятельств правонарушения и привлечения к ответственности лиц, причастных к нему». ***(Кибербезопасность разоблачила финансируемую РФ ботоферму хейтеров "Крымской платформы" // ООО «УКРАИНСКАЯ ПРЕСС-ГРУППА» (https://day.kyiv.ua/ru/news/300821-kiberbezopasnost-razoblachila-finansiruemuyu-rf-botofermu-heyterov-krymskoy-platformy). 30.08.2021).***

***

## *Боротьба з кіберзлочинністю в Україні*

---

**«Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, за заявою «Національного координаційного центру кібербезпеки» при РНБО, працює над блокуванням шахрайських ресурсів, які збирали дані про банківські картки українців, використовуючи популярність телеканалу «1+1».**

Зловмисники створили мережу шахрайських сайтів та запустили рекламну кампанію в соціальній мережі Facebook з пропозицією для громадян України отримати значні суми виплат, які нібито передбачені рішеннями влади чи будуть виплачені спонсорами за опитування.

Щоб підвищити довіру громадян та заманити їх у пастку, в рекламі та на фішинговому сайті були використані логотип «1+1», а також уривки з випусків «Телевізійної служби новин», яка виходить на цьому каналі.

Реклама веде на фішинговий сайт airmauritiusticket.com, з якого всіх, хто використовує IP-адреси українського сегмента мережі інтернет, перенаправляють на інший сайт, де для отримання грошей пропонується пройти опитування. Після низки перенаправлень на різні сайти довірливих громадян просять ввести дані банківської картки для отримання грошей та переказати незначну суму – 138 грн». ***(Шахраї виманюють банківські реквізити, маскуючись під сайт каналу «1+1» // Компьютерное Обозрение (https://ko.com.ua/shahrayi_vimanyuyut_bankivski_rekviziti_maskuyuchis_pid_sajt_kanalu_1_1_138275). 05.08.2021).***

***

**«Протягом липня Служба безпеки припинила та нейтралізувала 65 кібератак на інформсистеми органів державної влади, повідомила пресслужба СБУ.** Вказано, що фахівці проаналізували понад 31 тисячу критичних подій інформаційної безпеки.

Найчастіше основними типами кібератак були:

з'єднання з командно-контрольними серверами (C&C Server);

спроби отримання несанкціонованого доступу (Brute Force Attack);

атаки на вебдодатки (Web App Attack);

шкідливе програмне забезпечення (Malware) та інші.

В СБУ також додали, що на базі Ситуаційного центру забезпечення кібербезпеки спецслужби функціонує система управління подіями інформаційної безпеки (SIEM). Вона моніторить події у режимі реального часу і дозволяє аналізувати стан інформаційної безпеки. Потенційно критичні події безпосередньо обробляються аналітиками безпеки. В СБУ вказали, що це дозволяє оперативно виявляти, реагувати та попереджувати загрози у національному кіберпросторі…» ***(Минулого місяця СБУ блокувала 65 кібератак на сайти органів влади // Дзеркало тижня. Україна (https://zn.ua/ukr/UKRAINE/minuloho-misjatsja-sbu-blokuvala-65-kiberatak-na-sajti-orhaniv-vladi.html). 03.08.2021).***

***

**«В Луцке нейтрализовали мощную ботоферму, которую финансировали представители РФ.**

Киберспециалисты СБУ разоблачили новый очаг информационно-подрывной деятельности против госбезопасности Украины, сообщили в пресс-центре ведомства.

По заданию своих «кураторов» злоумышленники в соцсетях агитировали за создание так называемых «Малороссии» и «Новороссии», а также за присоединение всего востока Украины к «великой России».

Чтобы скрыть правонарушения, они использовали специальное оборудование для анонимизации каналов связи. «Технику» разместили по шести подпольными адресам.

Деньги за распространение враждебного контента агитаторы получали в иностранной валюте через российские платежные системы.

Установлено, что один из организаторов ботофермы - житель областного центра.

Для распространения в интернете деструктивных публикаций они создали тысячи фейковых аккаунтов.

Во время обысков по адресам расположения «ячейки» правоохранители обнаружили: GSM-шлюзы, компьютерное оборудование, банковские карточки, более тысячи сим-карт операторов мобильной связи, финансовые документы и другие материалы с доказательствами противоправной деятельности.

В рамках уголовного производства, начатого следователями органов безопасности по ч. 1 ст. 361 (несанкционированное вмешательство в работу компьютеров, автоматизированных систем, компьютерных сетей или сетей электросвязи) и ч. 2 ст. 110 (посягательство на территориальную целостность и неприкосновенность Украины) Уголовного кодекса Украины, проводятся следственные действия для установления всех обстоятельств правонарушения и привлечения к ответственности виновных лиц». ***(Кибербезопасность разоблачила финансируемую РФ пророссийскую ботоферму // ООО «УКРАИНСКАЯ ПРЕСС-***

***ГРУППА» (https://day.kyiv.ua/ru/news/190821-kiberbezopasnost-razoblachila-finansiruemuyu-rf-prorossiyskuyu-botofermu). 19.08.2021).***

***

**«За допомогою спеціального телекомунікаційного обладнання фігуранти видавали міжнародний телефонний трафік за псевдонаціональний. Таким чином, міжнародні виклики тарифікувалися за цінами національних.**

Протиправну діяльність викрили співробітники відділу протидії кіберзлочинам Хмельниччини спільно зі слідчим управлінням обласної поліції.

Кіберполіція встановила, що до протиправних дій причетні мешканці Хмельницького. Фігуранти розмістили спеціалізовані апаратно-програмні комплекси у власних оселях та в орендованих приміщеннях в Україні та закордоном.

Спеціалізоване телекомунікаційне обладнання зловмисники використовували для заробітку на незаконній маршрутизації міжнародного телекомунікаційного трафіку. У такому випадку міжнародний телефонний трафік перенаправлявся у внутрішню телекомунікаційну мережу мобільних операторів. У результаті міжнародні дзвінки тарифікувалися за цінами національних. Також, використовуючи сім-карти мобільних операторів країн СНД, забезпечували підміну оригінальних номерів вихідного дзвінку.

Крім цього, послугами зловмисників користувались телефонні шахраї, колекторські спілки та шахрайські кол-центри. Також створювались умови для діяльності так званих ботоферм, тобто реєстрації та анонімізації особистості у соціальних мережах, месенджерах, дошках оголошень та інших сервісах.

Встановлено, що користувачами послуг були представники Російської Федерації та інших країн СНД.

Правоохоронці провели обшуки за місцем мешкання фігурантів. За результатами вилучили комп’ютерну техніку зі встановленим спеціалізованим програмним забезпеченням, близько трьох тисяч сім-карток операторів зв’язку, значну кількість телекомунікаційного обладнання (sim-банки, GoIP шлюзи та 3g модеми).

За даним фактом відкрито кримінальне провадження за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України. Санкція статті передбачає позбавлення волі на строк від 3 до 6 років. Встановлюються всі особи, причетні до протиправної діяльності. Слідчі дії тривають.

Процесуальне керівництво здійснює Хмельницька обласна прокуратура. Слідчі дії проводилися спільно регіональним управлінням СБУ». ***(На Хмельниччині кіберполіція заблокувала нелегальний центр комутації міжнародного зв’язку // Національна поліція (https://www.npu.gov.ua/news/kiberzlochini/na-xmelnichchini-kiberpolicziya-zablokuvala-nelegalnij-czentr-komutacziji-mizhnarodnogo-zv-yazku/). 30.08.2021).***

***

**«Октябрьский районный суд Мариуполя вынес приговор несовершеннолетнему украинцу за распространение вредоносного программного обеспечения через мессенджер Telegram…**

Лицеист Мариупольского морского лицея, в свободное от учебы время, решил подзаработать, продавая ПО для взлома компьютеров пользователям мессенджера Telegram. Вознаграждение юноша получал на карточку Приватбанка.

По заключению эксперта, вышеуказанное программное обеспечение является вредоносным ПО типа «Ramson/Winlock», имеющее функционал блокировки доступа к компьютеру и вымогательство (шантаж) выкупа от зараженного компьютера.

В судебном заседании обвиняемый рассказал, что в начале октября 2020 года один из пользователей Telegram предложил ему создать программное обеспечение для блокировки работы компьютера. Обратившись к своему знакомому с такой просьбой, он получил соответствующую программу, которую за 300 грн прислал заказчику.

В дальнейшем, к нему обратился еще один пользователь мессенджера с аналогичной просьбой, которому он также реализовал вредоносное ПО в этот раз уже за 350 грн. В содеянном юный предприниматель искренне раскаялся и попросил суд освободить его от уголовной ответственности и передать под надзор отцу.

Действия обвиняемого суд квалифицировал по ч.1 ст.361-1 УК Украины и по ч.2 ст. 361-1 УК Украины, как умышленный сбыт вредоносных программных средств, предназначенных для несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров), совершенный повторно.

На основании п. 3 ч. 2 ст. 105 УК Украины суд освободил обвиняемого от наказания без определения его вида и размера и применил принудительные меры воспитательного характера, а именно - передал его под надзор отца до достижения совершеннолетия.

Кроме этого, суд обязал юношу оплатить сумму в размере 8989 грн. 75 коп за проведение экспертиз». ***(Артем Сереженок. Несовершеннолетний украинец продавал вредоносное ПО пользователям Telegram // Internetua (http://internetua.com/nesovershennoletnii-ukrainec-prodaval-vredonosnoe-po-polzovatelyam-telegram). 21.08.2021).***

***

## Міжнародне співробітництво у галузі кібербезпеки

**«Україна подала офіційний запит щодо приєднання до роботи Об'єднаного центру передових технологій з кібероборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence), що базується у Таллінні.**

Як повідомляє «Європейська правда», про це йдеться у заяві на сайті Ради національної безпеки і оборони.

Напередодні до Естонії приїжджала делегація Національного координаційного центру кібербезпеки при РНБО. Під час зустрічі із державним секретарем Міністерства оборони Естонії Кусті Салмом сторони обговорили шляхи поглиблення практичного співробітництва між Україною та Естонією у сфері кібербезпеки.

«Зокрема сторони обмінялися думками щодо перспективи залучення України до роботи Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE). Від імені секретаря РНБО України Олексія Данілова українська сторона виступила з офіційним запитом на приєднання до CCDCOE», - йдеться у заяві.

В РНБО зазначили, що залучення України до роботи CCDCOE може стати важливим кроком на шляху до повноправного членства в НАТО.

Центр має акредитацію НАТО - формально не входячи до командної структури, він має величезний вплив на дії Альянсу у сфері кіберзахисту. Центр заснували сім країн, а сьогодні він налічує 20 учасників – 17 членів НАТО та 3 країни-партнери.

Унікальність центру полягає в тому, що там разом працюють військові, цивільні, представники уряду. Робота центру сфокусована на трьох основних напрямках: дослідження, тренування та навчання». ***(Україна подала офіційний запит на приєднання до Об'єднаного центру з кібероборони НАТО // Європейська правда (https://www.eurointegration.com.ua/news/2021/08/4/7126215/). 04.08.2021).***

***

**«Що таке Глобальна коаліція з цифрової безпеки (далі – Коаліція)? Це проєкт Всесвітнього економічного форуму, обговорення якого розпочалася у 2019 році в межах платформи медіа, розваг та спорту, проте пандемія коронавірусу посилила виклики та прискорила запуск проєкту.**

Завданням Коаліції є об'єднання представників урядів, бізнесу, академічної спільноти та громадянського суспільства для забезпечення цифрової безпеки шляхом вирішення проблем за трьома напрямками: правила модерації контенту, регуляторна політика, бізнес-моделі та конкуренція.

Україна приєдналася до Коаліції з моменту її створення 29 червня 2021 року. До Коаліції також приєдналася Великобританія, Швеція, Австралія, Сінгапур, Індонезія та Бангладеш, IT-компанії Microsoft, Otto, NetClean, Two Hat Security, посадовці UNICEF та інші міжурядові та неурядові організації.

Керівним документом Коаліції є біла книга Всесвітнього економічного форуму «Advancing Digital Safety: A Framework to Align Global Action», в якій викладені основні проблеми у сфері цифрової безпеки, виклики на шляху їх подолання, а також пропоновані кроки для всіх стейкхолдерів.

Які проблеми має вирішити коаліція

Серед пріоритетних проблем у сфері цифрової безпеки аналітики виділяють: перше – дезінформацію у сфері охорони здоров'я; друге – експлуатацію та жорстоке поводження з дітьми; третє – екстремізм та тероризм.

Хоча всі три проблеми існують майже стільки ж, скільки існує інтернет, глобальний локдаун суттєво збільшив проникнення онлайн-середовища в життя людей, що призвело до загострення зазначених проблем.

До прикладу, боротьба з дезінформацією у сфері охорони здоров'я стала пріоритетом для багатьох урядів та IT-компаній. Опитування ресурсу Axios (США) в партнерстві з консалтинговою компанією Ipsos (Франція) демонструють, що громадяни дезінформовані щодо питань охорони здоров'я та менш схильні вакцинуватися, що становить загрозу для безпеки суспільств.

Для боротьби з неправдивою інформацією онлайн-платформи вдалися до видалення проблематичного контенту: протягом 2020 року YouTube видалив понад 800 000 відео, а Facebook (разом з Instagram) за той же період видалили 1 млн публікацій з неправдивою інформацією щодо COVID-19.

Окрім видалення публікацій, платформи блокували профілі користувачів, які поширювали недостовірну інформацію щодо пандемії, а також співпрацювали з урядами та неурядовими організаціями для перевірки контенту на достовірність та переадресації користувачів на офіційні джерела. В Україні таким джерелом є Міністерство охорони здоров'я.

Ризики для неповнолітніх користувачів цифрового середовища досліджувалися UNICEF із розподілом на категорії шкідливого контенту. Опитування продемонструвало, що понад 70% респондентів мали досвід контакту, принаймні, з одним з видів шкідливого контенту. Найбільша кількість: сексуальний контент – 33% опитуваних, та насильницький контент – 30%.

Окрім ризиків контакту зі шкідливим контентом, неповнолітнім загрожує можливість натрапити на осіб, які за допомогою різних платформ створюють умови для сексуальної експлуатації дітей. Така експлуатація відбувається за допомогою сервісів прямих трансляцій.

За даними опитування щодо випадків використання платформ для сексуальної експлуатації дітей, респонденти найчастіше згадували Skype (39% опитаних), Snapchat (29,9%) та Facebook включно з Facebook messenger та Facebook live (24%).

Загрози тероризму та екстремізму в аспекті роботи онлайн-платформ стосуються, в першу чергу, можливостей радикально налаштованих груп організовуватися, координуватися та поширювати свої переконання через такі платформи. Наприклад, штурм Капітолію США демонстрантами 6 січня 2021 року координувався за допомогою Twitter та Facebook.

Платформи протидіють цьому, в першу чергу, блокуючи подібні групи або окремих користувачів. Утім такі блокування несуть і певні ризики.

Критики вважають, що блокування профілів окремих осіб також може порушувати право на свободу вираження поглядів (наприклад, блокування Twitter-акаунту Дональда Трампа).

З іншого боку, онлайн-сервіси зазнають критики за запізнілу та обмежену реакцію. Як у випадку штурму з тим самим Капітолієм.

*Які виклики існують на шляху подолання проблем*

Вирішення цих та інших проблем потребують значної роботи законодавчих та регуляторних органів у тісній співпраці з IT-індустрією.

В першу чергу, урядам необхідно співвіднести фундаментальні права – право на приватність, право на свободу вираження поглядів – з необхідними кроками на шляху до безпечнішого цифрового простору.

Одним з конфліктів, про який згадують автори дослідження, є співвідношення приватності та безпеки. Щоб виявляти шкідливий контент, наприклад, сексуальну експлуатацію дітей, необхідно, серед іншого, сканувати повідомлення користувачів.

Коли Facebook припинив сканування повідомлень своїх користувачів на вимогу регулювання ЄС, випадки виявлення контенту із сексуальною експлуатацією дітей зменшилися на 46% у перші три тижні після такої заборони. Пізніше ЄС скорегував своє законодавство для виявлення подібного контенту.

Іншою проблемою є забезпечення свободи вираження поглядів. Онлайн-платформи є приватними компаніями, що мають право встановлювати свої вимоги щодо того, який контент є прийнятним для розміщення на їхніх ресурсах.

Зазвичай, бачення приватних компаній є вужчим за законодавчі рамки. Це пояснюється бізнес-моделлю таких компаній, джерелом прибутку яких є розміщення рекламних матеріалів.

Розміщення контенту, який законодавчо допустимий, але може спровокувати негативну реакцію, наприклад, розміщення фотографії військового злочину, може відлякувати рекламодавців.

Серед інших проблем експерти зазначають:

- складнощі у законодавчому визначенні комплексних технологій (наприклад, чи є Facebook форумом, публікаційною платформою, сервісом прямих трансляцій або рекламним сервісом);
- питання відповідальності платформи за дії третіх осіб за допомогою сервісів цієї платформи (особливо якщо такі користувачі знеособлені);
- складнощі взаємодії між зонами з різним законодавчим полем.

Що пропонується?

Автори Білої книги пропонують конкретні кроки для збільшення рівня цифрової безпеки, які мають здійснити всі стейкхолдери.

До прикладу, цифровим платформам рекомендують:

1) збирати аналітику щодо безпеки користувацького досвіду;

2) взаємодіяти між собою для унеможливлення інтернет атак шляхом одночасного булінгу на всіх акаунтах жертви;

3) створити посаду Офіцера з цифрової безпеки, який матиме право голосу при прийнятті рішень на рівні керівництва;

4) узгодити стандарти роботи команд з модерації контенту, поліпшувати умови їхньої роботи.

Рекламодавцям рекомендують оновити або створити регламенти, спрямовані на дотримання безпеки споживача та розподіляти кошти на рекламні кампанії на цифрових платформах відповідно до них. Крім цього рекомендується більш тонко обирати ключові слова для рекламних кампаній, аби спрямовувати фінансування на безпечний контент.

Регуляторам пропонують створити органи онлайн-безпеки, відступати від окремих правил та змінювати законодавство для забезпечення цифрової безпеки, а

також сконцентруватися на превенції завдання шкоди, не допускаючи при цьому обмеження свободи слова.

Всім залученим рекомендують обмінюватися позитивним досвідом та взаємодіяти з іншими стейкхолдерами.

*Що це означає для України*

Для України приєднання до Коаліції, в першу чергу, означає додаткові інструменти для забезпечення безпеки онлайн-простору.

Оскільки уряд України має доволі обмежені важелі впливу на дії найбільших онлайн-платформ, долучення до Коаліції надасть ще один канал зв'язку із найбільшими ІТ-компаніями.

Посилення комунікації з онлайн-платформами може бути використане урядом, наприклад, для боротьби з кібератаками та ботофермами, недопущення втручання у перебіг виборчих кампаній, коригування політики модерування дописів та стимулювання до створення україномовних команд з аналізу контенту.

Приєднання до Коаліції від самого початку надасть змогу привернути більшу увагу до позиції нашого уряду з тих чи інших питань. Крім того, досвід України у протидії дезінформації, яку поширює Росія, також може бути врахований при роботі Коаліції.

Важливо уточнити, що Коаліція визначає лише бажаний вектор розвитку, проте не покладає на своїх членів жодних обов'язків». ***(Михайло Процайло. Україна – член Глобальної коаліції з цифрової безпеки: що це значить і що дає країні // Економічна правда (https://www.epravda.com.ua/columns/2021/08/3/676543/). 03.08.2021).***

***

**«Секретар Ради Національної безпеки України Олексій Данілов назвав кібератаки «зброєю номер один» у сучасних війнах.**

Про це Данілов заявив під час зустрічі із представниками Комітету зі Збройних Сил Конгресу Сполучених Штатів та його керівником Адамом Смітом.

На зустрічі РНБО та Комітет зі Збройних Сил Конгресу США також обговорили питання актуальних потреб України у військовій та оборонній сферах.

На думку Данілова, кібератакам потрібно приділити посилену увагу, адже це головна зброя не лише сучасних, а й майбутніх війнах.

– Сфера кібербезпеки є ключовою складовою національної безпеки, – наголосив секретар РНБО.

Крім цього Данілов вкотре звернувся до голови Комітету із проханням посприяти вступу України до Об'єднаного центру передових технологій з кібероборони НАТО.

*Небезпека кібератак*

Не лише Україна вбачає у хакерських атаках реальну загрозу національній безпеці.

Президент Сполучених Штатів Джо Байден заявив про те, що кібератаки можуть стати причиною реальної війни між великими державами із застосуванням справжньої зброї». ***(Софія Зінов'єва. Кібератаки є зброєю номер один у сучасних та майбутніх війнах – Данілов // ФАКТИ. ICTV***

***(https://fakty.com.ua/ua/ukraine/20210816-kiberataky-ye-zbroyeyu-nomer-odyn-u-suchasnyh-ta-majbutnih-vijnah-danilov/). 16.08.2021).***

***

**«Голова Хмельницької обласної ради Віолета Лабазюк підписала меморандум про взаєморозуміння з Фондом цивільних досліджень та розвитку США.**

У ньому визначено основні аспекти співпраці щодо впровадження безпечних інформаційно-комунікаційних технологій в територіальних громадах краю.

Вже у вересні у Хмельницькому за участю представників Ради національної безпеки України, Фонду цивільних досліджень та розвитку США відбудеться семінар з основ кібербезпеки для керівників територіальних громад та органів державної влади.

Наступним кроком стане впровадження навчального онлайн-курсу з основ кібербезпеки для посадовців місцевого самоврядування та державних службовців.

Відтак область стане першою в країні, де реалізовуватиметься програма підготовки у сфері розбудови можливостей з безпеки інформації, кібербезпеки та підвищення обізнаності публічних управлінців». ***(Ірина КОЗАК. Хмельниччина: Посадовців навчатимуть кібербезпеки // Голос України (http://www.golos.com.ua/article/350058). 20.08.2021).***

***

**«Сингапур и США подписали серию меморандумов о взаимопонимании (MOU), чтобы расширить свое сотрудничество в области кибербезопасности в сфере обороны, финансов, исследований и разработок.** Такие инициативы будут включать дальнейший обмен информацией, совместные упражнения, обучение и развитие компетенций.

В понедельник в рамках трехдневного визита вице-президента США Камалы Харрис в азиатскую страну на этой неделе были подписаны три меморандума о взаимопонимании.

Одно из них связано с соглашением между Агентством кибербезопасности Сингапура (CSA) и Агентством кибербезопасности и безопасности инфраструктуры США (CISA) об углублении сотрудничества в области кибербезопасности, помимо обмена данными и обмена данными. Два правительственных агентства будут стремиться включить новые области сотрудничества в области критических технологий, а также исследований и разработок, среди прочего.

Генеральный директор CSA Дэвид Кох отметил, что обе страны разделяют «глубокие взаимные интересы» в расширении сотрудничества в области кибербезопасности, особенно потому, что кибербезопасность теперь стала ключевым фактором, позволяющим двум странам использовать цифровизацию для роста своей экономики и улучшения жизни своего населения.

Директор CISA Джен Истерли сказала: «Киберугрозы не ограничиваются границами, поэтому международное сотрудничество является ключевой частью подхода администрации Байдена-Харриса к кибербезопасности. Меморандум о

взаимопонимании позволяет нам укрепить наше существующее партнерство с Сингапуром, чтобы мы могут более эффективно работать вместе, чтобы коллективно защищаться от угроз сегодняшнего дня и обезопасить себя от рисков завтрашнего дня».

Во втором меморандуме о взаимопонимании, подписанном между Министерством обороны Сингапура (Mindef), вооруженными силами Сингапура (SAF) и Министерством обороны США, обе страны будут стремиться к сотрудничеству в рамках различных инициатив в области киберпространства. Сюда входят усилия по установлению «взаимопонимания» и обмену данными, а также сотрудничество в «создании потенциала».

Начальник сил обороны Сингапура генерал-лейтенант Мелвин Онг сказал: «Этот меморандум о взаимопонимании о сотрудничестве в киберпространстве между оборонными ведомствами Сингапура и США является важным шагом в формализации нашего сотрудничества в киберпространстве и отражением нашей неизменной приверженности расширению нашего сотрудничества в области обороны во многих областях. Мы надеемся на сотрудничество с США в этом сложном ландшафте кибербезопасности».

По словам Миндефа, у обеих стран были «обширные» оборонные бои, которые включали в себя обмены между военными, обучение и сотрудничество в области оборонных технологий. Сюда входили предыдущие соглашения, такие как Стратегическое рамочное соглашение 2005 года, в котором Сингапур признавался крупным партнером по сотрудничеству в области безопасности, и Соглашение о расширенном оборонном сотрудничестве 2015 года, которое расширило сотрудничество в сфере обороны по различным областям безопасности, включая киберзащиту и биозащиту.

Третий меморандум о взаимопонимании, касающийся Валютного управления Сингапура (MAS) и Министерства финансов США, направлен на продвижение инициатив в области кибербезопасности и укрепление двустороннего институционального партнерства. Оба финансовых агентства обмениваются информацией о киберугрозах с 2018 года, говорится в совместном заявлении в понедельник.

Соглашение предусматривает сотрудничество в различных областях, включая обмен информацией о правилах и инцидентах в области кибербезопасности, а также анализ угроз, обучение сотрудников для стимулирования сотрудничества в области кибербезопасности и инициативы по повышению квалификации, такие как трансграничные учения по кибербезопасности.

Министр финансов США Джанет Л. Йеллен отметила, что соглашение о сотрудничестве в области кибербезопасности повысит киберустойчивость финансовых систем обеих стран.

Управляющий директор MAS Рави Менон сказал: «Учитывая растущую сложность кибератак и то, насколько взаимосвязана глобальная финансовая система, тесное сотрудничество необходимо для обеспечения киберустойчивости наших финансовых систем. Этот Меморандум о взаимопонимании между Казначейством США и MAS будет особенно полезным в области обмена информацией о киберугрозах и трансграничных учений по кибербезопасности».

***(Eileen Yu. Singapore, US pledge deeper collaboration in cybersecurity // (https://www.zdnet.com/article/singapore-us-pledge-deeper-collaboration-in-cybersecurity/). 23.08.2021).***

***

## Коронавірус COVID-19 та питання кібербезпеки

**«Губернатор італійського регіону Лаціо Нікола Дзінгаретті розповів у понеділок, що хакерська атака, яка в неділю вивела з ладу систему запису на вакцинацію в регіоні, відбулася з-за кордону…**

За словами Дзінгаретті, атака не завадила і не завадить роботі швидкої допомоги, відділень невідкладної допомоги, переливанню крові, госпіталізаціям та іншим медичним послугам.

Але поки проблема з атакою не буде вирішена, жителі регіону не зможуть зареєструватися через регіональний веб-сайт на щеплення. «Реєстрація тимчасово припинена», - сказав він.

Губернатор охарактеризував цю атаку як "ймовірно, найсерйознішу з тих, що коли-небудь відбувалися на території країни". Атаку розслідують експерти з розвідки і кібербезпеки.

Дзінгаретті відкинув як безпідставні повідомлення про вимогу викупу хакерами і додав, що напад було скоєно з-за кордону. Він сказав, що друга спроба злому, розпочата приблизно через дві години після першої, незабаром після опівночі неділі була успішно відбита.

За словами Дзінгаретті, існуючі записи на прийом першої або другої дози вакцини, призначені до 13 серпня, будуть виконані.

«Злом жодним чином не сповільнить процес вакцинації», - запевнив губернатор.

Близько 70% жителів Лаціо, до якого входить також Рим, у віці від 12 років і старші повністю вакциновані. В країні ця цифра становить 60%.

Комісар з питань охорони здоров'я Лаціо Алессіо Д'Амато сказав, що в неділю було зроблено близько 50 тисяч щеплень проти COVID-19, і єдиний наслідок атаки - сповільнення реєстрації даних, оскільки всю інформацію доводилося реєструвати вручну.

Нещодавно Італія оголосила, що доказ вакцинації або імунітету проти COVID-19 стане обов’язковим для цілої низки заходів.

Цей крок викликав протести по всій країні проти запровадження так званого «зеленого пропуску», який показує, що люди були вакциновані, отримали негативний тест або одужали від COVID-19». ***(Систему запису на вакцинацію в італійському Лаціо атакували хакери з-за кордону // Європейська правда (https://www.eurointegration.com.ua/news/2021/08/2/7126137/). 02.08.2021).***

***

**«Отчет о состоянии кибербезопасности Сингапура в 2020 году, опубликованный Агентством кибербезопасности Сингапура (CSA) 8 июля 2021 года, пролил свет на киберугрозы во время COVID-19.**

В 2020 году наблюдался рост киберугроз, таких как программы-вымогатели, фишинговые атаки и онлайн-мошенничество, поскольку киберпреступники извлекли выгоду из пандемии COVID- 19 за счет:

Использование страха и беспокойства для обмана жертв путем выдачи себя за правительство или органы здравоохранения, мошенничества, связанного с вакцинацией, а также поддельных веб-сайтов и приложений, связанных с COVID-19, для таких действий, как кража учетных данных и распространение вредоносного ПО.

Использование все более широкого использования новых непроверенных технологий и обходных путей для облегчения отслеживания контактов и организации работы на дому.

Нацеливание на производственно-сбытовую цепочку вакцины и использование изощренных фишинговых кампаний для кражи данных, учетных данных и конфиденциальной информации, относящейся к исследованиям, разработке и распространению вакцин.

В том же году американский поставщик информационных технологий SolarWinds также подвергся атаке на цепочку поставок. Ранее хакеры проникли в производственную сеть SolarWinds, чтобы вставить вредоносный код в обновление программного обеспечения для широко используемой платформы. Обновление было загружено клиентами SolarWinds, включая правительства и компании из списка Fortune 500. Это создавало бэкдор в сети каждой жертвы и использовалось хакерами для установки большего количества вредоносных программ, позволяя хакерам маскироваться под законных пользователей и получать неограниченный доступ к сетям и хранимым активам жертвы. Взлом SolarWinds имел потенциальный эффект домино, поскольку жертвы, которые были основными поставщиками, были уязвимы для взлома второго уровня, когда хакеры могли дополнительно скомпрометировать другие цепочки поставок.

*Ключевые киберугрозы 2020 года*

В 2020 году количество киберпреступлений увеличилось, составив 43% от общего числа преступлений в Сингапуре, при этом онлайн-мошенничество является основной категорией киберпреступлений. Киберпреступность относится к онлайн-мошенничеству, кибер-вымогательству и преступлениям в соответствии с Законом о неправомерном использовании компьютеров, относящимся к несанкционированному доступу, использованию или модификации компьютеров, компьютерных материалов и компьютерных услуг.

К наиболее распространенным угрозам кибербезопасности относятся:

Вымогатели: CSA видел 154% скачок числа зарегистрированных случаев вымогателей, в основном влияет на малые и средние предприятия (МСП s). CSA также отметил, что вымогатели операторы переходят от неизбирательного действия, оппортунистической атаку целевого подхода в области рыболовства для больших жертв. Операторы программ-вымогателей также применяют тактику

«утечки и позора», чтобы заставить жертв платить выкуп, чтобы предотвратить публичную утечку украденных данных, например утечку данных.

Серверы управления и контроля (C&C) и ботнет-дроны: CSA зафиксировала рост числа вредоносных C&C серверов, размещенных в Сингапуре, на 94%. C & C-серверы - это централизованные устройства, используемые злоумышленниками для поддержания связи со скомпрометированными системами, также известными как ботнеты, в целевой сети. Также было обнаружено в среднем 6600 дронов-ботнетов с сингапурскими IP-адресами, что больше, чем в среднем в 2019 году в 2300.

Фишинг: несмотря на снижение фишинговых атак на 1%, CSA обнаружило 47 000 сингапурских фишинговых URL. Более половины организаций, подделанных в ходе этих фишинговых инцидентов, были крупными компаниями, занимающимися технологиями или социальными сетями, либо работающими в банковском и финансовом секторах. Полиция Сингапура, Министерство кадров и Министерство образования были тремя наиболее фальшивыми правительственными учреждениями Сингапура, многие из которых связаны с фишинговыми письмами.

Утечки веб-сайтов: по сравнению с 2019 годом количество повреждений веб-сайтов.sg сократилось на 43%, при этом большинство жертв - это представители малого и среднего бизнеса, а не правительственные веб-сайты, которые пострадали. Однако значительное снижение может также означать, что группы активистов выбрали другие платформы с потенциально более широким охватом, такие как социальные сети, для продвижения своей повестки дня.

*Новые тенденции*

По мере развития угроз кибербезопасности организации сталкиваются со следующими проблемами:

Плохо настроенные сети и системы, которые были созданы для обеспечения непрерывности бизнеса во время удаленной работы, увеличивая угрозы и подвергая организации дополнительным рискам.

Растущий риск атак на цепочку поставок, поскольку организации зависят от поставщиков технологий в поддержке своих бизнес-операций.

Постоянно развивающиеся атаки программ-вымогателей превращаются из единичных единичных инцидентов в массовые системные угрозы, потенциально становясь проблемой национальной безопасности.

Чрезвычайно важно, чтобы организации регулярно проверяли свою гигиену кибербезопасности, сетевые соединения и рабочие зависимости, а также обеспечивали обновление систем / программного обеспечения, информирование сотрудников об угрозах, а также быстрое обнаружение вторжений и их сдерживание.

*Предупредительные меры*

По мере того, как организации борются с киберугрозами, нижеследующее служит неисчерпывающим списком превентивных мер, которые организации могут учитывать в борьбе с развивающимися угрозами кибербезопасности. («Надлежащая защита данных с помощью методов проектирования для систем ИКТ», совместно разработанная Комиссией по защите личных данных Сингапура и комиссаром Гонконга по конфиденциальности личных данных.)

Сведите к минимуму сбор персональных данных, гарантируя, что организация не будет собирать данные без необходимости, и для этого есть действительная цель.

Реализуйте защиту и безопасность данных с помощью дизайна, при котором вопросы защиты данных и безопасности рассматриваются на начальных этапах любой системы, услуги, продукта или процесса и на протяжении всего их жизненного цикла.

Расшифруйте требование к безопасности вашей организации к ИКТ поставщикам при разработке решений на заказ и убедитесь, что они зарегистрированы в договоре или объеме работ. При составлении требований организации должны определить и принять во внимание отраслевые стандарты и кодексы практики в области технологий и кибербезопасности. Примеры включают Руководство по управлению технологическими рисками, опубликованное валютным управлением Сингапура для финансового сектора, или Практический кодекс кибербезопасности для критически важной информационной инфраструктуры, опубликованный CSA для владельцев критически важной информационной инфраструктуры в соответствии с Законом о кибербезопасности 2018.

Проводите оценку воздействия защиты данных в начале проектов или после создания предварительного проекта новой системы ИКТ, чтобы оценить типы данных и действия по их обработке. Это поможет организациям выявлять и оценивать пробелы и риски в дизайне новой системы в отношении персональных данных и действий по их обработке.

Отчитываться перед пользователями и персоналом с помощью политик защиты данных и уведомлений, которые уведомляют этих лиц о целях и получают необходимое согласие на сбор, использование, обработку и раскрытие их личных данных.

Как говорится, кибербезопасность сегодня - это гораздо больше, чем просто технология. Помимо предоставленных им инструментов, организации не могут позволить себе ослабить бдительность, но должны сохранять бдительность и идти в ногу с новыми технологиями и изменениями в ландшафте, чтобы свести к минимуму свою подверженность киберугрозам и рискам». ***(Jonathan Kok, Joyce Lee. Fighting evolving cybersecurity threats in Singapore: No letting the guard down // WITHERS (https://www.withersworldwide.com/en-gb/insight/fighting-evolving-cybersecurity-threats-no-letting-the-guard-down). 18.08.2021).***

***

## Світові тенденції в галузі кібербезпеки

**«Компания Varonis Systems, разработчик программных решений для защиты от комплексных кибератак, представила доклад о рисках кибербезопасности, которые возникают в компаниях при некорректной настройке популярной CRM-системы Salesforce, в частности рабочего пространства Salesforce Community.**

Рабочее пространство Salesforce позволяет клиентам и партнерам компании работать в Salesforce удаленно: открывать заявки на поддержку, задавать вопросы, управлять подписками и многое другое. Однако некорректная настройка рабочего пространства может привести к тому, что конфиденциальные данные станут доступны пользователям сети интернет, а анонимные пользователи смогут запрашивать конфиденциальную информацию: списки клиентов, обращения в службу поддержки, адреса электронной почты сотрудников.

Обладая такими данными, злоумышленники могут не только использовать их для разведки в рамках фишинговой кампании, но и украсть конфиденциальную информацию о компании, ее деятельности, клиентах и партнерах. Иногда мошенники способны получить информацию из других сервисов, интегрированных с учетной записью Salesforce.

Аналитики Varonis обнаружили множество общедоступных рабочих пространств Salesforce, которые неправильно настроены и раскрывают конфиденциальную информацию. Чтобы предотвратить потенциальные риски утечки данных, команда Varonis выделяет четыре ключевые рекомендации по конфигурированию Salesforce Community.

Аудит прав доступа гостевого пользователя. Убедитесь, что разрешения гостевого профиля не раскрывают ничего лишнего (учетные записи, календари сотрудников и т.п.);

Отключение доступа к API для гостевого профиля;

Назначение «владельца по умолчанию» для записей, созданных гостевыми пользователями;

Активация безопасного доступа гостевых пользователей.

Рабочие пространства являются публичными и по умолчанию индексируются Google. Несмотря на то, что это удобно для клиентов и партнеров, это облегчает злоумышленникам, обнаружившим уязвимость или неправильную конфигурацию, поиск рабочих пространств и злоупотребление полученными из них данными». ***(Некорректная конфигурация Salesforce повышает риск утечки конфиденциальных данных при дистанционной работе // Компьютерное Обозрение (https://ko.com.ua/nekorrektnaya_konfiguraciya_salesforce_povyshaet_risk_utechki_konfidencialnyh_dannyh_pri_distancionnoj_rabote_138429). 19.08.2021).***

***

**«Около 56% предприятий Азиатско-Тихоокеанского региона признают, что отказываются от цифровых процессов, чтобы приспособиться к удаленной или гибкой работе.** И это несмотря на то, что 48% выразили повышенную обеспокоенность по поводу способности их компании справляться с угрозами безопасности.

Последний показатель был выше, чем у их коллег в Северной и Южной Америке, 41% из которых были так же более обеспокоены, чем раньше, способностью своей организации противодействовать киберугрозам, показало исследование глобальной информационной безопасности EY 2021 года. В ходе исследования, проведенного в марте и мае этого года, было опрошено 1010

респондентов по всему миру, из которых 20% - из Азиатско-Тихоокеанского региона, 36% - из Северной и Южной Америки, а остальные 43% - из Европы, Ближнего Востока, Индии и Африки (EMEIA).

Исследование показало, что всего 20% в Азиатско-Тихоокеанском регионе заявили, что группы по кибербезопасности были частью этапа планирования любой инициативы по цифровой трансформации. Респонденты также отметили, что, хотя бизнес-менеджеры признали сильные стороны команды кибербезопасности в традиционных областях, таких как контроль рисков, они не всегда считали ее стратегическим партнером.

Фактически, 71% руководителей кибербезопасности охарактеризовали свои отношения с владельцами бизнеса как нейтральные или негативные. Около 44% заявили, что их взаимодействие с отделами маркетинга и персонала было неудовлетворительным.

Несмотря на появление изощренных кибератак, в отчете EY отмечается, что 57% организаций в регионе не уверены, достаточно ли надежны их средства защиты от кибербезопасности для борьбы с новой тактикой взлома.

Около 73% указали на рост разрушительных атак, таких как программы-вымогатели, за последний год, что значительно выше 47% в отчете за 2020 год.

Еще 47% предупредили, что бюджет их компании на кибербезопасность недостаточен для смягчения проблем, возникших за последние 12 месяцев. Фактически, 41% ожидали серьезного нарушения, которого они могли бы избежать, если бы вложили больше средств в кибербезопасность, по сравнению с 29% в Северной и Южной Америке.

Отчет показал, что респонденты из Азиатско-Тихоокеанского региона выделяли 0,05% своего годового дохода на кибербезопасность, что было аналогично среднемировому уровню 0,04%.

Кибер-лидер EY в Азиатско-Тихоокеанском регионе Ричард Уотсон сказал: «Компании планируют новую волну инвестиций в технологии, чтобы процветать в эпоху после COVID-19. Если кибербезопасность не будет обсуждаться в инвестиционных обсуждениях, угроза будет продолжать расти с годами до Им следует подумать о том, чтобы разделить расходы на кибербезопасность на весь бизнес, чтобы поддержать трансформацию».

Руководитель отдела кибербезопасности EY Asean Стив Лэм добавил, что компании осознают, что «временные технологические решения», внедренные в первые дни карантина, неадекватны для надежной поддержки новых норм в работе.

По словам Лам, в связи с тем, что некоторые части Юго-Восточной Азии все еще находятся в изоляции, такие проблемы для руководителей информационной безопасности в регионе еще больше усугубляются нехваткой и высокой текучестью кадров на местных рынках в области кибербезопасности. Он отметил, что если бы эти руководители смогли заполнить пробелы в талантах, руководители по информационным технологиям могли бы задействовать текущую трансформацию бизнеса и технологий своей компании в ответ на пандемию и добиться улучшений в отношении кибербезопасности организации.

Уотсон сказал: «Директора по информационной безопасности должны принимать трудные решения, пересматривая требования к кибербезопасности,

чтобы лучше соответствовать меняющимся потребностям бизнеса после пандемии COVID-19. Сопоставление стратегии кибербезопасности и профиля рисков своей организации с бизнес-целями и целями ИТ обеспечит согласованность и укрепление стратегических отношений между директорами по информационной безопасности и генеральными директорами., и остальная часть топ-менеджера ".

«Во времена большего недоверия и когда киберфункция находится под более пристальным вниманием, чем когда-либо, у руководителей по информационной безопасности есть возможность лучше продемонстрировать стратегическую важность своей роли и повысить свой авторитет в бизнесе, особенно после пандемии», - сказал он. добавлен.

УДАЛЕННЫЕ МЕРОПРИЯТИЯ УВЕЛИЧИВАЮТ РИСКИ БЕЗОПАСНОСТИ ОБРАЗОВАНИЯ

В отдельной заметке, опубликованной в четверг, Check Point Software Technologies сообщила, что кибератаки на образовательный и исследовательский сектор Юго-Восточной Азии выросли на 28% в июле 2021 года до в среднем 1739 атак в неделю по сравнению с первой половиной 2021 года.

В глобальном масштабе этот рост составил 29% для сектора, при этом Индия стала страной с наибольшей целевой аудиторией, за ней следуют Италия, Израиль, Австралия и Турция. Сектор образования и исследований Индии подвергался в среднем 5 196 атакам в неделю на организацию, что на 22% больше, чем в первом полугодии.

По данным Check Point, в отраслевом разрезе Южная Азия также была наиболее целевым регионом, за ней следовали Восточная Азия и Австралия / Новая Зеландия.

Региональный директор компании-производителя средств безопасности Asean и региональный директор в Корее Теонг Энг Гуан отметил: «Сектор образования в Юго-Восточной Азии подвергся атакам значительно чаще, чем другие отрасли в июле месяце. Школы, университеты и исследовательские центры являются привлекательными целями для киберпреступников, потому что они часто недостаточно ресурсов с точки зрения безопасности.

«Временный переход к дистанционному обучению в короткие сроки усугубляет угрозу безопасности, - сказал Теонг. «Из-за того, что так много учеников входят в систему из своих домашних сетей с помощью личных устройств, текущий школьный сезон представляет ряд новых угроз безопасности, к которым многие не готовы бороться. Организации в секторе образования должны проявлять инициативу в своих стратегиях защиты. Это важно постоянно менять и укреплять свои пароли и использовать технологии, предотвращающие кибератаки, такие как программы-вымогатели». ***(Eileen Yu. Half of APAC firms bypass processes to accommodate remote work // ZDNet (https://www.zdnet.com/article/half-of-apac-firms-waver-on-processes-to-accommodate-remote-work/). 19.08.2021).***

***

**«Опыт в области кибербезопасности пользуется большим спросом. Столкнувшись с такими угрозами, как фишинг, программы-вымогатели и**

**утечки данных, предприятиям нужны сотрудники по информационной безопасности в своих командах, чтобы защитить свои сети от атак.**

Несмотря на то, что есть намерение создать и улучшить команды по кибербезопасности, недавние исследования показывают, как компании часто совершают ошибки при приеме на работу, что приводит к трудностям с набором и удержанием сотрудников по ИТ-безопасности.

Количество незаполненных вакансий не только затрудняет обеспечение безопасности сетей для предприятий, но и влияет на людей, которые уже работают в группах по кибербезопасности, которые, как ожидается, сделают все необходимое для обеспечения безопасности сети, но с небольшими затратами. необходимого персонала.

Это приводит к выгоранию, из-за чего людям становится труднее выполнять свою работу в то время, когда растущая потребность в защите удаленных сотрудников увеличивает их рабочую нагрузку. В некоторых случаях выгорание означает, что люди могут вообще уйти из отрасли, когда их навыки необходимы больше всего.

Итак, почему организации изо всех сил пытаются заполнить вакансии, когда есть рабочая сила, в то время как наем сотрудников по кибербезопасности, возможно, важнее, чем когда-либо прежде? Потому что компании часто не понимают, что они ищут, что приводит к ошибкам при приеме на работу.

Объявления о работе вне сферы кибербезопасности содержат требования к должности, включая опыт и квалификацию. Отделы кадров берут эти шаблоны и применяют их к информационной безопасности, которая часто не соответствует таким же строгим требованиям к квалификации.

Без формальной квалификации можно иметь высокую квалификацию и большой опыт в области кибербезопасности, однако многие компании, пытающиеся нанять сотрудников службы безопасности, считают квалификацию и сертификаты обязательными.

Алисса Миллер, специалист по информационной безопасности бизнеса и публичный докладчик по кибербезопасности, провела обширное исследование практики найма в отрасли, а также выступила с докладом на TED по этому вопросу. Она говорит, что почти три четверти вакансий начального уровня, которые она просматривала, требуют сертификации сертифицированного специалиста по безопасности информационных систем (CISSP), что требует многих лет обучения, стоит денег, чтобы сдать экзамен - и нереально для тех, кто ищет за свою первую работу в отрасли.

«Из описаний предполагаемых должностей начального уровня, на которые я смотрел, 71% из них требуют CISSP. Это не начальный уровень, потому что для получения CISSP нужно иметь пятилетний опыт», - говорит Миллер.

В некоторых случаях компании рекламируют вакансии на стажировку - то, что в обычных обстоятельствах позволяет людям учиться на рабочем месте, одновременно помогая компании. Однако даже когда дело доходит до рекламы стажировок в области кибербезопасности, есть объявления, требующие от соискателя пятилетнего опыта работы в этой области. Людей с многолетним

профессиональным опытом просят устраиваться на работу за небольшую плату или даже бесплатно.

«Если у вас есть пятилетний опыт работы в сфере кибербезопасности, вы больше не стажер, а на тот момент вы - продвинутый профессионал - думаете ли вы, что собираетесь получить пятилетнего ветерана в области кибербезопасности за оплату стажера? Нет., конечно, нет, - говорит Миллер.

Кибербезопасность включает в себя определенный набор навыков, на освоение которых люди потратили время и усилия. Природа отрасли означает, что, когда дело доходит до повышения квалификации, многие профессионалы в области информационной безопасности сделали карьерный путь из-за большого интереса к кибербезопасности, а некоторые из них являются самоучками, демонстрируя способности, необходимые для достижения успеха, даже если у них нет конкретных сертификатов.

Это может сбивать с толку отделы кадров, которые привыкли просматривать и нанимать кандидатов на основании того, что кандидат имеет определенную квалификацию, которой могут не обладать специалисты по информационной безопасности. Кто-то может иметь многолетний опыт работы в отрасли, но если HR не видят, что они считают правильной квалификацией, их заявление может быть отклонено, несмотря на практический опыт.

Короче говоря, кибербезопасность развивается по той же схеме, что и другие профессии в области вычислительной техники и технологий до нее. «Мы прошли через все это с помощью разработки программного обеспечения 10 лет назад, и теперь кибербезопасность - это как раз тот момент», - говорит Адам Энбар, генеральный директор и соучредитель Flatiron School, которая преподает в кампусе и онлайн-учебные курсы по разработке программного обеспечения, науке о данных. и кибербезопасность.

«У вас есть работодатели, которые нанимают, но они действительно не знают, для чего нанимают, и они даже не знают, что искать».

Это не сводится к тому, что опытные профессионалы будут работать за небольшую плату или бесплатно - у некоторых предприятий просто нереалистичные ожидания относительно того, что требуется для работы. Помимо обязательной сертификации, нередко можно увидеть объявления о вакансиях, в которых просят о продолжительном опыте работы в дисциплинах, которые существуют всего несколько лет.

«Описание работы получило, чтобы лучше они должны быть сосредоточены на правильных вещах. - они не могут просить 10 лет Kubernetes. Опыт, когда Kubernetes только существовали в течение шести лет. Есть много примеров таких описаний, которые делают подобные глупости», - говорит Миллер.

Тогда есть вопрос времени. Некоторые компании будут активно нанимать сотрудников после серьезного инцидента, связанного с кибербезопасностью, или потому, что они опасаются стать следующей жертвой масштабной утечки данных, кампании вымогателей или другой кибератаки. В этом сценарии нанимающие компании хотят получить мгновенные результаты от профессионалов в области кибербезопасности с многолетним опытом работы в операционном центре безопасности (SOC).

«Большинство сообщений написано для людей с опытом работы от пяти до десяти лет. Это происходит потому, что работодатели часто начинают вкладывать средства и посвящать время найму профессионалов в области кибербезопасности, когда они сталкиваются с кризисом - и в этот момент вам не нужен кто-то с минимальным», - говорит Кристин Изуакор, основатель и генеральный директор Cyber Pop-up, компании, предоставляющей услуги кибербезопасности по запросу, и инструктор по кибербезопасности для Udacity.

Стратегия, которая была бы лучше, чем попытки паники нанять персонал службы кибербезопасности после инцидента, состояла бы в том, чтобы с самого начала иметь их в штате - людей, которые хорошо знают компанию и могут помочь защитить инциденты от возникновения в первую очередь или могут отреагировать в правильный путь, если что-то пойдет не так.

«Решение состоит в том, чтобы организации были более активными в поиске этих людей для создания команды по кибербезопасности, вместо того, чтобы просто ждать кибератаки или другого кризиса безопасности. При этом у сотрудников есть время, чтобы учиться и расти в ролях», - говорит Изуакор.

Это потребует изменения отношения к найму. Компании не могут просто ожидать, что опытные профессионалы в области кибербезопасности появятся из ниоткуда и согласятся работать с зарплатой начального уровня. Компании должны признать, что они должны начать нанимать людей в самом начале своей карьеры. Хотя у них может быть меньше опыта, они могут учиться на работе и, если о них позаботятся, могут стать положительным вложением средств для организации, даже если у них нет никаких технических знаний с самого начала.

В своем выступлении на TED Миллер объясняет, как такой человек, как бариста, может обладать необходимыми навыками, чтобы преуспеть в карьере в области кибербезопасности. Они могут делать много разных вещей одновременно, готовя и разнося кофе, так что сказать, что они не могут воспользоваться этим опытом и использовать его в роли аналитика безопасности?

«Я ищу кого-то, кто действительно хорошо разбирается в этих множественных входах, например, бариста - они могут взять то множество поступающих вещей и объединить их в задачи, а затем расставить приоритеты и выполнить эти задачи. Вот о чем я прошу аналитик SOC», - говорит она.

Расширяя таким образом поиск сотрудников по кибербезопасности, организации имеют больше шансов диверсифицировать рабочую силу, что может помочь улучшить кибербезопасность для всех, привнося в комнату разные точки зрения и соображения, а также имея возможность лучше реагировать на новые угрозы и вопросы.

«Организациям необходимо искать людей, которые имеют разный опыт и могут адаптироваться к растущему ландшафту угроз и новым вызовам. Разносторонний персонал поможет в борьбе с любыми киберугрозами и развитии существующих кибер-возможностей», - говорит Изуакор, добавляя что инвестиции в обучение этих сотрудников также являются ключевыми.

«Из-за темпов развития технологий постоянное развитие талантов имеет решающее значение. Реализуя надежную программу обучения и повышения квалификации, люди получают возможность учиться и продвигаться по своей

карьере, в то время как организации могут опередить растущую конкуренцию в отрасли за счет развития внутренних талантов ".

Кибербезопасность - жизненно важная часть современного бизнеса, поэтому предприятиям следует вкладывать средства в найм нужных людей. Требование пятилетнего опыта для должности начального уровня не сработает, равно как и упражнение для галочки, требующее определенной квалификации в отрасли, известной тем, что люди присоединяются нетрадиционными способами, и где новые угрозы означают, что всегда есть новые наборы навыков. требуется.

В таком случае, когда дело доходит до найма сотрудников в сфере кибербезопасности, компаниям необходимо заранее подумать. Набор сотрудников - это не то, что нужно делать только для того, чтобы исправить ситуацию после инцидента - это основная часть ведения бизнеса, и к ней следует относиться соответствующим образом. Вот почему необходимо нанимать правильных людей и относиться к ним с уважением и заботой. Совершите ошибку, и ваша существующая команда по кибербезопасности может выгореть и уйти - и единственные люди, которые выиграют, - это киберпреступники». ***(Danny Palmer. Cybersecurity jobs: This is what we're getting wrong when hiring – and here's how to fix it // ZDNet (https://www.zdnet.com/article/cybersecurity-jobs-this-is-what-were-getting-wrong-when-hiring-and-heres-how-to-fix-it/). 20.08.2021).***

***

**«На этой неделе S&P Global Market Intelligence и Immuta опубликовали новое исследование, в котором подчеркивается, сколько крупных организаций пытаются управлять своими данными и использовать их.**

Отчет, проведенный 451 Research, показал, что 55% респондентов заявили, что данные, которые они получают для анализа, часто устарели или устарели к тому времени, когда они до них доходят. Компания 451 Research опросила 525 лидеров по данным в США, Канаде, Великобритании, Германии и Франции. Все участники опроса работают в организациях, в которых работает более 1000 сотрудников.

Результаты опроса отражают широкую дискуссию среди предприятий о балансе эффективного использования данных с конфиденциальностью и безопасностью данных. 84% респондентов заявили, что, по их мнению, требования к конфиденциальности и безопасности данных ограничат доступ к данным в их организациях в течение следующих 24 месяцев.

Около 40% респондентов, работающих в качестве поставщиков данных, заявили, что им не хватает персонала или навыков для работы на своих должностях, а почти 30% указали на отсутствие автоматизации как на проблему.

По крайней мере, 90% респондентов заявили, что качество данных и доверие становятся более важными, чем объем или количество данных. Роль директора по данным становится все более заметной в организациях. Большинство респондентов заявили, что у директора по данным был прямой доступ к генеральному директору.

Согласно опросу, 60% респондентов заявили, что в их организациях есть директор по данным, а 40% - нет. Цифры также соответствовали размеру

организации, при этом более крупные предприятия с большей вероятностью имели главного специалиста по данным.

«Результаты очевидны. По мере того, как рабочие процессы и процессы обработки данных со временем становятся более сложными - и по мере роста организационного спроса на данные - в цепочке поставок данных возникают явные точки трений», - сказала Пейдж Бартли, старший аналитик 451 Research.

«Главный из них - поставщики данных, которые имеют ограниченные ресурсы, нехватку навыков и небольшую автоматизацию, которым поручено пытаться доставить постоянный поток соответствующих данных растущему числу потребителей данных».

Опора на облако также растет, согласно опросу, который показал, что 76% респондентов работали в организациях, которые чаще использовали облачные технологии данных для хранения, вычислений и совместного использования в течение следующих 24 месяцев. Из тех, кто все еще пытается перейти в облако, 43% заявили, что это связано с безопасностью, 40% указали на проблемы с соблюдением требований, а 35% заявили, что конфиденциальность данных является проблемой.

В целом 65% респондентов заявили, что данные стали важнее для их собственной работы сейчас, чем когда-либо за последние 24 месяца.

Более 71% заявили, что количество потребителей данных в их организациях с течением времени неуклонно растет. Еще 73% добавили, что большему количеству потребителей человеческих и машинных данных потребуется доступ к данным в течение следующих двух лет.

Согласно опросу, на изменения в потреблении и развертывании данных также влияет законодательство, которое обнаружило, что 84% заявили, что на их предприятие распространяются такие правила, как GDPR и HIPAA.

Конфиденциальность и безопасность данных также требуют изменений. Более 83% заявили, что правила безопасности данных ограничат их доступ к данным в их организации в течение следующих двух лет.

Респонденты также жаловались на тот факт, что данные не были доступны в реальном времени, выражая недовольство плохо подготовленными группами обработки данных, неспособными предоставить инструменты самообслуживания для работы с данными. Почти 40% заявили, что их данные доступны только в определенный момент времени.

Более 62% респондентов заявили, что они использовали бесплатные облачные инструменты для решения задач, связанных с данными.

«Респонденты из регулируемых организаций также с гораздо большей вероятностью сообщили, что их организация использует стратегию внедрения «сначала облако» (31%) или «облако вперед» (45%), в то время как респонденты из нерегулируемых организаций непропорционально чаще сообщали об использовании облачных технологий. консервативная (46%) или скептическая (9%) стратегия», - говорится в отчете. «Предположение, что регулируемые отрасли или фирмы склонны уклоняться от облачных технологий, в лучшем случае устарело».

По мнению 65% респондентов, организации также испытывают трудности с управлением доступом к данным и их использованием.

Генеральный директор Immuta Мэтт Кэрролл сказал, что отсутствие связи между поставщиками и потребителями данных подчеркивает насущную проблему для предприятий и государственного сектора по повышению скорости и доступа к данным.

«Результаты ясно показывают, что понимание и ценность для бизнеса не могут быть быстро и легко получены из данных, если они не могут быть совместно использованы, смоделированы и проанализированы без проблем», - сказал Кэрролл.

«Этот отчет подтверждает то, что испытали наши клиенты. Хорошая новость заключается в том, что, понимая эти болевые точки, организации могут решать их и двигаться вперед, чтобы максимизировать ценность корпоративных данных и минимизировать риски. Инвестиции в автоматизацию и масштабируемость устраняют препятствия на пути внедрения облачных технологий и открывает двери для более эффективного доступа к данным и их использования для улучшения бизнес-результатов». ***(Jonathan Greig. Survey shows 40% of organizations don't have a chief data officer // ZDNet (https://www.zdnet.com/article/40-of-orgs-dont-have-a-chief-data-officer/). 13.08.2021).***

***

**«Агентство по кибербезопасности и безопасности инфраструктуры (CISA) выпустило сегодня новое загружаемое руководство по обучению сотрудников кибербезопасности, чтобы помочь будущим и нынешним специалистам в области кибербезопасности и информационных технологий (ИТ) наметить успешный карьерный путь.** Это руководство представляет собой универсальный источник информации и ресурсов, которые помогут профессионалам начать и / или продвигать свою карьеру в области кибербезопасности посредством обучения.

«Персонал, занимающийся кибербезопасностью, находится на переднем крае безопасности нашей страны, - сказал Эрик Голдштейн, исполнительный помощник директора по кибербезопасности CISA. «Наша цель - предоставить необходимые инструменты, чтобы эта критически важная рабочая сила знала, где найти доступное обучение, которое поможет им быть хорошо подготовленными и квалифицированными. Это исчерпывающее руководство поможет людям определить направление работы и выявить области для роста ».

Используя это руководство, специалисты по кибербезопасности поймут применимые рабочие роли, задачи и знания, навыки и способности (KSA), которые являются ключами к успеху; и открыть для себя возможности обучения и профессионального развития для развития навыков и максимального раскрытия потенциала. Также они найдут:

Сертификаты кибербезопасности начального, среднего и продвинутого уровней

Тренинги по профессиональному развитию и курсы подготовки к сертификации

Опыт и практические возможности

Дополнительные кибер / ИТ-ресурсы со всего федерального правительства

Руководство по обучению сотрудников кибербезопасности - это первый шаг, который поможет профессионалам наметить путь к будущему успеху в сообществах кибербезопасности на федеральном уровне и уровне штатов, на местном, племенном и территориальном уровнях (SLTT). Загрузите и просмотрите новое руководство по обучению сотрудников кибербезопасности или узнайте больше о тренингах и упражнениях CISA по кибербезопасности по адресу: cisa.gov/cybersecurity-training-exercises. CISA стремится помогать людям развивать свою карьеру, предоставляя им доступ к обучению и инструментам для продвижения по службе». ***(CISA RELEASES NEW CYBER TRAINING GUIDE // Cybersecurity and Infrastructure Security Agency (CISA) (https://www.cisa.gov/news/2021/08/06/cisa-releases-new-cyber-training-guide). 09.08.2021).***

***

**«В апреле 2021 года Министерство труда выпустило руководство по кибербезопасности для планирования доверенных лиц и участников в виде трех отдельных документов: Советы по найму поставщиков услуг с сильной практикой кибербезопасности; Лучшие практики программы кибербезопасности; и Советы по сетевой безопасности.** Примечательно, что это руководство применимо как к пенсионным планам, так и к планам здравоохранения / социального обеспечения и, по-видимому, представляет собой дополнительный уровень соответствия выше HIPAA.

Первые два документа включали в себя контрольные списки положений, которые спонсоры плана должны искать в своих контрактах с поставщиками услуг, такими как сторонние администраторы (TPA), попечители, хранители, инвестиционные менеджеры и тому подобное. Третий документ был больше ориентирован на отдельных лиц и включал типичные предложения, такие как частая смена паролей и отказ от обмена информацией для входа в систему с другими.

*Способы применения руководства DOL на практике*

За последние несколько месяцев мы поговорили с несколькими поставщиками услуг от имени наших клиентов и получили постоянное сообщение: «Мы работаем над соблюдением нового руководства». Фактически, что касается сотрудников пенсионных планов, мы понимаем, что они работают со своими торговыми группами, чтобы определить, выполнимы ли некоторые из рекомендаций DOL и какой ценой. В то же время мы понимаем, что они изучают свои системы, чтобы определить, какие улучшения безопасности можно внести и в какие сроки.

Однако, в отличие от большинства случаев, DOL официально не запрашивал комментарии от юридических лиц, TPA, доверительных управляющих, кастодианов или инвестиционных менеджеров перед выпуском этого руководства. Даже когда DOL использует этот подход, он обычно использует подход «белой книги», когда вносит свои предложения и запрашивает комментарии. Изучив отзывы, DOL часто пересматривает или дополняет свое первоначальное руководство.

На этот раз этого не произошло, и, что важно, из нескольких ресурсов мы понимаем, что DOL спрашивает о кибербезопасности в ходе регулярных проверок и аудитов. То есть DOL не указал отложенную дату вступления в силу, но считает, что это руководство имеет силу сейчас.

*Как фидуциары могут готовиться сейчас*

Хотя такое быстрое развитие вызывает беспокойство, мы считаем, что разумным фидуциарам следует рассмотреть следующие шаги:

Свяжитесь с каждым из ваших поставщиков и спросите, где они проводят оценку и внедрение Руководства по кибербезопасности DOL, и получите твердые обязательства относительно того, когда ожидать появления документации.

Спросите этих поставщиков, определили ли они уже, что будут соблюдать или не будут соблюдать какие-либо конкретные аспекты руководства.

Изучите контракты с поставщиками, чтобы определить, какая защита кибербезопасности существует в настоящее время, и подумайте, есть ли конкретные недостатки, которые можно устранить, прежде чем получить сообщение от поставщиков.

Отслеживайте общение и включайте статус каждого поставщика в регулярные собрания и протоколы заседаний комитета администраторов плана.

Обратите внимание, что руководство по кибербезопасности DOL является очень подробным и не содержит подробностей. Это может затруднить определение того, что именно должны делать спонсор плана и поставщик. Например, HIPAA предоставляет специальное правило для «регистрационной информации». Эта фраза означает довольно базовую информацию о том, кто является участником плана медицинского страхования, например, имена лиц, на которые распространяется страховое покрытие, и стоимость выбранного ими варианта плана медицинского обслуживания. Он не включает подробную информацию о претензиях. Согласно HIPAA, информация о регистрации обычно не считается «защищенной медицинской информацией» («PHI»). Таким образом, если есть нарушение информации о зачислении, о нем не нужно сообщать. Информация о регистрации не обязательно должна соответствовать строгим и подробным Правилам безопасности HIPAA. Это хорошо с точки зрения спонсора плана.

Содержит ли руководство по кибербезопасности DOL аналогичную концепцию «базовой» информации, например, участвует ли конкретный сотрудник (например, «Джо Смит») в пенсионном плане работодателя? Не ясно. В руководстве по кибербезопасности DOL упоминается множество вещей, которые необходимо защищать (включая «данные участников»; «личную информацию»; «конфиденциальную информацию»; «личную информацию»; «служебную информацию»; «информацию»; «конфиденциальную информацию» и «данные»). Ни один из этих терминов не определен. Возможно, некоторые из них - например, «конфиденциальная информация», которая подразумевает, что некоторая информация, относящаяся к плану, может не быть «конфиденциальной», - могут позволить спонсору плана утверждать, что новое руководство по кибербезопасности DOL не применяется к этому конкретному набору информации. Дальнейшие указания DOL будут приветствоваться». ***(Mike Wieber, John Barlament. How DOL's Cybersecurity Guidance Impacts Retirement and***

***Health/Welfare Plans // Quarles & Brady LLP (https://www.quarles.com/publications/how-dols-cybersecurity-guidance-impacts-retirement-and-health-welfare-plans/). 19.08.2021).***

***

**«Управление цепочкой поставок - сложный процесс, в котором участвует множество партнеров, организаций и технологических систем.** Без обеспечения последовательного подхода к надежной превентивной кибербезопасности во всех этих отдельных объектах постоянно вырисовывается риск атак.

Одна из самых больших угроз - это недостаточное внимание к киберзащите, существующей в операциях партнеров-поставщиков. Для покупателей усилия по привлечению должного уровня внимания к предотвращению внутренней атаки становятся излишними, если на внедренный процесс отрицательно влияет атака на операции партнера - сбои часто сразу же сказываются на клиентах (будь то в отношении для них, получающих продукт / услугу или их данных, которые были скомпрометированы).

Как они могут наладить отношения с другими отделами, чтобы гарантировать, что процессы адаптированы и любые атаки не увенчаются успехом?

Межведомственное понимание последствий кибератак - особенно в том, что касается удержания клиентов и потери доходов - имеет жизненно важное значение и не может быть достигнуто с помощью разовых учебных упражнений или презентаций. Вместо этого он должен включать в себя постоянную программу обучения, презентации или общения по распознаванию признаков нападения - и, в первую очередь, запланированные шаги по минимизации любых последствий, если они произойдут.

Могут существовать препятствия, которые необходимо преодолеть, когда речь идет о переходе на отдельные отделы, но это можно преодолеть за счет подхода к проблеме сверху вниз, начиная с уровня совета директоров, который признает серьезность угрозы прибыльности и репутации.

Как компании могут работать со своими поставщиками над этим, чтобы снизить риски и усилить надзор? Должны ли они проводить регулярные проверки систем и процессов поставщиков?

Ключевым способом защиты от этого риска для покупателей является обеспечение того, чтобы проверенные уровни кибербезопасности являлись частью критериев для приобретения новых партнеров и взаимоотношений с внешними цепочками поставок. Согласовав с самого начала формализованный подход к превентивной кибербезопасности, который охватывает основные стратегические, технологические и связанные с обучением элементы, риск внешней атаки на партнера, компрометирующей цепочку поставок, сводится к минимуму». ***(SARAH RIDING. What are the biggest cyber security risks for those working in procurement or supply management? // LoupedIn (https://loupedin.blog/2021/08/what-are-the-biggest-cybersecurity-risks-for-those-working-in-procurement-or-supply-management/#page=1). 17.08.2021).***

***

**«Управление суперинтенданта финансовых учреждений (OSFI) только что выпустило обновленные требования, регулирующие, как финансовые учреждения, регулируемые на федеральном уровне (FRFI), должны раскрывать и сообщать OSFI об инцидентах, связанных с технологиями и кибербезопасностью.** Консультации, которые затрагивают банки, страховые компании и кредитные союзы, регулируемые на федеральном уровне, заменяют Информационное сообщение об инцидентах кибербезопасности от января 2019 года, которое вступило в силу в марте 2019 года. С одновременным выпуском обновленной самооценки кибербезопасности OSFI OSFI значительно ужесточили свои требования, демонстрируя растущую озабоченность потенциальным воздействием кибербезопасности на финансовую систему и отдельные финансовые учреждения.

Изменения, внесенные OSFI в обновленные рекомендации, потребуют от FRFI внесения изменений в свои внутренние процессы управления инцидентами, соглашения и шаблоны, используемые со сторонними поставщиками услуг. Изменения можно увидеть в красной линии, сравнивающей рекомендации 2019 года и 2021 года, показанные ниже.

*Ниже кратко излагаются некоторые из значительных изменений.*

Информационный бюллетень содержит новую явную цель, которая заключается в поддержке «скоординированного и комплексного подхода к осведомленности OSFI и реагированию на инциденты, связанные с технологией и кибербезопасностью в финансовых учреждениях, регулируемых на федеральном уровне (FRFI)».

В данном информационном бюллетене «технологический инцидент или инцидент кибербезопасности» определяется «как инцидент, который оказывает влияние или может повлиять на работу FRFI, включая его конфиденциальность, целостность или доступность его систем и информации». Это заменяет определение в предыдущем сообщении, которое нацелено на инциденты, только «потенциально способные или, по оценке, могут существенно повлиять на нормальную работу FRFI».

Консультант также изменяет пороговое значение и время для сообщения об инцидентах безопасности в OSFI. Предыдущие рекомендации требовали сообщать об инцидентах, если они были оценены FRFI как «высокого или критического уровня серьезности». Согласно Рекомендации, FRFI должны сообщать OSFI обо всех инцидентах, связанных с технологией или кибербезопасностью. Консультативный совет требует отчитываться «в течение 24 часов или, если возможно, раньше». Как написано, это, по-видимому, требует отчетности об инциденте даже до того, как FRFI узнает об инциденте или получит возможность подтвердить или классифицировать уровень его серьезности. Это изменение по сравнению с требованием в соответствии с предыдущим уведомлением сообщать о происшествии «как можно скорее, но не позднее, чем через 72 часа». после определения инцидента необходимо сообщить. Новое требование к отчетности намного строже, чем в соответствии с PIPEDA, согласно которому уведомления

должны «направляться при первой возможности после того, как организация определит, что нарушение имело место».

OSFI также внесла значительные изменения в критерии сообщения об инциденте. Критерии отчетности являются более многочисленными и включают критерии, которые, вероятно, также приведут к большему количеству инцидентов, подлежащих отчетности. В соответствии с рекомендациями инцидент, о котором необходимо сообщить, может иметь одну или несколько из следующих характеристик:

Воздействие имеет потенциальные последствия для других FRFI или канадской финансовой системы;

Воздействие на системы FRFI, влияющие на расчеты, подтверждения или платежи на финансовых рынках (например, инфраструктуру финансового рынка), или влияние на платежные услуги;

Воздействие на операции, инфраструктуру, данные и / или системы FRFI, включая, помимо прочего, конфиденциальность, целостность или доступность информации о клиентах;

Сбои в работе бизнес-систем и / или операций, включая, помимо прочего, сбои в работе коммунальных служб или центров обработки данных, а также потерю или ухудшение связи;

Операционное воздействие на ключевые / критические системы, инфраструктуру или данные;

Были активированы группы или планы аварийного восстановления, или сторонний поставщик сделал заявление о сбое, которое влияет на FRFI;

Оперативное влияние на внутренних пользователей, которое оказывает влияние на внешних клиентов или бизнес-операции;

Количество затронутых внешних клиентов растет; неизбежно негативное влияние на репутацию (например, раскрытие информации общественности и / или СМИ);

Воздействие на третью сторону, влияющую на FRFI;

Была активирована команда или протоколы FRFI по управлению технологиями или киберинцидентами;

Инцидент, о котором было сообщено Совету директоров или высшему / исполнительному руководству;

Об инциденте FRFI было сообщено:

Офис уполномоченного по вопросам конфиденциальности;

другой департамент федерального правительства (например, Канадский центр кибербезопасности);

другие местные или иностранные надзорные или регулирующие организации или агентства;

любые правоохранительные органы;

обратился к внутреннему или внешнему консультанту

Инцидент FRFI, по которому было возбуждено требование киберстрахования;

Инцидент, который FRFI оценивает как высокую или критическую серьезность, уровень или ранжированный Приоритет / Серьезность / Уровень 1 или 2 на основе внутренней оценки FRFI; или

Инциденты, связанные с технологией или кибербезопасностью, которые нарушают внутренний аппетит к риску или пороговые значения.

В случае инцидентов, которые не соответствуют или не соответствуют конкретным критериям, перечисленным выше, или когда FRFI является неопределенным, рекомендуется уведомлять OSFI в качестве меры предосторожности.

Приложение 1 к Информационному бюллетеню содержит неполный список примеров инцидентов, о которых необходимо сообщить, описания сценариев и воздействий. Сценарии включают кибератаки, доступность и восстановление услуг, взлом со стороны третьих лиц и угрозы вымогательства.

Как и в случае с предыдущими рекомендациями, FRFI должны предоставлять обновления после первоначального раскрытия информации в OSFI. Предварительная рекомендация требовала отчетности до тех пор, пока «не будут предоставлены все существенные подробности инцидента». Консультативный совет отказался от стандарта существенности. В предыдущем уведомлении содержался подробный список того, какая информация должна быть сообщена в OSFI. Консультативный комитет заменил этот список новой формой отчетности и разрешения инцидентов.

Информационное сообщение теперь также содержит новые потенциальные санкции для FRFI, которые не сообщают об инцидентах, как ожидалось в Информационном сообщении. Теперь «Неспособность сообщить об инцидентах, как описано выше, может привести к усилению надзорного надзора, включая, помимо прочего, усиление деятельности по мониторингу, включение в списки наблюдения или постановку FRFI».

*Комментарии*

Многие организации, ведущие свою деятельность в Канаде, уже обязаны сообщать о нарушениях данных, например о общеприменимом нарушении обязательств по уведомлению о гарантиях безопасности в соответствии с Законом о защите личной информации и электронных документах (PIPEDA). PIPEDA требует уведомлений Уполномоченного по вопросам конфиденциальности и отдельных лиц, если «в данных обстоятельствах разумно полагать, что нарушение создает реальный риск причинения значительного вреда человеку», как это определено в PIPEDA.

У FRFI есть дополнительные требования к отчетности для своего регулирующего органа (OSFI) с марта 2019 года. Консультативный совет обновляет эти требования, снижая порог отчетности. Кроме того, несмотря на то, что кибербезопасность является основным направлением Информационного бюллетеня, она также включает риски, связанные с технологическими сбоями, что значительно увеличивает количество типов инцидентов, о которых необходимо сообщать.

Обязательства по консультированию накладываются на другие обязательства по обеспечению безопасности, установленные OSFI для FRFI. Например, в

соответствии с Руководством OSFI по аутсорсингу B-10, ожидается, что FRFI заключат контракт с поставщиком услуг на обеспечение безопасности, которое «будет соизмеримо с безопасностью FRE и должно соответствовать разумным стандартам в данных обстоятельствах». OSFI также «ожидает наличия соответствующих средств защиты и защиты конфиденциальности данных». OSFI также рекомендует FRFI использовать обновленную самооценку кибербезопасности или аналогичные инструменты для оценки своего текущего уровня кибербезопасности, а также для разработки и поддержания эффективных методов кибербезопасности.

Консультативный совет потребует от FRFI обновить свои внутренние технологии и политику и процедуры инцидентов кибербезопасности, чтобы обеспечить отправку отчетов в OSFI при необходимости. Кроме того, поскольку почти все финансовые учреждения, регулируемые на федеральном уровне, в Канаде полагаются на третьи стороны в предоставлении им услуг, таких как аутсорсинг, SAAS, обработка платежей и облачные сервисы, контракты с третьими сторонами, возможно, потребуется обновить, чтобы они соответствовали этим новым требованиям. Для соглашений о шаблонах также могут потребоваться некоторые обновления». ***(Barry B. Sookman. OSFI Advisory tightens technology and cyber security incident reporting requirements // McCarthy (https://www.mccarthy.ca/en/insights/blogs/techlex/osfi-advisory-tightens-technology-and-cyber-security-incident-reporting-requirements#page=1). 17.08.2021).***

***

**«Компании, в том числе стартапы, ориентированные на технологии, часто тратят много времени и денег на стратегию кибербезопасности.** Они могут использовать новейшие, лучшие инструменты и технологии, но они не помнят чего-то важного - человеческий фактор часто является самым большим риском кибербезопасности.

Это было особенно очевидно, поскольку многие люди работали удаленно во время пандемии.

Работодатели несут огромные убытки, связанные с кибербезопасностью, часто из-за человеческой ошибки или отсутствия обучения и знаний о передовых методах кибербезопасности среди сотрудников, включая руководителей высокого уровня.

До тех пор, пока вы не научитесь понимать человеческий фактор кибербезопасности, у вас не будет полностью успешной стратегии, и ваш стартап окажется под угрозой.

Ниже приведены некоторые из ключевых вещей, которые вам следует знать за пределами сугубо технических вопросов. Это человеческие компоненты кибербезопасности, которые так же важны, как и используемые вами технологии.

*Программы повышения осведомленности о безопасности*

Важным первым шагом, независимо от того, являетесь вы стартапом или нет, является наличие общей программы повышения осведомленности о кибербезопасности.

Осведомленность о безопасности не связана с обучением. Вместо этого он больше ориентирован на более широкую культуру безопасности в вашей организации.

Вся ваша бизнес-культура построена вокруг понимания каждым своей роли в кибербезопасности и шагов, которые они должны предпринимать в своей повседневной работе.

Программы повышения осведомленности - это тоже не о каком-то конкретном инструменте. Эти программы повышения осведомленности могут развиваться и меняться по мере необходимости, и они начинаются сверху, а это означает, что вам нужно моделировать поведение, которое вы хотите видеть у своих сотрудников.

Вы можете связать свою культуру кибербезопасности с другими элементами корпоративной культуры. Например, вы можете сделать так, чтобы ваши сотрудники могли поступать правильно, что выходит за рамки кибербезопасности.

*Обучение*

Обучение - это особый элемент программы повышения осведомленности о безопасности, но это не одно и то же.

С помощью программы обучения безопасности вы выходите за рамки высокоуровневого внимания к кибербезопасности, а вместо этого вы обучаете сотрудников конкретным методам и предоставляете им актуальную информацию для повседневной работы.

При создании программы обучения вам необходимо иметь конкретные и измеримые цели для каждого шага на этом пути.

Одна из больших ошибок, которую совершают даже организации корпоративного уровня в отношении обучения сотрудников кибербезопасности, заключается в том, что у них нет метрик для определения успеха или неудачи, поэтому они в конечном итоге не знают, где можно улучшить.

Когда вы создаете учебные программы для своих сотрудников, вы должны изо всех сил стараться познакомить их с тем, где они находятся с точки зрения их стиля обучения. Электронное обучение может быть хорошим вариантом, потому что оно позволяет вашим сотрудникам учиться в таком темпе и в удобной для них форме.

По ходу дела получайте постоянную обратную связь. Узнайте больше о том, что вашим сотрудникам нравится и что не нравится в вашем обучении кибербезопасности, чтобы вы могли настраивать его по ходу дела.

*Подключите кибербезопасность к высшей цели*

Скорее всего, ваши сотрудники выбрали работу в вашем стартапе, потому что им нужна целеустремленность. Добавление целеустремленности ко всему, что делают ваши сотрудники, будет мотивировать их и находить отклик у них, и это не исключает кибербезопасности.

Например, сообщите каждому из своих сотрудников, что они играют жизненно важную роль в защите данных и информации вашей компании. Взлом не просто будет дорогостоящим. Это также может нанести ущерб вашему бренду и репутации, чем, вероятно, гордятся ваши сотрудники.

Поймите человеческие ловушки

Когда дело доходит до кибербезопасности, ваша рабочая сила может быть вашей самой сильной стороной, но вы также должны быть честны с собой в отношении человеческих слабостей.

Все мы люди, и это может привести к рискам кибербезопасности. Когда вы честны с собой в отношении этих рисков, это дает вам больше возможностей для защиты от них.

Например, прискорбная реальность заключается в том, что лень может быть причиной рисков для кибербезопасности.

Например, ваши сотрудники могут работать удаленно и хуже использовать свои протоколы безопасности.

Люди тоже могут просто ошибаться. Вот почему такая, казалось бы, прозрачная вещь, как фишинг, остается одним из основных способов получения киберпреступниками доступа к компаниям и данным.

*Что все это значит для вашего стартапа?*

Подходите ко всему, что вы делаете, в первую очередь с учетом человеческого фактора. Кибербезопасность - не исключение. Отсюда вы можете разработать более надежную стратегию кибербезопасности, включающую также технологии». ***(Joe Silverman. Understanding the Human Element of Cybersecurity // New York Computer Help (https://www.newyorkcomputerhelp.com/blog/2021/08/27/understanding-the-human-element-of-cybersecurity/). 27.08.2021).***

***

**«Мир стал свидетелем наихудших видов кибератак, которые поставили под угрозу нашу личную конфиденциальность, украли личную информацию и привели к потере бизнеса и производительности в миллиарды долларов.** За последние пять лет произошло увеличение числа кибератак со стороны домашних хакеров, а с пандемией риск только увеличился вместе с удаленной работой. Риск кибератак требует принятия надлежащих мер безопасности, таких как назначение министра кибербезопасности для правительств, который будет защищать людей и организации.

Единственный способ защитить Интернет - это для всех правительств серьезный подход к кибербезопасности. Это означает создание министра кибербезопасности в каждом правительстве для наблюдения за практикой кибербезопасности в своей стране. Это единственный способ для правительств быть уверенным в том, что все страны знают о методах кибербезопасности.

Министр кибербезопасности - это не новость, но это должно происходить повсюду, поскольку все больше людей полагаются на технологии и Интернет, чем когда-либо прежде. Аргумент в пользу такой позиции прост: наше современное общество работает на компьютерах и сетях, так что может ли лучше защитить его, чем опытный лидер, понимающий важность национальной безопасности?

Действия правительства в поддержку инициатив в области кибербезопасности

Некоторые страны недавно назначили программы или руководителей руководителями отдела кибербезопасности.

В 2018 году правительство Канады создало Канадский центр кибербезопасности (Cyber Center) в качестве национального органа страны по кибербезопасности и реагированию на киберугрозы. В рамках Национальной стратегии кибербезопасности Канады Киберцентр будет предоставлять консультации и рекомендации предприятиям и всем канадцам в качестве центрального надежного источника информации для правительства.

После пандемии правительства стали уделять больше внимания реализации мер безопасности для кибербезопасности. В ноябре 2020 года ОАЭ учредили новый национальный совет по кибербезопасности для разработки политики и законов, направленных на усиление кибербезопасности. Премьер-министр Рашид Аль Мактум заявил, что безопасность в цифровом пространстве так же важна, как и безопасность в различных областях.

Точно так же в ноябре 2020 года британское правительство объявило, что министерство обороны, правительство и штаб-квартира коммуникаций объединят усилия для создания партнерства: Национальные киберсилы (NCF). Их цель - помочь предприятиям и правительственным организациям защитить себя от киберугроз, включая нарушение работы или разрушение систем связи, представляющих угрозу безопасности. Это изменение такта было вызвано многими причинами; главная из них - рост числа киберинцидентов как внутри страны, так и за рубежом.

*Почему каждой организации нужна выделенная кибер-команда*

Почему каждой организации нужна назначенная кибер-команда? Ответ заключается в том, что кибербезопасность стала самой важной проблемой безопасности. Быстрый рост технологий происходит быстрее, чем любой другой технологический прогресс, с которым мы столкнулись, а кибератаки становятся все более частыми и изощренными с каждым днем. Кибербезопасность - не совсем новая тема для обсуждения. Тем не менее, в последнее время он стал популярным, поскольку хакеры во всем мире становятся все более изощренными. Поскольку наша жизнь все больше зависит от технологий и Интернета, нет права на ошибку.

Target кибератаки обеспечивает только один пример уязвимости, с которыми сталкиваются организации. Короче говоря, в период с 27 ноября по 15 декабря 2013 года в филиале розничной сети в США произошло нарушение безопасности. Хакеры украли имена, адреса и номера телефонов клиентов, а также номера платежных карт и коды проверки кредитных карт и использовали эту информацию для кражи денег с банковских счетов клиентов. В целом пострадали около 40 миллионов счетов клиентов с платежными картами.

Эта кибератака обошлась Target в 18,5 млн долларов США. Тем не менее, худшее последствие заключалось в том, что это повредило репутации розничного продавца, заставив его клиентов чувствовать себя неуверенно в отношении своей личной информации и заставив их не доверять Target и другим крупным розничным торговцам. Инцидент с Target - лишь один из многих примеров того, как крупные компании имеют уязвимости в системе безопасности, которые могут использовать хакеры. Это событие послужило толчком для разработки компанией комплексной программы информационной безопасности, включая наем руководителя или должностного лица, ответственного за выполнение программы.

*Квалификация лидера в области кибербезопасности*

Каждая система информационных и коммуникационных технологий (ИКТ) уязвима для атак. В современном мире компьютерные сети стали настолько сложными, что знания - единственный инструмент, которым мы, люди, можем защитить их от кибератак. Алгоритмы, криптография, безопасность данных и конфиденциальность имеют решающее значение для понимания кибербезопасности.

Кибербезопасность требует другого набора навыков и потребует совершенно нового типа политика в правительстве. Нынешним политикам не хватает математической подготовки, которая им необходима, чтобы досконально понять сложность киберпространства. Дело не только в понимании технологии. Кибербезопасность настолько сложна и быстро меняется, что министрам необходимо разбираться в большом количестве дисциплин, включая социальные науки, поведенческую науку, психологию и экономику, чтобы понять, как киберпространство можно использовать как против правительства, так и для него.

*Специалисты по кибербезопасности*

Поскольку ни один министр или физическое лицо не может быть осведомлено абсолютно обо всем в сфере кибербезопасности, правительствам и предприятиям в равной степени необходима команда консультантов по кибербезопасности.

Команда по кибербезопасности похожа на любую другую команду: в нее входят разные члены, каждый из которых обладает уникальными навыками. Наиболее важными из них являются инженеры по безопасности, которым поручено защищать системы и сети организации. Инженер по безопасности должен быть знаком с технологиями, которые использует организация, а также с угрозами, для борьбы с которыми она предназначена. Однако разработка подробного плана безопасности, подобного этому, может быть чрезвычайно сложной и трудоемкой. Навыки инженера по безопасности различаются, но включают в себя знание методов и процессов безопасности, таких как реагирование на инциденты и тестирование на проникновение, а также знания в области безопасности ИТ и ОТ.

Хотя некоторые страны недавно назначили министра кибербезопасности для решения вопроса о том, что кибератаки становятся все более распространенными и изощренными, принятие руководящих ролей в области кибербезопасности должно распространяться на большие и малые организации. Понимая экономические последствия закрытия предприятий и приостановки операций, правительствам следует уделять больше внимания поиску решения, будь то министр кибербезопасности или что-то еще». ***(Anas Chbib. Why every government should have a cybersecurity minister // BetaNews, Inc. (https://betanews.com/2021/08/27/government-need-cybersecurity-minister/). 27.08.2021).***

***

**«NortonLifeLock и Avast объявили о сделке на 8 миллиардов долларов, согласно которой два поставщика услуг по кибербезопасности потребителей объединят свои соответствующие предприятия.** Эти двое подчеркнули

«убедительное стратегическое и финансовое обоснование» слияния, но каково реальное влияние на клиентов и отрасль кибербезопасности?

Хотя дьявол кроется в деталях, но есть некоторые опасения, что объединение двух основных игроков может привести к росту цен и облегчить жизнь киберпреступникам.

*Что дальше для клиентов?*

Сделка, о которой было объявлено 10 августа, еще не была одобрена регулирующими органами, она станет поворотным моментом для обеих компаний. По его условиям, NortonLifelock со штаб-квартирой в Аризоне приобретет все акции Avast, стоимость которых оценивается в 8,1-8,6 млрд долларов. Главный исполнительный директор NortonLifeLock Винсент Пилетт останется руководителем, а босс Avast Ондржей Влчек станет президентом новой компании. Подавляющее большинство (87%) из ее 500 миллионов клиентов будут происходить из Avast, а штаб-квартира новой компании будет находиться в столице Чешской Республики Праге и Темпе, штат Аризона.

Во многих отношениях рынок созрел для такой крупной сделки - учитывая огромное количество независимых игроков в сфере безопасности, которые продают продукцию потребителям. Несмотря на то, что за последние годы Avast сменил несколько восточноевропейских конкурентов с «freemium» на «премиум», в том числе AVG и Avira, сделав его привлекательной перспективой для слияний и поглощений (M&A).

Итак, чего ожидать покупателям? С одной стороны, они могут получить выгоду от доступа к расширенному портфелю продуктов, который стремится объединить заявленную силу Avast в области конфиденциальности и самооценку NortonLifeLock, направленную на идентификацию. По мере того, как компании начинают строить общее будущее, клиенты также будут надеяться на большую ясность в этой дорожной карте.

Индекс киберрисков Trend Micro за первую половину 2021 года показал, что данные о потребителях и клиентах занимают 4-е место в мире по уровню риска. Таким образом, у компаний должны быть стратегии для защиты этих ценных данных. Тем не менее, объединение крупных поставщиков в области кибербезопасности также создает новые риски для клиентов. Например, если фирмы объединят свои соответствующие кодовые базы, злоумышленникам станет проще разработать способы обхода этих продуктов. Утверждается, чтоAvast и AVG сделали это после сделки M&A, и сегодня бренды получают одинаковые баллы в большинстве тестов AV, «потому что внутри тестируется один и тот же код». В том же отчете предполагается, что численность персонала в новой фирме Norton-Avast может быть сокращена до 25%. Если это приведет к сокращению числа исследователей вредоносных программ, то могут пострадать и инновации, что сделает клиентов менее защищенными.

*Как развивается компания Trend Micro*

Trend Micro предлагает широкий спектр ведущих в отрасли инструментов кибербезопасности, предназначенных для защиты всех аспектов цифровой жизни потребителей - от ноутбуков и мобильных устройств до сетей умного дома, паролей и онлайн-безопасности для детей и семей. Есть несколько причин, по

которым сделка NortonLifeLock-Avast вряд ли вызовет серьезную угрозу этому бизнесу.

Во-первых, большая часть доходов Avast поступает из Европы, что не является приоритетом для потребительского бизнеса Trend Micro. Меньшее присутствие чешской фирмы на рынке США также будет меньшей угрозой, скрытой внутри Norton. Забегая вперед, пока нет намека на то, что сделка поставит под угрозу модель freemium, на которую приходится так много исторического успеха Avast. Но всегда существует риск того, что объединение поставщиков приведет к повышению цен для клиентов. Если это произойдет, потребители могут быть уверены, что компания Trend Micro всегда будет стремиться предлагать рынку конкурентоспособные, многофункциональные альтернативы». ***(What the Norton-Avast Merger Means for Cybersecurity // CyberSecDN (https://cybersecdn.com/index.php/2021/08/27/what-the-norton-avast-merger-means-for-cybersecurity/). 27.08.2021).***

***

**«Чем больше данных мы храним в сети - от финансовых до медицинских и личных записей - тем больше потребность в кибербезопасности. Поскольку хакеры продолжают взламывать сети, специалисты по кибербезопасности полагаются на помощь в защите данных и компьютерных сетей крупных организаций.**

Мы поговорили с Аланом Ринаржевски, MIS, и Дональдом Маккракеном, доктором философии, которые являются членами глобального факультета Университета Пердью, чтобы узнать больше о кибербезопасности и выявить основные навыки кибербезопасности, необходимые для успеха в этой конкурентной сфере.

*Почему кибербезопасность - это растущая область*

По данным Бюро статистики труда США, сфера кибербезопасности демонстрирует колоссальный рост, и он будет только продолжаться. Ожидается, что занятость аналитиков информационной безопасности, в том числе специалистов по кибербезопасности, вырастет на 31% с 2019 по 2029 год, что намного быстрее, чем в среднем по другим профессиям *.

Рынажевски говорит, что наш ненасытный аппетит к Интернету способствует этому росту.

«Мы размещаем все в сети», - говорит он. «Наши камеры видеонаблюдения доступны по всему миру. Наши смартфоны хранят информацию. Наши машины подключены к Интернету. Общая картина такова, что теперь мы поместили в наши сети все, что имеет ценность, даже наши самые сокровенные секреты. Это означает огромную зарплату для людей, которые могут скомпрометировать эту информацию».

Маккракен соглашается, что эта ситуация создает пробел в навыках кибербезопасности, говоря: «Компании понимают, что они не так безопасны, как они думали».

«Им необходимо нанять людей, которые будут защищать эти сети и устройства и обеспечивать безопасность людей», - говорит Рынаржевски.

>> Узнайте больше об одном дне из жизни профессионала в области кибербезопасности

*Стать профессионалом в области кибербезопасности*

Согласно BLS, специалисты по информационной безопасности обычно должны иметь степень бакалавра в области компьютерных наук, такой как информатика, обеспечение информации, программирование или в смежных областях, таких как кибербезопасность. Работодатели могут предпочесть, чтобы аналитики имели опыт работы в смежной профессии.

Дипломы последипломного образования, такие как степень магистра наук в области управления кибербезопасностью, могут расширить ваши возможности.

*Сертификаты для профессионалов в области кибербезопасности*

Для профессионалов в области кибербезопасности доступно несколько сертификатов. Работодатели могут предпочесть, чтобы кандидаты имели сертификаты для подтверждения своих знаний. Некоторые из наиболее распространенных сертификатов:

Сертифицированный этический хакер: это удостоверяет, что вы знакомы с новейшими инструментами, методиками и приемами взлома коммерческого уровня, используемыми хакерами и специалистами по информационной безопасности для законного взлома организации.

Сертифицированный специалист по безопасности информационных систем: этот сертификат подтверждает, что вы можете эффективно разрабатывать, внедрять и управлять лучшей в своем классе программой кибербезопасности.

Безопасность+: это подтверждает, что у вас есть базовые навыки, необходимые для выполнения основных функций безопасности и продолжения карьеры в области ИТ-безопасности.

«Если ваша компания имеет дело с конкретным поставщиком или есть компания, в которой вы надеетесь работать, получение сертификатов конкретного поставщика также может помочь», - говорит Рынаржевски.

12 навыков, которые вам нужны в кибербезопасности

Чтобы стать экспертом в области кибербезопасности, вам понадобятся определенные навыки. Рынаржевски и Маккрэкен поделились некоторыми ключевыми навыками и социальными навыками, которые, по их мнению, являются наиболее важными.

*6 сложных навыков, которые вам нужны в кибербезопасности*

Жесткие навыки - это усвоенные способности, приобретенные и улучшенные в процессе обучения и практики. Эти навыки больше ориентированы на умение выполнять задачи и их выполнение. К основным навыкам, которые вам понадобятся в кибербезопасности, относятся:

Знание компьютеров и оборудования: это общие навыки любого, кто работает с компьютерами.

Сетевая безопасность: «Вы хотите знать, как все работает, что считается безопасным, а что - небезопасным», - говорит Рынаржевски.

Программирование: Рынажевский говорит, что знание языков программирования может помочь вам автоматизировать работу, которую необходимо выполнить.

Статистический анализ: «На самом деле вы ищете аномалии в своей сети, чтобы выяснить, что не так», - говорит Рынаржевский. «Понимание того, как анализировать сетевую статистику, определенно поможет».

Системная инженерия: это требует понимания того, как системы и устройства работают вместе.

Анализ уязвимости: это возможность посмотреть, насколько ваши сети могут быть небезопасными, и узнать, как их защитить.

6 мягких навыков, которые вам нужны в кибербезопасности

Мягкие навыки более поведенческие и связаны с личностью. Следовательно, по данным Investopedia, их труднее преподавать. Человек, обладающий этими мягкими навыками, может добиться большего успеха:

Адаптивность: сюда относится спокойный темперамент. «Если в технологии есть одна константа, так это то, что она всегда меняется», - говорит Маккракен. «Вы должны быть готовы к переменам».

Быть аналитичным: это означает всегда быть готовым к изучению и пониманию предстоящей задачи.

Надежность: любой работодатель захочет, чтобы вы были надежными, приходя вовремя и уделяя все внимание своей работе, - говорит Рынаржевски.

Дотошность: исключительное внимание к деталям может помочь вам при работе с очень сложными системами.

Решение проблем: Рынажевски говорит, что любопытство помогает находить решения для уязвимостей и других проблем компьютерных сетей.

Быть командным игроком: «Если команда не может сотрудничать, команда никогда не добьется успеха», - говорит Маккракен. «Эффективное общение также является частью этого. Они должны уметь передать то, что они знают и что они нашли».

«Вы должны постоянно учиться, если хотите заниматься кибербезопасностью», - говорит Маккракен...» ***(The 12 Most In-Demand Cybersecurity Skills You Need to Be Successful // Purdue University Global (https://www.purdueglobal.edu/blog/information-technology/top-cybersecurity-skills/). 25.08.2021).***

***

**«В результате пандемии COVID-19 картина угроз во многом изменилась, и организации изо всех сил пытаются защититься от оппортунистических кибератак.**

Это был ключевой вывод из отчета VMware Global Security Insights за 2021 год, составленного на основе опроса 3542 ИТ-директоров, технических директоров и директоров по информационной безопасности со всего мира в декабре 2020 года.

Почти 80% сообщили о росте кибератак из-за сотрудников, работающих на дому. Аналогичный процент заявили, что атаки стали более изощренными, а 4 нарушения из 5 были признаны существенными. Шестьдесят один процент респондентов признал необходимость другого взгляда на безопасность из-за расширенной поверхности угроз.

*Всплеск кибератак*

Во время пандемии количество кибератак увеличилось по ряду причин. Во-первых, поверхность угрозы расширилась, поскольку организации повсюду отправляли сотрудников домой для удаленной работы. Рабочие внезапно стали использовать компьютеры со своими детьми для удаленного обучения, а также домашнюю сеть с любым количеством интеллектуальных устройств.

Вдобавок традиционная преступность переместилась в онлайн. «Картели киберпреступности были усилены пандемией, потому что традиционная организованная преступность не могла работать из-за изоляции», - сказал глава VMware по стратегии кибербезопасности Том Келлерманн во время интервью в прямом эфире Global Security Insights Report. Многие кибер-картели создали сложную структуру квази-стартапов, в которую входят разработчики и группы контроля качества. Некоторые даже пользуются поддержкой международных правительств.

Келлерманн сообщил, что некоторые страны считают киберпреступников национальным достоянием. «Там осуществляется защита, потому что правительства часто рассматривают эти группы как способ нейтрализации экономических санкций и способ создать своих доверенных лиц для создания почти повстанческого движения против своих геополитических врагов», - сказал Келлерманн…

И, наконец, организации не спешили менять свои взгляды на безопасность, одновременно переводя большую часть своей инфраструктуры в облако. «Злоумышленники - оппортунисты, поэтому мы тоже должны быть оппортунистами», - сказал Джеймс Аллибэнд, старший стратег по безопасности VMware. «Мы должны изменить статус-кво [и] убедиться, что существующие у нас традиционные процессы безопасности не обязательно повлияют на нас в будущем».

Итак, как организации могут защитить себя?

*Не все облака созданы равными*

В то время как почти все опрошенные использовали стратегию, ориентированную на облако, похоже, что существует некоторая неуместная вера в безопасность общедоступного облака. Келлерманн посоветовал думать о публичной облачной среде как о «очень хорошем жилом доме в очень тяжелом районе». Безопасность следует строить с точки зрения нулевого доверия, и ее необходимо внедрять с нуля.

Главный стратег VMware по кибербезопасности Рик МакЭлрой сравнил ИТ-команды, создающие инфраструктуру, со строительством многоквартирного дома: «К вам приходят архитекторы, которые планируют такие вещи, как водопровод, электричество, достаточная площадь в квадратных футах. Они не планируют, чтобы кто-то врезался в этот многоквартирный дом и выбил вашу дверь. Это наша работа».

Аллибэнд согласился, сказав: «Вы должны защитить эти среды с самого начала и встроить это в свою стратегию».

*Встроенные системы раннего обнаружения*

Организации должны найти плохих игроков, прежде чем нападать. Вместо того, чтобы полностью полагаться на процессы безопасности, предотвращающие

попадание угроз в вашу среду, важно найти их, если и когда они попадут внутрь. И приступы, как правило, не происходят сразу. Обычно злоумышленники тратят пару недель на изучение вашей инфраструктуры перед атакой, поэтому их можно обнаружить до того, как они начнут действовать.

Келлерманн сказал: «Вы должны предположить, что профилактика в какой-то момент потерпит неудачу. Когда это произойдет, как быстро вы сможете обнаружить и отреагировать?»

Директора по информационной безопасности ищут способ обнаружить эти угрозы. «На самом деле директора по информационным технологиям ищут решения, которые позволят им увидеть эти облачные среды», - сказал МакЭлрой. Они ищут средства управления, которые являются единообразными и поддающимися аудиту, и которые могут отслеживать их данные в различных облачных средах.

*Защитите любое рабочее пространство*

Во время пандемии удаленная работа резко возросла. И похоже, что любое рабочее место здесь, чтобы остаться. Но при таком большом количестве сотрудников, работающих вне офиса, поверхность атаки увеличивается в геометрической прогрессии. Когда в домашней сети работает несколько устройств, существует множество уязвимостей.

«В домах отсутствует цифровое дистанцирование, и нам действительно нужно обращать на это внимание. … Ваше рабочее устройство не должно быть подключено к той же сети, что и ваши интеллектуальные устройства, точка, - сказал Келлерманн. Обеспечение безопасности удаленной среды является обязательным.

*Упростите безопасность*

Безопасность стала сложной, с множеством элементов управления и виджетов, которые могут быть использованы злоумышленниками. «Мы должны начать упрощать безопасность, это номер один. Слишком много инструментов, в которых слишком много пробелов », - сказал МакЭлрой.

Поскольку компании используют ряд инструментов для защиты различных частей своего бизнеса, возрастает риск, если они не общаются друг с другом. Одно приложение безопасности может не знать о взломе другого приложения безопасности. «Вам действительно следует стандартизировать одну платформу. И какая бы платформа ни была, вам следует в ближайшее время стандартизировать ее», - сказал Келлерманн.

*Ударьте злоумышленников там, где это больно*

В конечном итоге киберпреступники попадают в бизнес, потому что это выгодно. Сильным стимулом для их бизнеса является то, что большая часть работы автоматизирована. МакЭлрой предполагает, что компании удорожают ведение бизнеса киберпреступниками, заставляя их замедляться и выполнять больше работы вручную.

«Если бы каждая программа-вымогатель была написана на заказ, теперь мы начинаем разрушать эту экономику. Теперь они фактически не могут получить огромную [рентабельность инвестиций], потому что их временные затраты слишком велики», - сказал МакЭлрой. «Проще говоря, мы должны заставить их

проводить больше времени. … Мы должны развернуть технологию, чтобы усложнить задачу».

*Новая Норма*

В конечном итоге ландшафт угроз сильно изменился, и он уже не вернется в прежнее состояние.

«Мы должны понять, что это норма, и в ближайшее время это не изменится. Если я смогу начать менять свое мышление и пойму, что живу в плохом районе и несу ответственность за свою самооборону, то я собираюсь изменить свое собственное поведение», - сказал МакЭлрой. «Я собираюсь изменить культуру организации, в которой я работаю, и для этого мне нужно что-то вроде наблюдателей за соседями»…

Пандемия поставила безопасность на передний план и в центре внимания руководителей бизнеса. МакЭлрой призвал руководителей службы безопасности воспользоваться этой возможностью: «Мы помогали организациям работать во время глобальной пандемии. Организации довольны многими руководителями службы безопасности и тем, как нам это удалось. Давайте воспользуемся этим так же, как злоумышленники воспользовались этой катастрофой, и давайте поднимем флаг немного дальше, чем мы когда-либо думали, это возможно». ***(Radius Staff. Surge in Cyberattacks Targets the Anywhere Workforce // VMware, Inc. (https://www.vmware.com/radius/surge-in-cyberattacks-targets-anywhere-workforce/). 25.08.2021).***

***

**«Развитие технологий приводит к появлению различных инноваций, таких, например, как дипфейки (англ. deepfake).** Это видео, изображение или аудиозапись, которые были обработаны с помощью технологии искусственного интеллекта. Например, на видео с дипфейком можно сделать так, чтобы человек говорил или делал что-то, чего в реальной жизни не было.

Дипфейки выглядят очень убедительно, и продолжающееся развитие технологий только усложнило различие между реальным и поддельным контентом. Хотя технология deepfake относительно нова, она стремительно становится все более серьезной проблемой, поскольку используются преступниками для проведения мошеннических афер и атак с методами социальной инженерии, а также для распространения дезинформации.

По оценкам экспертов (PDF), ущерб от мошеннических афер с дипфейками в 2020 г. превысил 250 млн. долл. Вне сомнения, по мере развития технологии дипфейков будет совершенствоваться и то, как преступники используют ее для атак на домашних и корпоративных пользователей.

Созданные посредством ИИ «синтетические медиа», дипфейки, имитируют лица, движения и голоса людей с такой точностью, что их часто невозможно отличить от оригинала без специальных инструментов.

Алгоритмы машинного обучения позволяют манипулировать такими биометрическими данными как выражение лица и тон человеческого голоса, чтобы создавать реалистичное изображение событий, которые никогда не происходили. Хотя не все подделки используются со злым умыслом.

Чтобы создать дипфейковое видео с каким-нибудь человеком, автор начинает с загрузки в нейронную сеть сотен часов реальных видеоматериалов, на которых записан этот человек в разных ситуациях, чтобы как можно лучше «обучить» компьютер распознавать подробные закономерности и характеристики данного человека. Это делается для того, чтобы дать алгоритму реалистичное представление о том, как выглядит данный субъект с разных сторон.

Затем возможности обученной нейронной сети объединяются с методами компьютерной графики, для наложения реальных кадров человека на синтезированные ИИ лицевые и речевые паттерны.

Хотя многие считают, что для создания дипфейков требуются сложные инструменты и экспертные навыки, это не так – их можно сделать даже с базовыми навыками компьютерной графики. Главное, что нужно для создания дипфейка, – это доступ к видео или аудиозаписям какого-либо человека. Однако сегодня это не является проблемой, учитывая ошеломляющее количество доступных источников информации.

Быстрое развитие технологии дипфейка создало возможность для технически подкованных преступников наносить серьезный финансовый ущерб. Злоумышленники в своих интересах активно используют дипфейки для кражи персональных данных и онлайн-личности, распространения дезинформации в обществе, финансового шантажа, мошенничества и автоматизированных кибер-атак. Вот лишь некоторые распространенные виды мошенничества с помощью дипфейков.

Афера с «мертвыми душами» состоит в том, что преступник крадет данные умершего человека и пытается использовать его в «живом виде» для получения финансовой выгоды. Украденная личность может быть использована для получения доступа к онлайн-сервисам и учетным записям или для подачи заявок на банковские карты, кредиты и т.д.;

Мошенничество с открытием счетов заключается в том, чтобы использовать украденные или поддельные личности для открытия новых банковских счетов. Как только преступник открыл счет, он может нанести серьезный финансовый ущерб, обналичив кредитные карты или взяв кредиты, которые он не намерен возвращать;

Мошенничество с использованием синтезированных личностей – более сложный вид, который, как правило, труднее обнаружить. Вместо того чтобы использовать украденную личность одного человека, преступники добывают информацию и сведения по нескольким людям, чтобы создать/ синтезировать нового «человека», которого на самом деле не существует. Затем эта синтезированная личность используется для финансовых транзакций или получения новых кредитов.

Последние инновации существенно сократили количество времени и данных, необходимых для создания реалистичных дипфейков. По мере того как они станут более доступными, число подобных атак, вероятно, будет продолжать расти.

Одной из первых известных атак с использованием дипфейка стала афера 2019 г., когда генеральный директор энергетической компании получил телефонный звонок якобы от своего босса. На самом деле, это был поддельный

голос, сгенерированный ИИ, но на слух это было сложно определить, поэтому работник спокойно выполнил поручение о переводе 243 тыс. долл. в течение часа.

Несмотря на все большую реалистичность, дипфейк можно попытаться выявить, если быть внимательным. Любые признаки, вроде неестественной интонации речи, роботизированного тона, неестественного моргания или движений человека, не синхронизированных с речью движений губ, низкое качество звука или видео – являются поводом усомниться и перепроверить поступившую информацию.

Со своей стороны компании могут бороться с угрозой атаки с использованием дипфейков, главным образом, обучая своих сотрудников тому, как распознавать потенциальные подделки. Чаще всего обучение сотрудников мерам информационной безопасности является первой линией защиты компании от кибер-атак. Предоставление четких корпоративных правил реагирования и наличие системы внутренней проверки подозрительных сообщений является важным началом, когда речь заходит о безопасности компании.

О серьезности проблемы свидетельсвтуе хотя бы тот факт, что в 2020 г. в США был принят закон, который криминализировал создание и распространение видео с дипфейками, которые не помечены должным образом, и обозначил направление дальнейших исследований и разработок средств обнаружения дипфейков». ***(Евгений Куликов. Дипфейки как угроза информационной безопасности // Компьютерное Обозрение (https://ko.com.ua/dipfejki_kak_ugroza_informacionnoj_bezopasnosti_138408). 17.08.2021).***

***

**«Специалисты института SANS по поручению компании Nozomi Networks провели опрос организаций и компаний в промышленной сфере. Как показали результаты опроса, организации, использующие автоматизированные системы управления технологическим процессом (АСУ ТП) и другие операционные технологии (OT), все больше обеспокоены киберугрозами.**

Почти 70% респондентов считают, что риск кибератак на их OT-среды является высоким, что является значительным увеличением по сравнению с 51% в 2019 году, когда SANS провел аналогичный опрос.

Хотя многие организации обеспокоены рисками кибератак на свои OT-среды, 48% респондентов не знают, сталкивались ли их компании со взломами в прошлом году. Примечательно, что в 2019 году такой же ответ дало 42% опрошенных. Это указывает на необходимость организациям улучшить свои возможности по обнаружению и реагированию на кибератаки.

Только 12% респондентов были уверены, что их системы не были скомпрометированы, а 15% обнаруживали взломы, вызвавшие нарушения в производственных процессах.

Большинство респондентов обвинили в инцидентах хакеров, за которыми следовали организованная преступность, поставщики услуг и подрядчики, сотрудники, активисты и APT-группировки

В качестве первоначальных векторов атак, связанных со взломами, респонденты указали внешние удаленные службы (36%), за которыми следовала эксплуатация общедоступных приложений (32%), подключенных к Сети устройств (28%), фишинг (26%), съемные носители (24%) и скомпрометированные рабочие станции инженеров (18%).

За последние годы многие компании предприняли шаги по улучшению состояния безопасности ОТ-систем. Почти половина организаций увеличили свой бюджет кибербезопасности АСУ ТП. По словам более половины респондентов, теперь они могут обнаружить факт взлома в течение 24 часов, по сравнению с 34% в 2019 году». ***(70% компаний и организаций опасаются кибератак на АСУ ТП и ОТ-системы // SecurityLab.ru (https://www.securitylab.ru/news/523848.php). 30.08.2021).***

***

## *Сполучені Штати Америки*

**«Группа двухпартийных депутатов Палаты представителей и Сената в четверг представила закон, призванный помочь федеральному правительству лучше отслеживать и анализировать киберпреступность после резкого увеличения кибератак за последний год.**

Закон о лучших показателях киберпреступности положит начало процессу улучшения того, как правительство и правоохранительные органы собирают данные о киберпреступности, при этом многие преступления в настоящее время не регистрируются или не отслеживаются, что затрудняет принятие мер правительством.

В законопроекте будут реализованы шаги по изменению этой тенденции, такие как требование к Министерству юстиции работать с Национальной академией наук над разработкой таксономии киберпреступности.

Это также обеспечит включение отчетов о киберпреступлениях от должностных лиц на всех уровнях в Национальную систему отчетности по инцидентам ФБР и потребует от Государственного управления отчетности сообщать о текущих мерах по киберпреступности и различиях в сообщении о проблемах кибербезопасности по сравнению с другими видами преступной деятельности.

Законодательством руководит респ. Эбигейл Спанбергер в Доме с другими спонсорами, включая представителей Блейка Мура, Эндрю Гарбарино и Шейла Джексон Ли.

Законопроект одновременно вносится в Сенат сенатором. Брайан Шац и Том Тиллис, Джон Корнин и Ричард Блюменталь являются соавторами.

«Киберпреступность все чаще подвергает американские семьи, предприятия и государственные учреждения серьезному риску», - говорится в заявлении Спанбергера в четверг. «Но слишком долго наше правительство было ужасно неподготовленным к кибератакам следующего поколения. Самоуспокоение в отношении нашей системы классификации киберпреступлений может поставить

под угрозу общественную безопасность, нашу способность конкурировать в мировой экономике и даже нашу национальную безопасность».

«Наша национальная система классификации преступлений устарела, и Закон о лучших показателях киберпреступности предусматривает разумные меры для улучшения показателей киберпреступности, прогнозирования будущих тенденций и обеспечения наличия у правоохранительных органов необходимых инструментов и ресурсов», - добавила она.

Законопроект был внесен после нескольких крупных инцидентов в области кибербезопасности в последние месяцы, включая обнаружение в декабре взлома SolarWinds, в котором хакеры, связанные с правительством России, получили доступ к системам девяти федеральных агентств и 100 групп частного сектора.

Совсем недавно атаки программ-вымогателей на Colonial Pipeline и производителя мяса JBS USA выявили уязвимости в важнейших цепочках поставок, особенно после года, когда киберпреступники воспользовались уязвимыми организациями во время пандемии COVID-19.

Гарбарино, высокопоставленный член подкомитета по кибербезопасности Комитета внутренней безопасности Палаты представителей, заявил в своем заявлении: «Киберпреступность процветает, но, несмотря на рост числа атак, затрагивающих американцев, у нас нет четкого представления о полном масштабе проблемы» и что «мы должны использовать все имеющиеся в нашем распоряжении инструменты» для отражения атак.

Джексон Ли, председатель подкомитета Судебного комитета Палаты представителей по преступности, терроризму и внутренней безопасности, заявил в четверг, что «для того, чтобы делать больше для противодействия киберугрозам, нам нужны более точные данные о частоте подобных преступлений».

«На кону стоит общественная безопасность и киберпревосходство Америки, и сейчас самое время действовать», - сказал Мур в отдельном заявлении.

Кибербезопасность была проблемой, которую администрация Байдена была вынуждена уделять приоритетное внимание с первого дня. Президент Байденвступил в должность из-за обострения инцидентов. Администрация предприняла ряд шагов для противодействия киберугрозам, в том числе Байден подписал в мае распоряжение об усилении кибербезопасности федерального правительства и наложил санкции на Россию за ее участие во взломе SolarWinds.

Ранее на этой неделе Национальный кибер-директор Крис Инглис поддержал идею создания Бюро кибер-статистики при Министерстве внутренней безопасности для сбора, анализа и публикации информации о киберинцидентах, предоставленной группами, занимающимися кибербезопасностью.

Новый закон не имеет отношения к этим усилиям, но в четверг Спанбергер подчеркнул необходимость принятия мер в этой сфере.

«Я горжусь тем, что возглавляю введение этого двухпартийного, двухпалатного законодательства - потому что этот закон поможет предотвратить превращение большего числа американцев в жертвы и цели в Интернете», - сказал Спанбергер». ***(MAGGIE MILLER. Lawmakers roll out bipartisan bill to help track cyber crimes // THE HILL (https://thehill.com/policy/cybersecurity/566553-lawmakers-roll-out-bipartisan-bill-to-help-track-cybercrimes). 05.08.2021).***

***

**«После встречи по вопросам кибербезопасности в Белом доме в среду президент Байден получил обещания от крупных технологических компаний потратить значительные суммы на повышение киберустойчивости страны.** Microsoft и Google, например, вложили миллиарды в конкретные инвестиции в кибербезопасность.

Встреча последовала за серией драматических инцидентов в области кибербезопасности, включая атаку вымогателя Colonial Pipeline, которая остановила поставки газа и нефти на юго-востоке, атаку на цепочку поставок программного обеспечения SolarWinds и обширный взлом серверов Microsoft Exchange.

В заявлении Белого дома говорится, что для устранения угроз кибербезопасности необходимы «общенациональные усилия». С этой целью:

Microsoft объявила, что инвестирует 20 миллиардов долларов в течение следующих пяти лет в развитие «кибербезопасности по замыслу» и предоставление передовых решений безопасности. Компания также объявила, что немедленно выделит 150 миллионов долларов на технические услуги, чтобы помочь федеральным, государственным и местным органам власти повысить свою безопасность.

Google выделила 10 миллиардов долларов в течение следующих пяти лет на расширение программ нулевого доверия, помощь в обеспечении безопасности цепочки поставок программного обеспечения и повышение безопасности открытого исходного кода. Компания также заявила, что поможет 100000 американцев получить признанные в отрасли сертификаты цифровых навыков.

Apple создаст новую программу, чтобы сделать цепочку поставок технологий более безопасной. В рамках этих усилий компания планирует работать со своими поставщиками для массового внедрения многофакторной аутентификации, обучения безопасности, устранения уязвимостей, регистрации событий и реагирования на инциденты.

IBM заявила, что обучит 150 000 человек навыкам кибербезопасности в течение следующих трех лет и будет сотрудничать с более чем 20 колледжами и университетами, которые исторически были черными, для создания центров лидерства в кибербезопасности.

Amazon объявила, что предложит владельцам учетных записей Amazon Web Services бесплатное устройство многофакторной аутентификации. Он также планирует сделать свой тренинг по вопросам безопасности, который он в настоящее время предлагает для сотрудников, бесплатным для общественности.

Белый дом также получил обязательства от поставщиков киберстрахования и образовательных организаций улучшить положение в области безопасности страны.

Президент Байден издал кибербезопасность распоряжение в начале мая, требуя от федеральных агентств модернизировать свой кибер - защиту.

Ранее в этом году администрация Байдена также запустила 100-дневную инициативу по повышению кибербезопасности в электроэнергетическом секторе. В

среду администрация объявила, что эта инициатива улучшила состояние кибербезопасности более чем 150 электроэнергетических компаний и теперь будет распространяться на трубопроводы природного газа.

Кроме того, в среду Белый дом заявил, что Национальный институт стандартов и технологий (NIST) разработает новую структуру для повышения безопасности и целостности цепочки поставок технологий. Для этого он будет работать с партнерами, включая Microsoft, Google и IBM». ***(Stephanie Condon. Biden gets Google, Apple, others to join "whole-of-nation" cybersecurity effort // ZDNet (https://www.zdnet.com/article/tech-giants-make-cybersecurity-commitments-after-white-house-meeting/). 25.08.2021).***

***

**«После еще одного года атак программ-вымогателей и цепочек поставок Microsoft заявляет о своей роли в реализации майского указа президента США Джо Байдена о кибербезопасности на практике.**

Microsoft - одна из 18 компаний, занимающихся кибербезопасностью, которые были выбраны для сотрудничества с Национальным институтом стандартов и технологий (NIST) в разработке проектов Zero Trust, которые федеральные агентства могут реализовать в соответствии с Указом 14028.

Вместо того, чтобы сосредоточиться на укреплении периметра сети, Zero Trust предполагает, что организация уже была взломана, и включает дизайн, который признает необходимость защиты данных как внутри, так и за пределами сети, на управляемых и неуправляемых устройствах.

Среди других поставщиков консорциума Zero Trust - Amazon Web Services, Appgate, Cisco, F5, FireEye, IBM, McAfee, MobileIron, Okta, Palo Alto Networks, PC Matic, Radiant Logic, SailPoint Technologies, Symantec, Tenable и Zscaler. Примечательно, что Google и его инициатива нулевого доверия BeyondCorp отсутствует.

Распоряжение Байдена требовало от CISA и NIST создания эталонов для организаций, управляющих критически важной инфраструктурой. Он последовал за взломом SolarWinds, нацеленным в первую очередь на федеральные агентства и технологические компании США, атаками на почтовый сервер Exchange и атакой программы-вымогателя Colonial Pipeline. Атака SolarWinds, в частности, подчеркнула необходимость нулевого доверия, поскольку атаки происходят на фоне массового перехода к удаленной работе во время пандемии.

Поставщики, участвующие в проекте, будут работать с Национальным центром передового опыта в области кибербезопасности (NCCoE) NIST для «разработки практических, совместимых подходов к проектированию и созданию архитектур Zero Trust», которые коммерчески доступны в американских компаниях, занимающихся кибербезопасностью.

Microsoft ранее определила пять сценариев, в которых нулевое доверие может помочь агентствам выполнить заказ Байдена, включая обнаружение конечных точек и реагирование на них, многофакторную аутентификацию и непрерывный мониторинг.

Azure Active Directory занимает центральное место в планах Microsoft по большинству из пяти сценариев, которые включают приложения SaaS, унаследованные приложения, средства защиты удаленного администрирования и сегментацию облака. Azure также играет ключевую роль в «микросегментации» сети.

Хотя приказ Байдена распространяется только на федеральные агентства, Белый дом действительно побудил частный сектор принять «амбициозные меры» в том же направлении.

Microsoft отмечает, что предлагаемые ею примеры решений будут включать коммерческие продукты и продукты с открытым исходным кодом.

Отдельно Linux Foundation поддержал приказ Байдена разработать спецификацию программного обеспечения (SBOM) или «официальную запись, содержащую детали и взаимосвязи цепочки поставок различных компонентов, используемых при создании программного обеспечения».

Предложения Zero Trust от поставщиков предназначены для согласования с NIST SP 800-207, Zero Trust Architecture, которая была разработана в результате встреч с Советом Федерального директора по информационным технологиям (CIO), федеральными агентствами и представителями отрасли». ***(Liam Tung. Microsoft touts role in meeting Biden's order to fend off major hacks on the US // ZDNet (https://www.zdnet.com/article/microsoft-touts-role-in-meeting-bidens-cybersecurity-order/). 18.08.2021).***

***

**«3 августа 2021 года Сенат по национальной безопасности и правительственным делам (HSGAC) выпустил отчет под названием «Федеральная кибербезопасность: данные Америки все еще находятся под угрозой».**

47-страничный отчет содержал важные детали, подтверждающие вывод о том, что «согласно генеральным инспекторам агентства, средняя оценка общей зрелости информационной безопасности агентства - C-».

После почти двух десятилетий федеральной кибербезопасности и управления рисками в соответствии с Федеральным законом об управлении информационной безопасностью (FISMA) 2002 г. и Федеральным законом о модернизации информационной безопасности (также FISMA) 2014 г. выделенное федеральное финансирование кибербезопасности составило миллиарды долларов. существенно не улучшила общую ситуацию. Распространяются сообщения о том, что HSGAC в настоящее время рассматривает реформу законодательства FISMA, и это одновременно является положительным моментом и поводом для беспокойства. Если в новом законодательстве будут повторяться недостатки предыдущих версий, это может стать поводом для беспокойства. Однако, если новое законодательство, наконец, исправит это с третьей попытки, то «Внук FISMA» станет желанным вкладом в политику кибербезопасности и управления рисками на федеральном предприятии.

Две предыдущие версии FISMA неадекватно отражали сложную и чрезвычайно важную концепцию управления кибербезопасностью, и если текущие

обсуждения являются хоть одним признаком будущего этой концепции в законодательстве о реформе, управление кибербезопасностью, вероятно, снова будет неоднозначным. Большая часть проблемы заключалась в использовании слова «гарантировать». FISMA использовало слово «гарантировать» вместо слова «принуждение» в контексте того, что директор по информационным технологиям (CIO) должен «обеспечивать соблюдение закона». Этот простой выбор слов гарантировал, что ИТ-директор и подчиненный ему «старший офицер по информационной безопасности» не обладают значительными полномочиями. Например, меморандум от 7 апреля 2004 г. от главного юрисконсульта Департамента по делам ветеранов обнаружил, что сознательное использование слова «гарантировать» вместо слова «принуждение» гарантирует, что ИТ-директор и главный директор по информационной безопасности (CISO) не имеют полномочий применять политику кибербезопасности или удерживать людей несут ответственность за нарушение своих обязательств по кибербезопасности и управлению рисками. Одно, казалось бы, невинное слово может оказать невероятно важное влияние на эффективность законодательства.

В дополнение к теме управления FISMA решила подчинить директора по информационным технологиям директора по информационным технологиям, что является организационной схемой, которая больше не пользуется популярностью среди предприятий во всем Fortune 500 и Global 2000. Фактически, в законодательстве FISMA даже не используется название « Директор по информационной безопасности », чтобы указать роль; вместо этого он использует менее определенное и двусмысленное выражение «старший сотрудник по информационной безопасности агентства» и далее описывает роль как просто ответственность за выполнение обязанностей ИТ-директора в соответствии с законом. Поступая таким образом, FISMA не понимает, что роль ИТ-директора заключается в предоставлении предприятию «мощности, пинга и трубопровода», в то время как роль директора по информационной безопасности представляет собой принципиально иной континуум «идентифицировать, защищать, защищать, реагировать, и выздоравливай.

Неформальные беседы с сотрудниками на Капитолийском холме подтверждают, что их концепция CISO - это просто концепция безопасности информационных технологий, что не соответствует преобладающей в коммерческой отрасли тенденции отделять CISO от CIO и возлагать на CISO роль безопасности и рисков. управление бизнес-процессами, миссией и культурой организации. Современный CISO - это больше, чем «ИТ-безопасность». Проект нового закона о кибербезопасности, по всей видимости, циркулирует в Сенате, и это означает, что он возможно может быть принят на 117-м заседании Конгресса. Вопрос в том, будет ли это улучшением по сравнению с предыдущими версиями FISMA. Если этого не произойдет, то будет упущена возможность провести реальную реформу кибербезопасности, и впереди нас ждут те же два десятилетия неадекватного прогресса, как указано в недавней табеле успеваемости HSGAC.

Что новое законодательство должно содержать без двусмысленности, как минимум следующее:

Признание того, что предыдущая основа FISMA как системного, поэтапного подхода к информационной безопасности устарела и должна быть заменена подходом, ориентированным на укрепление персонала и управление поверхностью атаки. Система управления рисками не учитывает, что человек - это новый периметр предприятия.

Понимание того, что миграция в облако, безопасность в облако и цифровая трансформация являются преобладающими тенденциями кибербезопасности и управления рисками в федеральной (и коммерческой) кибербезопасности и управлении рисками.

Повышение уровня управления рисками до уровня руководства агентства. NIST SP 800-39 «Управление рисками информационной безопасности» требует, чтобы руководство агентства определило толерантность к риску и принятие риска, после чего ожидается, что ИТ-директор и директор по информационной безопасности будут реализовывать свои программы в соответствии с указаниями руководства. Формулировки FISMA по этому поводу в лучшем случае неоднозначны.

Четкий набор полномочий и управления для CISO, включая полномочия, соизмеримые с подотчетностью, и возможность для любого агентства создать другую цепочку подчинения для CISO, помимо CIO. Вместе с этим необходимо заменить слово «гарантировать» словом «обеспечить соблюдение», как в формулировке «Главный сотрудник по информационной безопасности должен обеспечить соблюдение закона».

Требование о том, чтобы Управление по управлению персоналом (OPM) признало, что область карьеры в области кибербезопасности требует специальных знаний, навыков и способностей, и поэтому создает новую серию вакансий по кибербезопасности, а не размещает специалистов по кибербезопасности в рамках существующей серии вакансий GS-2210 (Информация Серия управления технологиями).

Такие компании, как Cisco, сотрудничают с федеральными департаментами и агентствами на пути к повышению общей кибербезопасности и управлению рисками, и улучшенная законодательная среда в значительной степени поможет на этом пути. В конце концов, федеральная информационная безопасность - это защита национальных систем и сетей от тех, кто хочет причинить им вред. Новое и улучшенное законодательство пойдет намного дальше, чем предыдущие версии FISMA, в достижении этой благородной цели. К счастью, 117- й Конгресс имеет возможность принять его. На этот раз давайте разберемся». ***(Bruce Brody. Grandson of FISMA: Why We Desperately Need New Cybsersecurity Legislation from the 117th Congress // Cisco (https://blogs.cisco.com/security/grandson-of-fisma-why-we-desperately-need-new-cybsersecurity-legislation-from-the-117th-congress). 12.09.2021).***

***

**«Национальные центры академического мастерства в области кибербезопасности в составе Агентства национальной безопасности (NSA) предоставили грант в размере 1,67 миллиона долларов Центру обеспечения и**

**безопасности инфраструктуры (CIAS) Техасского университета в Сан-Антонио (UTSA), чтобы помочь сообществам стать более кибербезопасными по всей стране.**

CIAS будет работать с несколькими сообществами в течение двухлетнего гранта, начиная с Государственного университета Анджело (ASU) и города Сан-Анджело, чтобы помочь разработать общесистемную программу кибербезопасности K-12, поддержать местную промышленность и правительство, чтобы они были более эффективными. кибер-устойчивостью и помогать местным академическим учреждениям разрабатывать программы кибербезопасности для студентов, помогая создавать Центры академического мастерства.

Команда UTSA получила грант в результате конкурсного отбора, доступного только для университетов, определенных как Центры академического мастерства. UTSA - единственное латиноамериканское обслуживающее учреждение, имеющее три сертификата Национального центра передового опыта от АНБ и Министерства внутренней безопасности.

CIAS сотрудничает с ASU для разработки программы, которую можно будет передать и применить к сообществам любого размера.

«Сообщества по всей стране становятся все более мишенями для киберугроз - как внутренних, так и внешних, - вот почему сообщества должны применять общесоциальный подход для защиты своих граждан, организаций и инфраструктуры от кибератак», - сказал д-р Грег Уайт, директор CIAS. «Этот грант АНБ позволит CIAS работать с Государственным университетом Анджело над реализацией программы кибербезопасности, которая начинается с образования K-12 и продолжается до местных предприятий, правительства и широкой общественности».

CIAS в UTSA помогал государственным, местным, племенным и территориальным организациям (SLTT) создавать программы кибербезопасности с 2002 года. Учения по кибербезопасности, тренинги и оценки для штатов и сообществ также проводились в течение почти 20 лет, но это будет первая попытка интегрировать всю программу кибербезопасности в рамках всего сообщества.

«Мы рады возможности привнести наш опыт и ресурсы в город Сан-Анджело», - сказал д-р Уайт. «Эта программа будет способствовать развитию устойчивых инициатив, которые помогут всему сообществу стать опытным в вопросах кибербезопасности».

«Я служил с доктором Уайтом, когда мы оба были лейтенантами, дислоцированными на авиабазе Оффутт, штат Небраска, и майорами в Академии ВВС США в Колорадо-Спрингс, штат Колорадо, - сказал президент ASU Ронни Хокинс-младший. крайняя уверенность и уважение к его видению и мудрости, когда дело доходит до кибербезопасности. Для меня большая честь снова служить с ним; особенно в этом качестве за счет того, что ASU вносит свой вклад и поддерживает студентов по всему Сан-Анджело, пилотируя эту уникальную программу».

Двухлетняя пилотная программа, в частности, установит инициативу по кибербезопасности K-12 для начальных, средних и старших школ, которая предоставит планы уроков, инструменты и ресурсы по кибербезопасности для

учащихся, учителей и консультантов в течение учебного года. Он также расширит летние лагеря по кибербезопасности и будет способствовать созданию команд CyberPatriot и турниров Cyber Threat Defender.

Кроме того, этот грант поможет создать программу Культуры кибербезопасности, нацеленную на учащихся K-5, и коллегиальную инициативу, которая обеспечит информационную программу в местных средних школах, создаст команды национальных университетских соревнований по киберзащите, разработает сертификационный тренинг и окажет помощь 2-м и 4-м ученикам. - летние учебные заведения для соответствия требованиям для присвоения статуса Академического центра NSA / DHS.

Другие основные направления будут нацелены на создание местных ассоциаций кибербезопасности, создание инициативы непрерывного образования для оказания помощи людям в получении сертификатов, инициативу обучения для некоммерческих организаций, анализ текущих потребностей в специалистах по кибербезопасности в рамках сообщества, День кибербезопасности сообщества и программа кибербезопасности всего сообщества с использованием модели зрелости кибербезопасности сообщества, включающая создание организации по обмену информацией и анализу сообщества.

«Когда этот грант закончится, город Сан-Анджело станет образцом для других сообществ штата и страны», - сказал д-р Уайт. «Мы надеемся расширить эту программу на другие штаты в течение второго года пилотного проекта».

«Это первый в своем роде пилотный проект, который изменит правила игры для студентов и жителей Сан-Анджело», - сказал президент Хокинс. "Мы уже поговорили с мэром Брендой Гюнтер, доктором Карлом Детлоффом, суперинтендантом независимого школьного округа Сан-Анджело, и полковником Андресом Назарио, командиром базы ВВС Гудфеллоу, о продвижении этого пилота по всему городу, а также Тома Грина Графство. Этот пилотный проект также помогает нам в наших усилиях по признанию АНБ статуса Центра академического мастерства».

«Этот пилотный проект будет полезен для студентов и жителей Сан-Анджело. Город Сан-Анджело, ISD Сан-Анджело, округ Том Грин, база ВВС Гудфеллоу, и местные предприятия во всем нашем сообществе получат огромную выгоду от этого проекта», - сказал представитель Дрю Дарби. «Кибербезопасность была определена как одна из самых серьезных проблем экономической и национальной безопасности, с которыми сталкивается наша страна, и я благодарю президента Хокинса за его руководство и работу по обеспечению того, чтобы ASU оставался в авангарде программ и инициатив в области кибербезопасности», - заявил государственный представитель Дрю Дарби». ***(JOE HYDE. Angelo State Inks Deal with UTSA for Cybersecurity Program // West Texas from San Angelo, TX (https://sanangelolive.com/news/education/2021-08-26/angelo-state-inks-deal-utsa-cybersecurity-program). 26.08.2021).***

***

**«Сбой в программном обеспечении производства компании Palantir, которым пользуется ФБР США, больше года позволял неавторизованному**

**персоналу получать доступ к конфиденциальным материалам расследований. Как сообщает The New York Post, о проблеме говорится в адресованном федеральному суду письме прокуратуры Манхэттена по делу хакера Вирджила Гриффита (Virgil Griffith). Palantir отрицает свою вину и заявляет, что сбой произошел из-за неправильного использования программы экспертами ФБР.**

Гриффит был арестован в 2019 году по обвинению в предоставлении КНДР информации о том, как криптовалюта и блокчейн могут помочь стране обходить санкции США. Обвинение было построено на данных, полученных из профилей хакера в соцсетях с помощью судебного ордера в марте 2020 года. Как сообщается в письме прокуратуры, информация из Twitter и Facebook была загружена в ПО Palantir с настройками по умолчанию, поэтому доступ к ней был у неавторизованных служащих ФБР.

В период с мая 2020 года по август 2021 года доступ к материалам был получен четыре раза тремя аналитиками и одним агентом. Как сообщается в письме, прикрепленный к делу Гриффита агент ФБР узнал о проблеме от своего коллеги в начале текущего месяца. Получившие доступ к информации сотрудники ФБР сообщили прокуратуре, что не помнят, чтобы использовали ее в своих расследованиях.

«В ходе проведения отдельного расследования аналитик ФБР выявил связи между обвиняемым и субъектом этого другого расследования посредством поисков на Платформе, которая использовала возврат ордеров на обыск», - сообщается в письме.

Как заявляют в Palantir, никакого сбоя в ПО не было, а «клиент» просто не следовал «строгим протоколам, установленным для защиты возвращаемых ордеров». ***(Сбой в использующемся ФБР ПО позволял посторонним получать доступ к материалам расследований // SecurityLab.ru (https://www.securitylab.ru/news/523827.php). 27.08.2021).***

***

## *Китай*

**«17 августа 2021 года Государственный совет Китая опубликовал меры безопасности для критически важной информационной инфраструктуры (CII), которые вступят в силу 1 сентября 2021 года.**

CII относится к важной сетевой инфраструктуре и информационным системам, которые используются в общественных коммуникациях и информационных услугах, энергетике, транспорте, водном хозяйстве, финансах, общественных услугах, делах электронного правительства, технологиях национальной обороны и других важных отраслях и секторах, а также в сетях. инфраструктура и информационные системы, которые могут серьезно повлиять на национальную безопасность, национальную экономику, средства к существованию людей или общественные интересы в случае повреждения, нарушения или взлома.

Отраслевые регулирующие органы должны сформулировать правила для идентификации CII в пределах своей соответствующей юрисдикции, уведомить операторов об идентифицированной CII и хранить записи в Министерстве общественной безопасности. Факторы, которые отраслевые регулирующие органы могут учитывать при идентификации, включают сетевую инфраструктуру и информационные системы, которые важны для сектора и основных предприятий сектора; степень ущерба, который может быть причинен, если сетевая инфраструктура и информационные системы повреждены, нарушены или взломаны; и любое связанное с этим влияние, которое эти нарушения могут иметь на другие сектора.

Эти меры устанавливают высокие требования к безопасности для операторов CII, которые основаны на Законе КНР о кибербезопасности. Операторы CII должны синхронизировать планирование, формулирование и реализацию CII и мер защиты, охватывающих весь жизненный цикл CII. Оператор CII должен создать специальный отдел защиты безопасности и провести проверку биографических данных ключевого персонала, ответственного за вопросы защиты. Не реже одного раза в год он должен проводить регулярные проверки безопасности и оценки рисков. Если обнаружена какая-либо серьезная угроза или инцидент кибербезопасности, оператор должен принять корректирующие меры в соответствии с планами реагирования и сообщить об этом компетентному отраслевому регулирующему органу. Если оператор покупает какие-либо сетевые продукты или услуги, которые могут повлиять на национальную безопасность, он должен провести проверки безопасности.

Эти меры подчеркивают сотрудничество между государственными органами. Администрация киберпространства Китая, Министерство общественной безопасности и Министерство промышленности и информационных технологий создадут механизмы обмена информацией, предотвратят дублирование или дублирование проверок и обеспечат конфиденциальность любой информации, полученной в ходе принудительных действий». ***(China publishes protection measures for critical information infrastructure // CMS Legal (https://www.cms-lawnow.com/ealerts/2021/08/china-publishes-protection-measures-for-critical-information-infrastructure?cc_lang=en). 18.08.2021).***

***

## *Російська Федерація та країни ЄАЕС*

**«Власти Беларуси продолжают преследовать активистов и СМИ, критикующих правительство.** В среду суд Беларуси классифицировал группу хакеров, которая, по их утверждениям, атаковала белорусское правительство, как «экстремистскую». Информационное агентство БелаПан и несколько его сотрудников подверглись обыску и аресту.

По данным МВД в Минске, два канала группы Кибер Партизаны в онлайн-сервисе Telegram были классифицированы как «экстремистские», поскольку они «дискредитируют правоохранительные органы и представителей органов власти» и

«разжигают социальную вражду». Это означает, что распространение их контента становится наказуемым преступлением. По данным министерства, нарушителям грозит штраф или задержание полицией.

Затем группа заявила в Telegram, что этот шаг «несомненно, свидетельствует о качестве нашей работы». В июле Кибер Партизаны объявили, что провели «крупнейшую кибератаку в истории Республики Беларусь» на правительство авторитарного президента Александра Лукашенко.

Несмотря на массовые обвинения в мошенничестве, Лукашенко был официально объявлен победителем после президентских выборов в Беларуси в августе прошлого года, что вызвало массовые протесты исторического масштаба в восточноевропейской стране. Органы безопасности подавили протесты с помощью насилия.

*«Мы продолжим нашу работу»*

С момента предполагаемой хакерской атаки в июле Кибер Партизаны почти ежедневно публикуют в Telegram предполагаемые аудиозаписи, на которых сотрудники МВД отдают приказы о применении насилия против протестующих против Лукашенко. Группа также опубликовала личные данные сотрудников правоохранительных органов.

На прошлой неделе хакеры из Кибер Партизан, сообщили в электронном письме информационному агентству AFP, что они уже похитили более пяти терабайт данных — в основном из Министерства внутренних дел, "и не только". Они также утверждали, что отключили камеры МВД и спецслужб КГБ. Согласно их собственным заявлениям, они намерены продолжать кибератаки.

После спорных президентских выборов белорусские судебные органы также классифицировали большинство независимых СМИ в стране как "экстремистские". В среду следственные органы обвинили информационное агентство БелаПан в "организации действий, противоречащих общественному порядку". Агентство также подверглось налоговой проверке. В результате были выявлены "нарушения", которые могут привести к обвинению в уклонении от уплаты налогов.

Журналисты из СМИ сообщили, что полиция конфисковала оборудование, такое как мобильные телефоны и жесткие диски. Два репортера были временно арестованы. Бухгалтер компании и бывший начальник остались под стражей.

«Мы продолжим нашу работу», — заявил БелаПан. Некоторые сотрудники продолжат работу из-за рубежа. Сайты агентства belapan.by и belapan.com по состоянию на полдень были недоступны». ***(Хакеры Беларуси похитили терабайты данных МВД. Лукашенко преследует хакеров и журналистов // Epoch Times (https://www.epochtimes.com.ua/ru/novosti-obshchestva/hakery-belarusi-pohitili-terabayty-dannyh-mvd-lukashenko-presleduet-hakerov-i-zhurnalistov-138181). 20.08.2021).***

***

**«Президент Беларуси Александр Лукашенко провел совещание с Советом Министров республики.** На нём он уделил внимание информационной безопасности и заявил о том, что чиновникам нужно переходить на бумажные носители, если они не могут защитить цифровые данные.

В ходе своего выступления Лукашенко отметил, что нужно проработать вопросы защиты информации и не допустить уязвимости системы мониторинга общественной безопасности.

«Если не можете защитить в своих компьютерах информацию, тогда возвращайтесь к бумажным носителям. Пишите от руки и складывайте у себя в ящик», - резюмировал глава государства.

Он также поручил правоохранительным органам активизировать деятельность по борьбе с преступлениями в сфере высоких технологий». ***(Лукашенко предложил чиновникам радикальный способ защиты информации // SecurityLab.ru (https://www.securitylab.ru/news/523442.php). 17.08.2021).***

***

## *Австралія*

**«Два австралийских правоохранительных органа вскоре получат право изменять, добавлять, копировать или удалять данные после того, как в среду утром Сенат одобрил законопроект, разрешающий такую деятельность.**

Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 («Поправка в закон о надзоре (Идентифицировать и нарушить)»), в настоящее время ожидает королевскую санкцию, руки австралийской федеральной полиции (AFP) и разведка Австралийская комиссия по уголовному (ACIC) три новые силы для борьбы с интернет - преступностью.

Первый из ордеров - это ордер на нарушение данных, рекламируемый как способ предотвратить «продолжение преступной деятельности участниками и являющийся самым безопасным и наиболее целесообразным вариантом, когда эти участники находятся в неизвестных местах или действуют под анонимными или ложными именами». Этот ордер дает полицейским возможность «разрушать данные» путем их изменения, копирования, добавления или удаления.

Несоблюдение этого требования может привести к 10 годам тюремного заключения.

Второй - это ордер на сетевую активность, который позволит AFP и ACIC собирать информацию об устройствах или сетях, которые используются или могут быть использованы теми, на кого распространяется ордер.

Последний ордер - это ордер на захват аккаунта, который позволит агентствам взять под контроль онлайн-аккаунт в целях сбора информации для расследования.

Объединенный парламентский комитет по разведке и безопасности (PJCIS) рекомендовал принять в начале этого месяца закон о так называемом «взломе» при условии выполнения его 33 других рекомендаций. Теневой министр внутренних дел Кристина Кенелли подтвердила в Сенате в среду, что правительство выполнило «полностью или в значительной степени» 23 из 33 рекомендаций путем внесения поправок в законодательство или изменений в пояснительной записке к законопроекту.

К ним относятся усиление критериев выдачи ордеров, включая соображения конфиденциальности, общественных интересов, конфиденциальной и журналистской информации и финансовых последствий; обзоры ISLM и PJCIS; закат силы через пять лет; и положения о добросовестном иммунитете для приказов о помощи.

Из других 10 рекомендаций PJCIS четыре были приняты правительством и будут включены в его ответ на обзор законодательства о национальной безопасности.

Палата представителей во вторник приняла законопроект, в который было внесено в общей сложности 60 поправок, и, хотя лейбористы выразили свою поддержку законопроекту в результате того, что измененный документ является «лучшим законопроектом», зеленые австралийцы этого не сделали.

«Неудивительно, что две основные партии полностью согласованы друг с другом и ведут нас по дороге к состоянию наблюдения», - сказала сенатор от зеленых Лидия Торп.

«Фактически, этот законопроект позволит шпионским агентствам изменять, копировать или удалять ваши данные с помощью ордера на нарушение данных; собирать информацию о ваших действиях в Интернете с помощью ордера на сетевую активность; также они могут захватить ваши социальные сети и другие онлайн-аккаунты и профили с ордером на захват аккаунта.

«Что еще хуже, ордер на нарушение данных и сетевую активность может быть выдан членом Апелляционного административного трибунала - правда? Это возмутительно, что эти ордера не исходят от судьи вышестоящего суда».

Она сказала, что не совсем ясно, нужны ли вообще эти ордера, отметив, что в законопроекте «четко не указывается пробел в существующих полномочиях».

«Масштабы новых полномочий непропорциональны по сравнению с угрозами серьезных и организованных киберпреступлений, на которые они направлены», - сказала она.

«Отсутствуют доказательства, оправдывающие необходимость в ордерах такого рода, помимо уже имеющихся… ни одна другая страна в альянсе Five Eyes не наделила свои правоохранительные органы такими полномочиями, как этот законопроект».

Законопроект в настоящее время ожидает королевского одобрения». ***(Asha Barbaschow. Australia's 'hacking' Bill passes the Senate after House made 60 amendments // ZDNet (https://www.zdnet.com/article/australias-hacking-bill-passes-the-senate-after-house-made-60-amendments/). 25.08.2021).***

***

## *Інші країни*

**«Приблизно через місяць після протестів на комуністичній Кубі уряд прийняв неоднозначний закон про кібербезпеку.** Закон, опублікований у вівторок в Офіційному віснику, розглядається критиками як інструмент обмеження політичних і цивільних свобод на Карибському острові.

Новий закон визначає, наприклад, які дії в Інтернеті є кримінальним злочином, включаючи кібертероризм, підбурювання до суспільних безладів і поширення інформації, яка вважається помилковою або завдає шкоди репутації держави.

Заступник міністра зв'язку Вільфредо Гонсалес заявив інформаційному агентству AFP, що закон дозволить кубинцям захистити «свої особисті дані» і «своє приватне життя». Це також гарантує, що «ніхто не зможе спотворити правду».

*«Куба посилює контроль над інтернетом»*

За словами Хосе Мігеля Віванкі, директора американського підрозділу правозахисної організації Human Rights Watch, закон дозволяє інтернет-провайдерам блокувати доступ, якщо уряд вважає, що користувач поширює неправдиві новини. «Куба посилює контроль над Інтернетом», — сказав він.

Новий закон викликав обурення у багатьох кубинців, які виклали його в інтернет-мережі. «Ми маємо право мати іншу думку і висловлювати її», — написав один з користувачів. «Куба — це диктатура, яка криміналізує право на свободу слова», — написав інший користувач у Twitter.

Мобільний інтернет, який був введений на Кубі тільки у 2018 році, з того часу став для цивільних груп і активістів важливим інструментом поширення інформації.

Протести 11 і 12 липня приблизно у 40 кубинських містах стали найбільшими антиурядовими демонстраціями з часів революції 1959 року під керівництвом Фіделя Кастро. Люди висловлювали своє невдоволення найгіршій за останні 30 років економічній кризі й супутнім їй дефіцитом електроенергії та продовольства». ***(Куба — це диктатура, яка криміналізує право на свободу слова. Прийнято новий закон про кібербезпеку // Epoch Times (https://www.epochtimes.com.ua/novyny-suspilstva/kuba-ce-dyktatura-yaka-kryminalizuye-pravo-na-svobodu-slova-pryynyato-novyy-zakon-pro-kiberbezpeku-138162). 19.08.2021).***

***

**«Часто испытывающие нехватку ресурсов малые и средние предприятия в Сингапуре рассматривают киберстрахование как жизнеспособный вариант. Они рассматривают эти предложения как способ сбалансировать стоимость и необходимость защиты своих активов, особенно потому, что утечки данных остаются их самой большой проблемой.**

Небольшим организациям часто приходилось сталкиваться с ограниченными бюджетами и персоналом, и им хотелось иметь уверенность в том, сколько им нужно инвестировать. По словам Анг Юита, вице-президента по разработке стратегий Ассоциации малых и средних предприятий (ASME), отраслевой группы, в которую входят сингапурские малые и средние предприятия, это побуждает больше рассматривать киберстрахование как способ достижения этой цели.

Отвечая на вопрос ZDNet о внедрении киберстрахования среди малых и средних предприятий, Анг отметил, что такие услуги позволяют малым и средним предприятиям повысить свою позицию в области кибербезопасности при

одновременном управлении своими расходами. Киберстрахование, приобретенное с ежемесячной премией, помогло этим компаниям лучше определить, сколько им нужно вложить и что они получают взамен.

По его словам, это позволило малому и среднему бизнесу определить объем и инвестиции в свою защиту от кибербезопасности в ходе виртуального круглого стола, организованного Lenovo в четверг.

Хотя это может не решить все проблемы, Анг добавил, что киберстрахование представляет собой жизнеспособную альтернативу простой покупке средств безопасности, стоимость которых может быть трудной для окончательной оценки.

…существуют различные услуги по страхованию от киберпространства, охватывающие пакеты, которые включают некоторое покрытие расходов, понесенных во время атаки, и помощь в количественной оценке воздействия атаки на данные и интеллектуальную собственность. Они также часто связаны со службами оценки безопасности и реагирования на инциденты, поскольку в интересах страховщика будет гарантировать, что SMB получил определенный уровень готовности к кибербезопасности, и смягчить воздействие атаки.

Кроме того, страховщики стремились предоставлять больше услуг, ориентированных на малый и средний бизнес, поскольку эти компании имеют гораздо меньшую инфраструктуру и, следовательно, несут меньше рисков, которые необходимо оценивать и страховать, по сравнению с крупными предприятиями.

По словам Милада Асланера, глобального директора SentinelOne по стратегии киберзащиты и связям с общественностью, в частности, простота внедрения имеет важное значение для повышения готовности к обеспечению безопасности в сегменте малого и среднего бизнеса.

Выступая за круглым столом, он сказал, что инструменты автоматизации, такие как автономное обнаружение угроз и реагирование на них, сыграли ключевую роль, поскольку они помогут упростить операции для малых предприятий. По словам Асланера, возможность отката после инцидента с безопасностью также имеет решающее значение.

Особенно важно было заставить предприятия малого и среднего бизнеса лучше защищать свою инфраструктуру, поскольку многие из них поспешили выйти в Интернет в условиях глобальной пандемии. Он предупредил, что это увеличило их поверхность для атак и раскрыло больше их данных, что сделало их основной целью атак, отметив, что киберпреступники будут нацелены на компании с более слабым уровнем безопасности.

Рой Нг, директор Lenovo по центральному Азиатско-Тихоокеанскому региону по SMB, отметил, что многие компании SMB ошибочно полагали, что они слишком малы, чтобы стать жертвами хакеров. Ссылаясь на исследование Агентства кибербезопасности Сингапура, Нг сказал, что количество зарегистрированных атак с использованием программ-вымогателей в прошлом году в основном затронуло малый и средний бизнес.

По его словам, эти небольшие компании хранят данные о клиентах, которые представляют ценность для киберпреступников.

МАЛЫЙ И СРЕДНИЙ БИЗНЕС МЕНЕЕ АКТИВЕН ИЗ-ЗА ПРЯМОГО ВЛИЯНИЯ НА БИЗНЕС

Однако Анг отметил, что большинство малых и средних предприятий не были должным образом подготовлены к противодействию угрозам безопасности и уже не имели прочной основы, даже несмотря на то, что они ускорили свое цифровое внедрение за последние 1,5 года во время пандемии.

«Малые и средние предприятия решат проблему, когда она возникнет. [Они больше] сосредоточены на оперативных потребностях», - сказал он.

ZDNet спросил, считают ли эти предприятия сложным отражать атаки третьих лиц, которые требуют регулярной оценки, он повторил тенденцию малых и средних предприятий не предпринимать активных действий для решения проблем, если не существует непосредственной угрозы или риска.

Если требование не было оговорено в контракте на обслуживание, они будут отдавать приоритет другим бизнес-операциям. Однако он отметил, что они были особенно обеспокоены соблюдением Закона Сингапура о защите личных данных (PDPA).

Указывая на управление личными данными как на хорошую отправную точку для повышения осведомленности о безопасности, он сказал, что малые и средние предприятия больше беспокоятся о том, как им следует защищать свои данные, чтобы им не пришлось столкнуться с последствиями нарушения в соответствии с PDPA.

Асланер сказал, что малому и среднему бизнесу также необходимо будет улучшить свою систему безопасности, поскольку все больше предприятий рассматривают архитектурные изменения на фоне роста сторонних атак, уделяя основное внимание фреймворкам с нулевым доверием.

Он отметил, что организации добавляли требования к кибербезопасности в рамках своих соглашений с поставщиками. По его словам, тогда малые и средние предприятия должны будут обеспечить соответствие этим базовым требованиям, если они захотят продолжить бизнес с определенными корпоративными клиентами.

Крис Тан, технический специалист Lenovo в Центральной Азии и Тихоокеанском регионе, предположил, что малые и средние предприятия начали с идентификации своих активов, включая устройства и точки данных.

Нг также подчеркнул важность обучения пользователей, чтобы сотрудники могли помочь своей организации избежать потенциального воздействия и угроз.

Согласно недавнему исследованию IBM, утечки данных обходятся компаниям Asean в среднем в 2,64 миллиона долларов за инцидент по сравнению с глобальной цифрой в 4,24 миллиона долларов. Однако стоимость взлома была на 430 000 долларов выше, чем в среднем для компаний в Asean, которые не подвергались цифровой трансформации из-за пандемии COVID-19.

В отчете IBM говорится, что организациям в регионе потребовалось 307 дней на обнаружение и устранение утечки данных, в том числе 223 дня только на обнаружение инцидента». ***(Eileen Yu. Singapore SMBs keen on cyber insurance, most anxious about data security // ZDNet (https://www.zdnet.com/article/singapore-smbs-keen-on-cyber-insurance-concern-about-data-security/). 12.08.2021).***

***

**«Согласно новому отчету EY, более половины (52%) ирландских команд по кибербезопасности считают, что они подвержены серьезному нарушению, которого можно было бы избежать, вложив дополнительные средства.**

В рамках глобального исследования информационной безопасности (GISS) 2021 EY приняли участие 1430 руководителей высшего звена в области кибербезопасности, в том числе 50 в Ирландии. Из них 90% заявили, что за последние 12 месяцев они наблюдали рост атак, по сравнению с 72% во всем мире.

Многие ирландские специалисты по безопасности считали, что их компании недостаточно серьезно относятся к этой проблеме. Менее трети (30%) заявили, что, по их мнению, высшее руководство полностью понимает ценность и потребности групп по кибербезопасности, по сравнению с 42% во всем мире.

Кроме того, более двух третей (68%) заявили, что с командами по кибербезопасности консультировались слишком поздно или вообще не консультировались, когда исполнительное руководство принимало стратегические решения, в то время как 44% заявили, что их бюджеты слишком малы для решения новых проблем, возникших за последний год.

Кэрол Мерфи, партнер-консультант и глава отдела технологических рисков EY Ireland, прокомментировала: «Улучшения можно добиться, повысив осведомленность об этих угрозах на уровне совета директоров и руководителей. Кибербезопасность часто теряется в списке приоритетов, и это может оставить незащищенным весь бизнес.

«Однако с учетом того, что нормативная нагрузка быстро растет, советы директоров начинают осознавать угрозу и уровень необходимых ресурсов, но не раньше времени».

Были некоторые области, в которых ирландские команды чувствовали себя более оптимистично, чем в среднем по миру. 70% респондентов заявили, что уверены в способности своей цепочки поставок защищаться от атак и восстанавливаться после них, в то время как только 33% респондентов в мире заявили то же самое. Однако в отчете EY отмечается, что это «наводит на мысль о том, что некоторые могут быть чрезмерно самоуверенными» в секторе кибербезопасности Ирландии.

Но 60рс заявили, что уверены в понимании и предвидении новых угроз и стратегий атак, которые Мерфи назвал «обнадеживающими».

«Исследование GISS выявляет ряд пробелов между ирландскими предприятиями и их международными партнерами. Отчасти это связано с бюджетными ограничениями, но также связано с отсутствием внутренней коммуникации и кажущимся разрывом между командами кибербезопасности и руководителями», - добавила она.

«Учитывая глобальную чрезвычайную ситуацию в области общественного здравоохранения, понятно, что в некоторых случаях были сделаны поправки, чтобы облегчить быстрое внедрение политики работы на дому».

Однако Мерфи предупредил, что по мере того, как удаленная и гибридная работа становится частью нормальной рабочей жизни, предприятиям «необходимо срочно устранять возникающие пробелы в безопасности».

Компании сообщают об увеличении количества атак, которым они подвергаются, но их интенсивность и стоимость могут также расти. Недавний отчет Palo Alto Networks показал, что в первой половине 2021 года средние выплаты в ответ на атаки программ-вымогателей увеличились на 82%». ***(Jack Kennedy. 52pc of Irish cybersecurity teams feel at risk of major breach – EY report // Silicon Republic Knowledge & Events Management Ltd (https://www.siliconrepublic.com/enterprise/ey-cybersecurity-report-2021). 26.08.2021).***

***

## Кібервійни та протидія зовнішній кібернетичній агресії

**«Міністр оборони Литви Арвідас Анушаускас заявив, що в результаті хакерської атаки в середу, 11 серпня, хакерам не вдалося отримати будь-які документи. Листування МЗС зловмисники отримали в листопаді минулого року…**

«Ми хочемо уточнити, що кібернетичний злом був проведений в листопаді минулого року. Кібератаку також намагалися влаштувати вчора, але вона не була успішною», — сказав міністр.

Він пов'язує цей злом з Росією.

«Ці активні діючі в нашому регіоні угруповання хакерів, які влаштовують кібератаки, зламують бази даних, вони, як правило, пов'язані зі спецслужбами Росії», — сказав Анушаускас.

«Я думаю, що так», — відповів він на питання, чи пов'язує він і цей випад з Росією.

Про те, що сталося в листопаді литовські відомства не повідомляли.

Вчора ряд литовських ЗМІ повідомили про атаку на зовнішньополітичне відомство Литви. За відомостями редакцій було вкрадено понад півтора мільйона одиниць листування міністерства з послами в зарубіжних країнах, партнерами по НАТО, а деякі документи — з грифом «Секретно». Як стверджують хакери, в листуванні литовські дипломати розкрили таємниці США проти Європи — переважно щодо газопроводу Nord Stream 2 («Північний потік 2»). Зокрема, за їхніми словами, в листах також обговорюються відносини з Білоруссю і Китаєм.

Анушаускас повідомив, що не може підтвердити автентичність документів, крім того, частина їх засекречена.

«Коли відбувається витік якоїсь інформації, слід знати, що існує ризик включення в зміст документів і фейковий новин, недостовірних даних, які можуть бути сфальсифіковані», — сказав міністр оборони.

За його словами, вкрадено трохи документів. «За оцінками фахівців, це не повинен бути період десятиліть. Це повинен бути невеликий період», — зазначив він.

Він заявив, що після злому в листопаді МЗС були представлені рекомендації, як організувати систему кібербезпеки, щоб інциденти не повторилися.

За його словами, рекомендації проведені в життя.

«Зроблений вчора невдалий випад може бути доказом», — підкреслив Анушаускас.

Він додав, що незважаючи на те, що документи були вкрадені в листопаді, про це було повідомлено тільки в ці дні, коли в Литві відбувалися політичні хвилювання.

«Так передбачається відповідальність перед найрізноманітніші цілі — дестабілізації ситуації, репутаційної шкоди», — сказав він.

Президент Литви Гітанас Науседа повідомив, що під час кібератаки на МЗС республіки міг статися витік засекреченої інформації, що завдає шкоди союзникам Литви.

За його словами, витік цієї інформації «може завдати великої шкоди перш за все щодо союзників». «Але це потенційна втрата, яку я зараз ще не можу публічно розкрити», — додав президент». ***(Глава Міноборони Литви: ймовірно російська хакерська атака не увінчалася успіхом // Дзеркало тижня. Україна (https://zn.ua/ukr/WORLD/hlava-minoboroni-litvi-jmovirno-rosijska-khakerska-ataka-ne-uvinchalasja-uspikhom.html). 12.08.2021).***

***

**«На японські урядові установи та приватні компанії здійснили серію кібератак.**

Внаслідок хакерських дій у 129 урядових установах та компаніях стався витік даних.

Злочинцям вдалося отримати доступ до програм обміну інформацією.

Жертвами кібератаки стали секретаріат японського Кабінету міністрів, Міністерство закордонних справ та Міністерство національних земель, інфраструктури, транспорту та туризму.

Серед викраденої інформації були дані про системи клієнтів, матеріали щодо реалізації проектів, а також деяка особиста інформація – імена та адреси електронних скриньок.

Витік інформації помітила японська компанія Fujitsu, яка оновила дані про несанкціонований доступ до її програми ProjectWEB.

ProjectWEB – це програма, яку дуже часто використовують урядові структури та інші компанії в Японії…». ***(Софія Зінов'єва. Урядові установи Японії зазнали кібератаки: сталося 129 витоків даних // ФАКТИ. ICTV (https://fakty.com.ua/ua/svit/svitovi-novyny/20210812-uryadovi-ustanovy-yaponiyi-zaznaly-kiberataky-stalosya-129-vytokiv-danyh/). 12.08.2021).***

***

**«Європейський Союз стурбований активністю РФ у кіберпросторі і готовий відповідати санкціями проти конкретних осіб і організацій.**

Дії представників країни можуть бути небезпечними для держустанов і організації країн.

– ЄС неодноразово озвучував цю стурбованість високопоставленим російським співрозмовникам, – заявив посол ЄС у РФ Маркус Едерер.

ЄС вже застосував режим кіберсанкцій проти фізичних та юридичних осіб. Зокрема, проти декількох російських фізосіб і однієї державноїо юридичної особи.

Їх спіймали на кібератаці на Організацію із заборони хімічної зброї, яка розташована у Нідерландах…». ***(Людмила Грубник. У кіберпросторі активізувались хакери з РФ, ЄС погрожує санкціями // ФАКТИ. ICTV (https://fakty.com.ua/ua/svit/20200810-u-kiberprostori-aktyvizuvalys-hakery-z-rf-yes-pogrozhuye-sanktsiyamy/). 10.08.2021).***

***

**«За останнє десятиліття російський уряд здійснив понад 10 значних кібератак проти іноземних країн.** Іноді для того, щоб допомогти чи завдати шкоди конкретному політичному кандидату, іноді – аби посіяти хаос. Але завжди для просування проєктів російської влади. Починаючи з 2007 року, росіяни атакували колишні радянські колонії, такі як Естонія, Грузія та Україна, а потім їх атаки розповсюдилися на західні країни, такі як:

США;

Німеччина.

Початком значних кібератак можна вважати квітень – травень 2007 року. Естонія – крихітна балтійська держава – розлютила Москву, плануючи перенести меморіал Другої світової війни та могили російських солдатів.

Росія у відповідь тимчасово вимкнула інтернет в Естонії, що стало надзвичайно сильним ударом у найбільш залежній від інтернету економіці світу. DDoS-атака була зосереджена на урядових установах та фінансових установах, порушуючи їхній зв'язок і взаємодію. Наступного, 2008 року, коли Росія вдерлася до Грузії, російські хакери здійснили напад на грузинський інтернет. Вперше Росія координувала військові та кібердії. Внутрішні комунікації Грузії були фактично вимкнені.

У січні 2009 року, в рамках спроб переконати президента Киргизстану виселити американську військову базу, російські хакери закрили 2 із 4 провайдерів інтернет-послуг країни за допомогою DDoS-атаки.

В серпні 2009 року російські хакери закрили твітер і фейсбук у Грузії на честь першої річниці російського вторгнення.

У березні 2014 року вдруге російський уряд координував військові та кібер-дії. DDoS-атака в 32 рази потужніша за найбільшу відому, використану під час вторгнення в Грузію, порушила роботу інтернету в Україні. В цей час російські солдати та озброєні Росією бойовики захоплювали контроль над Кримом.

У травні 2014 року, за 3 дні до президентських виборів в Україні, хакерська група, яка базується в Росії, знищила виборчу комісію в країні під час нічної атаки.

Тоді навіть резервну систему зняли, але українським комп'ютерним експертам вдалося відновити систему до дня виборів. Українська поліція повідомила, що заарештувала хакерів, які намагалися сфальсифікувати результати виборів.

У травні 2015 року німецькі слідчі виявили хакерський злам комп'ютерної мережі німецького Бундестагу, що стало найбільшою хакерською атакою в історії Німеччини.

Пізніше внутрішня розвідувальна служба Німеччини заявила, що за нападом стоїть Росія, і що росіяни шукають інформацію, яка стосується німецьких лідерів та НАТО. Хакери намагалися проникнути до комп'ютерів партії канцлера Ангели Меркель.

У жовтні 2015 року експерти з безпеки заявили, що російський уряд намагався зламати комп'ютери уряду Нідерландів, щоб знищити звіт про збиття рейсу MH17 над Україною. У грудні 2015 року російські хакери:

захопили центр управління української електростанції;

заблокували контролери у їхніх власних системах;

залишили 235 тисяч будинків без електроенергії.

У 2015 – листопаді 2016 року у США російські хакери проникли на комп'ютери Демократичної партії та отримали доступ до особистих електронних листів партійних чиновників, і розповсюдили їх.

У 2020 році група програмістів російської зовнішньої розвідки, відома як APT29 або Cosy Bear, проникла в мережі багатьох урядових установ США, зокрема у міністерства фінансів, торгівлі, енергетики та Національну адміністрацію ядерної безпеки.

Цей злам був настільки серйозним, що 12 грудня 2020 року уряд США провів позачергове засідання для обговорення ситуації.

Хакерська атака 7 травня 2021 року паралізувала трубопровід "Колоніальний", який постачає приблизно 45% бензину та дизельного палива для Східного узбережжя США.

ФБР визначило групу DarkSide, яка вимагала викуп. Ця група хакерів діє з серпня 2020 року і здійснює атаки, які шифрують комп'ютерні системи, пізніше вимагаючи від своїх адміністраторів викуп.

США відповіли санкціями

Після нападу президент Джо Байден сказав, що прямі докази відповідальності російського уряду відсутні. Проте він підтвердив наявність ознак того, що ці програми шантажу розробили в Росії.

То як же Сполучені Штати Америки відповіли на це? Звісно, санкціями.

До червня 2021 року санкції США запровадили щодо 170 російських осіб, зокрема щодо Російської федеральної служби безпеки (ФСБ) та Військового розвідувального управління (ГРУ).

Список санкцій також містив цілу мережу людей, пов'язаних з російським олігархом Євгеном Пригожиним, які періодично фінансували операції в США.

Це далеко не повний перелік злочинів, які здійснила Росія. У наступних випусках ми продовжимо знайомити вас із аналітичними матеріалами, які зібрали волонтери InformNapalm». ***(Михаил Макарук. Санкции как наказания за системные кибератаки: США проучивает Россию за хакерские нападения // ЗАО «Телерадиокомпания" Люкс "» (https://24tv.ua/ru/sankcii-nakazanija-za-sistemnye-kiberataki-ssha-rossija-novosti_n1714377). 16.08.2021).***

***

**«Агентство по кибербезопасности и безопасности инфраструктуры (CISA) объявило сегодня об открытии Совместного сотрудничества в области киберзащиты (JCDC), нового агентства, направленного на разработку планов операций по киберзащите и выполнение этих планов в координации с партнерами из федеральные межведомственные, частные и государственные, местные, племенные, территориальные (SLTT) государственные заинтересованные стороны (SLTT), чтобы снизить риск до инцидента и унифицировать защитные действия в случае инцидента.**

CISA создает JCDC для интеграции уникальных кибер-возможностей нескольких федеральных агентств, многих штатов и местных органов власти, а также бесчисленных организаций частного сектора для достижения общих целей. В частности, JCDC будет:

Разрабатывать и реализовывать комплексные общенациональные планы киберзащиты для устранения рисков и содействия скоординированным действиям;

Делитесь информацией, чтобы сформировать общее понимание проблем и возможностей киберзащиты;

Осуществлять скоординированные защитные кибероперации для предотвращения и снижения воздействия кибер-вторжений; а также

Поддерживайте совместные учения для улучшения операций по киберзащите.

«JCDC представляет собой захватывающую и важную возможность для этого агентства и наших партнеров - создание уникальной возможности планирования, которая будет проактивным обратным реагированием в нашем коллективном подходе к борьбе с наиболее серьезными киберугрозами для нашей страны», - сказала директор CISA Джен Истерли. «Отраслевые партнеры, которые согласились работать бок о бок с CISA, и наши межведомственные товарищи по команде разделяют ту же приверженность защите важнейших национальных функций нашей страны от кибер-вторжений и воображение для поиска новых решений. Вместе с этими чрезвычайно способными партнерами мы вначале сосредоточимся на усилиях по борьбе с программами-вымогателями и разработке системы планирования для координации инцидентов, затрагивающих поставщиков облачных услуг».

Первыми отраслевыми партнерами, участвующими в JCDC, являются Amazon Web Services, AT&T, CrowdStrike, FireEye Mandiant, Google Cloud, Lumen, Microsoft, Palo Alto Networks и Verizon. Это только начало, поскольку JCDC будет стремиться привлекать партнеров из частного сектора и SLTT из разных секторов по мере расширения наших сфер деятельности. Государственные партнеры включают Министерство обороны, Киберкомандование США, Агентство национальной безопасности, Министерство юстиции, Федеральное бюро расследований и Управление директора национальной разведки, а агентства по управлению рисками в секторах присоединяются к нашим усилиям по мере нашего продвижения вперед.

В последние месяцы различные крупные киберинциденты оказали влияние на наше критически важное инфраструктурное сообщество и вызвали последующие

последствия для американцев, которые полагаются на него для выполнения повседневных функций. Федеральное правительство, правительства SLTT и частный сектор неустанно работают над укреплением нашей оборонительной позиции, но никто из нас не может сделать это в одиночку. Как сообщество, JCDC будет использовать инновации, сотрудничество и воображение для защиты американского бизнеса, государственных учреждений и наших людей от кибер-вторжений». ***(CISA LAUNCHES NEW JOINT CYBER DEFENSE COLLABORATIVE // Cybersecurity and Infrastructure Security Agency (CISA) (https://www.cisa.gov/news/2021/08/05/cisa-launches-new-joint-cyber-defense-collaborative). 06.08.2021).***

***

**«Эксперты ИБ-компании Group-IB выявили связь между китайскими проправительственными хакерами и множественными кибератаками на российский госсектор в 2020 г.** По их мнению, за ними стоят как минимум две группировки или одна большая группа, объединяющая в себе несколько менее крупных. Это является нарушением соглашения между Россией и Китаем о взаимном ненападении в киберпространстве, подписанного в мае 2015 г.

*Китай взломал Россию*

Российские органы власти в 2020 г. подверглись ряду кибератак со стороны китайских APT-группировок. Об этом говорится в новом отчете компании Group IB, работающей в сфере информационной безопасности.

Отчет получил название «Искусство кибервойны» (The Art of Cyberwarfare, вероятно, по аналогии с известным древнекитайским трактатом «Искусство войны» (The art of war). Документ подготовлен руководитель группы исследования сложных угроз Threat Intelligence Group-IB Анастасией Тихоновой и ведущим специалистом по анализу вредоносного кода Threat Intelligence Group-IB Дмитрием Купиным. Авторы утверждают, что APT-группировки, атаковавшие российский госсектор, финансируются правительством КНР.

«Китайские прогосударственные группы — одно из самых многочисленных и агрессивных хакерских сообществ. Несколько десятков групп проводят атаки по всему миру, в том числе и в России. В первую очередь хакеров интересуют государственные ведомства, промышленные объекты, военные подрядчики, научно-исследовательские институты», – сказано в документе.

По оценке авторов отчета, хакеры атакуют российские госорганы, преследуя лишь одну цель – длительный шпионаж. Взламывая государственные компьютерные сети, злоумышленники крадут нужные им документы, при этом стараясь как можно дольше скрывать следы своего присутствия.

*Маскировка под ПО «Яндекса»*

Эксперты Group-IB приводят в качестве примера атаки использованием вредоноса Webdav-O. С их слов, он очень похож на троян BlueTraveller (он же RemShell), за которым может стоять китайская APT-группировка TaskMasters.

Согласно отчету американской ИБ-компании Sentinel Labs об атаке на российские федеральные органы власти в 2020 г. (опубликован в мае 2021 г.), приложение Webdav-O хакеры маскируют под утилиту Yandex Disk.

В ходе исследования специалисты Group-IB выяснили, что в распоряжении хакеров есть две версии Webdav-O – x64 и x86. Также им удалось установить, что троян существует с 2018 г., хотя против российских ФОИВов он был впервые использован именно в 2020 г. Отметим, что на американский онлайн-сканер вирусов VirusTotal сигнатуры Webdav-O были загружены в конце осени 2019 г.

*Китайские группировки-матрешки*

Отчет Sentinel Lab, упоминающийся в исследовании Group-IB, сам по себе базируется на отчете центра противодействия кибератакам «Ростелеком-Солар» и специализированной службы ФСБ России. Он был опубликован в мае 2021 г.

В документе Sentinel Lab говорится о малвари под названием Mail-O, замаскированном под программу Mail.ru Group Disk-O. Оно тоже использовалось в атаках на российские ФОИВы в 2020 г., но его использует китайская APT-группировка TA428.

Эксперты Group-IB утверждают, что в своих атаках TA428 регулярно использует троян Albaniiutas. Проанализировав его, они установили, что его нельзя считать по-настоящему самостоятельным трояном, написанным с нуля. Это всего лишь модифицированный BlueTraveller, которым пользуются хакеры из TaskMasters.

На основе всего этого Анастасия Тихонова и Дмитрий Купин пришли к выводу, что, вероятно, и TaskMasters, и TA428 участвовали в кибератаках на российский госсектор в 2020 г. Также они не исключают вариант, что в Китае существует некая гигантская группа хакеров, которая объединяет в себе несколько мелких группировок.

«Не менее весомым звучит предположение, что существует одна большая хакерская группировка, которая состоит из нескольких подразделений разведки Народно-освободительной армии Китая. Например, подразделение 61398 из Шанхая стоит за действиями хорошо известной группировки APT1 (aka Comment Crew), а подразделение 61419 из города Циньдао связано с группировкой Tick. Каждое подразделение атакует в меру своих возможностей, времени или выстроенной очередности. Таким образом, один троян может настраиваться и дорабатываться хакерами разных подразделений с разным уровнем подготовки и целями», – говорится в отчете.

Специалисты Group-IB подчеркнули, что китайские хакерские группировки регулярно обмениваются инструментами и инфраструктурами. Они не исключают, что в случае с атаками на российские ФОИВы они тоже так делали.

*Хакеры с многолетним опытом*

Обе упомянутые в отчете Group-IB хакерские группировки, появились не год и даже не два назад. Например, TA428 действует как минимум с 2013 г. По оценке экспертов компании, их ochodyst цели – это правительственные агентства в Восточной Азии, контролирующие государственные информационные технологии, а также внутреннюю и международную политику и экономическое развитие.

Первые упоминания о группе TaskMasters датированы 2010 г., но не исключено, что она появилась еще раньше. За прошедшие 11 лет входящие в ее состав киберпреступники провели атаки на различные компании и предприятия во многих странах мира, однако больше всего их жертв находятся в России и странах

СНГ. «Среди атакуемых организаций – крупные промышленные и энергетические предприятия, государственные структуры, транспортные компании», – отмечено в отчете Group-IB.

*Китай нарушает договор*

Следует отметить, что если за всеми атаками на российские ФОИВы действительно стоят китайские проправительственные хакеры, то это является прямым нарушением договоренности между Россией и КНР. По данным «Коммерсанта», еще в начале мая 2015 г. страны подписали соглашение о сотрудничестве в области международной информационной безопасности. Одно из положений документа гласит, что Россия и Китай не могут проводить кибератаки друг против друга. На момент публикации материала соглашение оставалось в силе и изменений не претерпевало». ***(Китайские хакеры в течение года атаковали российские госорганы. Это прямое нарушение договора между странами // CNews (https://www.cnews.ru/news/top/2021-08-05_kitajskie_hakery_v_techenie). 05.08.2021).***

***

**«Російській Федерації відомо, хто стоїть за масштабними кібератаками з використанням вірусів-вимагачів.**

У червні в Женеві відбувся саміт Байдена з главою Росії Володимиром Путіним. Президент країни-агресора за підсумками переговорів повідомив, що Москва і Вашингтон домовилися почати консультації з кібербезпеки. Однак Москва знає причетних до хакерських атак. Таку заяву зробив американський лідер, повідомляє CNN.

У мене був саміт з президентом Росії Володимиром Путіним. Я дав зрозуміти, що ми чекаємо, що вони залучать їх до відповіді, тому що російська влада знає, де вони та хто вони, — зазначив Байден.

Як відомо, в грудні 2020 року хакери проникли в системи американської компанії SolarWinds, яка виробляє програмне забезпечення для управління і забезпечення безпеки комп’ютерних систем. Завдяки кібератаці були зламані системи, що належать міністерству фінансів США, міністерству внутрішньої безпеки, Національному управлінню телекомунікацій і інформації, Мінторгу США, Пентагону, Міненерго та відомству, яке опікується безпекою в ядерній сфері NNSA.

Після хакерських атак у Вашингтоні заявили, що за ними стоїть хакерська група APT29 або Cozy Bear, пов’язана з російською розвідкою…» ***(Москва знає, хто стоїть за масштабними кібератаками — Байден // Ракурс (https://racurs.ua/ua/n159238-moskva-znaie-hto-stoyit-za-masshtabnymy-kiberatakamy-bayden.html). 26.08.2021).***

***

**«Сьогодні три країни світу змагаються у галузі кібербезпеки. Це США, Китай та Росія, які мають найбільший потенціал, а новою стратегічною візією є те, що все більше країн розвивають власні кіберможливості до захисту та атак, пише Лукаш Олейник для польського видання Dziennik Gazeta Prawna.**

Автор зазначає, що сьогодні пріоритетом є розвиток кібервійськ. І у цих змаганнях вже є кілька десятків країн. Але попереду США, Китай та Росія, в яких найбільший потенціал. Далі йдуть Франція, Нідерланди, Велика Британія.

Сусідня з Україною Польща також будує Війська оборони кіберпростору, хоча на сьогодні Варшава не опублікувала жодного стратегічного документа, у якому би йшлося про призначення цих кібервійськ.

Одним з елементів у кіберпросторі є нещодавній документ президента РФ Владіміра Путіна "Про стратегію національної безпеки РФ". В ньому йдеться про розбудову «цифрового суверенітету». У документі також йдеться про багато елементів, що стосуються безпеки інформації й кібербезпеки.

Країнам варто детально проаналізувати цей документ, попереджає автор. У ньому передбачено розбудову безпечної інфраструктури обігу державної інформації, створення системи прогнозування загроз, окреслення їх джерел та виокремлення наслідків, захист критичної інфраструктури від деструктивних атак, зменшення кількості витоків даних і порушення безпеки та інше, йдеться на шпальтах Dziennik Gazeta Prawna.

Однак, продовжує автор, найважливішим є прихований пункт у документі Путіна. Там йдеться про «розвиток сил та засобів інформаційної боротьби». У російській номенклатурі йдеться про «безпеку інформації». Це ширше, ніж західна термінологія, яка каже про безпеку у кіберпросторі. Експерт у статті каже, що "справа – зрозуміла: Росія у важливому документі прямо заявляє про розбудову засобів для кібератак та інформаційної боротьби. І це «безпрецедентне оголошення», резюмує Лукаш Олейник». ***(Путін зробив безпрецедентне оголошення. Росія офіційно вступає в еру кібервоєн – Dziennik Gazeta Prawna // Дзеркало тижня. Україна (https://zn.ua/ukr/WORLD/putin-zrobiv-bezpretsedentne-oholoshennja-rosija-ofitsijno-vstupaje-v-eru-kibervojen-dziennik-gazeta-prawna.html). 04.08.2021).***

***

## Кіберзахист критичної інфраструктури

**«Цифровизация и удаленный мониторинг стали важным шагом в нефтегазовой отрасли, однако данные достижения сделали морские буровые установки более уязвимыми к кибератакам, ставя под угрозу производственную безопасность.**

Специалисты из ИБ-фирмы Naval Dome провели исследование по выявлению и снижению киберрисков, характерных для морских глубоководных буровых

установок. Как показали результаты двухлетнего исследования, минимальные отраслевые правила и методы безопасности не соответствуют текущим технологиям платформы, требованиям к подключению и тактике по защите от кибератак.

Системы, установленные на морских платформах, традиционно были изолированными и не подключенными к Сети, что ограничивало успех атак хакеров. Однако обширное применение удаленного мониторинга и автономного управления, IoT-технологии и цифровизация сделали буровые установки гораздо более восприимчивыми к потенциальным кибератакам, пояснили эксперты.

Специалисты рассказали, как им удалось взломать технологические сети эксплуатации испытательных стендов, используя установочный файл программного обеспечения для динамического позиционирования и графики рабочих станций. Naval Dome смоделировала штатного специалиста по обслуживанию, который невольно использовал USB-накопитель с вредоносным программным обеспечением, содержащим три эксплоита для уязвимостей нулевого дня.

«Измененный файл был упакован таким образом, что выглядел и действовал как исходный, и прошел антивирусное сканирование, не будучи идентифицированным как вредоносный или обнаруженным установленной системой мониторинга сетевого трафика», — пояснили исследователи.

Хотя атака была проведена внутри неназванной компании, удаленное выполнение также можно было осуществить с использованием внешних сетевых подключений буровой установки.

По результатам тестов стало известно, что традиционных ИТ-систем «периметрального типа», трансплантированных ОТ-решений для кибербезопасности, таких как антивирусы, мониторинг сети и межсетевые экраны недостаточно для защиты и обеспечения безопасности критически важного оборудования.

Как отметили специалисты, необходимы более продвинутые специализированные решения для лучшей защиты оффшорной платформы от внешних и внутренних кибератак». ***(Морские буровые установки стали более уязвимыми к кибератакам // SecurityLab.ru (https://www.securitylab.ru/news/523824.php). 27.08.2021).***

***

## Захист персональних даних

**«Ймовірно, російське угруповання хакерів All World Cards виклало в прихованій мережі дані мільйона банківських карт громадян США та інших країн, повідомляє телеканал CNBC з посиланням на аналітиків компанії Q6 зі сфери кібербезпеки.**

Телеканал CNBC зняв сюжет, де показав скріншот з оголошенням All World Cards російською мовою про те, що вони "публікують у відкритому доступі" дані 1 млн банківських карт.

За даними аналітиків, дані банківських карт пропонуються іншим кіберзлочинцям.

Напередодні Міністерство юстиції США заявило, що хакери, відповідальні за масштабне кібернапад SolarWinds, в минулому році зламали акаунти в службах більше двох десятків прокурорів в США в 15 штатах і окрузі Колумбія. Зловмисники мали доступ до зламаним акаунтів з травня по грудень 2020 року». ***(Російські хакери виклали в даркнет дані мільйона банківських карт громадян США та інших країн // Дзеркало тижня. Україна (https://zn.ua/ukr/TECHNOLOGIES/rosijski-khakeri-viklali-v-darkneta-dani-miljona-bankivskikh-kart-hromadjan-ssha-ta-inshikh-krajin.html). 06.08.2021).***

***

**«Посещение спортивных событий всегда было любимым занятием ярых болельщиков, однако во время пандемии большинство мероприятий было отменено или перенесено на онлайн-платформы. Из-за этого довольно популярными стали трансляции в Интернете, а вместе с ними появились и новые риски для безопасности личных данных фанатов.**

В связи с этим специалисты ESET подготовили советы, которые помогут защитить устройства пользователей во время посещения стриминговых сервисов.

1. Обеспечить защиту роутера и домашней сети

Для просмотра онлайн-трансляций необходим роутер, который позволяет подключать множество устройств к домашней сети и получать доступ к стриминговым сервисам. Однако незащищенный роутер могут использовать злоумышленники для доступа и заражения всех подключенных к нему девайсов. Поэтому прежде чем подключить устройство и начать просмотр онлайн-трансляции, важно убедиться в корректности настройки вашего роутера.

Следующим шагом для защиты роутера и всей домашней сети является создание отдельных сетей с настроенными разрешениями. Это позволит отключать устройства, которые не используются, а также упростит выявление попыток проникновения злоумышленников.

2. Настроить смарт-телевизор

Для начала необходимо изменить на своих устройствах параметры конфиденциальности, а также разрешения на сбор информации поставщиком и ее передачу третьим лицам. Поскольку были инциденты, при которых некоторые провайдеры собирали личные данные своих пользователей, включая записи голоса и привычек просмотра.

Также опасность может представлять и включение всех возможных функций устройства, которые могут иметь неисправленные уязвимости и использоваться киберпреступниками. Поэтому пользователю важно выключать функции, которые ему не нужны. Кроме этого, стоит включить имеющиеся настройки безопасности, предложенные производителем, и родительский контроль в случае необходимости.

3. Установить актуальные обновления

На всех устройствах, на которых пользователь планирует смотреть онлайн-трансляции, необходимо регулярно обновлять операционную систему для исправления уязвимостей и предотвращения их использования киберпреступниками. В отличие от операционной системы компьютера или смартфона, встроенное программное обеспечение большинства смарт-телевизоров не обновляется автоматически. Для проверки наличия обновлений нужно найти сайт поставщика, указав номер модели устройства и текущую версию установленного встроенного ПО.

4. Использовать решения по безопасности

Устройства пользователя могут быть заражены вредоносным программным обеспечением или другими видами киберугроз. Поэтому стоит использовать комплексное решение для защиты смарт-телевизора от вирусов и программ-вымогателей или программу по безопасности для смартфонов и планшетов, которая в дополнение к функции Антивируса защищает устройство при осуществлении онлайн-платежей.

5. Выбирать надежные сервисы для просмотра

Для просмотра онлайн-трансляций доступны бесплатные и платные сайты, среди которых могут быть и вредоносные. В частности, на некоторых бесплатных ресурсах присутствует большое количество рекламы. По результатам анализа 23 000 стриминговых сайтов половина видеорекламы, которая отображалась на них, перенаправляла жертв на вредоносные сайты. Киберпреступники используют различные схемы для заманивания пользователей – от техник социальной инженерии до поддельных сайтов для майнинга криптовалюты.

Платные сайты могут быть более безопасными при условии, что они являются легитимными. Однако даже лидеры на рынке онлайн-трансляций, например, Disney+ или Amazon Prime и Hulu, не защищены от потенциальных рисков, в частности, утечек данных, которые ставят под угрозу информацию всех своих пользователей. Поэтому простыми и эффективными мерами для базовой защиты остается использование надежного и уникального пароля, а также проверка учетной записи с помощью ресурса haveibeenpwned». ***(Эксперты объяснили правила кибербезопасности на стриминговых сервисах // УНІАН (https://www.unian.net/science/eksperty-obyasnili-pravila-kiberbezopasnosti-na-strimingovyh-servisah-novosti-11517772.html). 19.08.2021).***

***

**«Великобритания объявила о планах изменить законы о защите данных и конфиденциальности, что правительство описывает как новый мандат, способствующий инновациям и экономическому росту.**

Новая серия «партнерств по обеспечению адекватности данных» позволит Великобритании вести международную торговлю со странами и организациями, включая США, Австралию, Республику Корея, Сингапур, Международный финансовый центр Дубая и Департамент цифровых технологий, культуры и СМИ Колумбии. & Sport (DCMS) сказал.

По мнению правительства, партнерство по обеспечению адекватности данных устранит необходимость в дорогостоящих мерах по обеспечению

соответствия данных при передаче личных данных в другие страны. В заявлении DCMS говорится, что это произойдет при одновременном обеспечении «высоких стандартов защиты данных».

Любые изменения в правилах передачи данных также должны быть признаны Европейским союзом адекватными - в противном случае существует риск, что это повлияет на передачу данных между Соединенным Королевством и ЕС.

Предлагаемые изменения являются частью планов правительства по «использованию возможностей данных для стимулирования роста и создания рабочих мест», хотя некоторые эксперты по конфиденциальности данных выразили озабоченность по поводу того, что изменения могут быть использованы для отката конфиденциальности данных для потребителей, привлеченных как часть Общие правила защиты данных (GDPR).

GDPR был введен по всему Европейскому Союзу в мае 2018 года, и, несмотря на то, что Великобритания проголосовала за выход из ЕС, законы о защите данных были применены. Но теперь правительство заявляет, что после Brexit страна может получить выгоду от отклонения своих законов о защите данных от законов остальной Европы.

«Теперь, когда мы покинули ЕС, я полон решимости воспользоваться этой возможностью, разработав ведущую в мире политику в области данных», - сказал Государственный секретарь по цифровым технологиям, культуре, СМИ и спорту Оливер Дауден.

«Это означает реформирование наших собственных законов о данных, чтобы они основывались на здравом смысле, а не на галочке», - добавил он.

В интервью The Telegraph Дауден выделил политику, касающуюся «бессмысленных» запросов файлов cookie, как нечто, от чего Великобритания может теперь отклониться, но несколько экспертов по конфиденциальности данных указали, что файлы cookie подпадают под действие совершенно иной директивы, чем GDPR.

Эксперты по конфиденциальности данных также выразили обеспокоенность по поводу того, что предлагаемые планы изменят роль Управления комиссара по информации (ICO) с функции регулятора конфиденциальности на содействие экономическому росту.

Представитель DCMS сказал ZDNet, что «мы не собираемся ставить под угрозу наши высокие стандарты данных, а также конфиденциальность и защиту данных».

Правительство намерено начать консультации о роли ICO в сентябре, чтобы «у него были полномочия для поощрения ответственного использования данных для достижения экономических и социальных целей, а также предотвращения нарушений конфиденциальности до того, как они произойдут».

DCMS также объявила о предпочтительном преемнике Элизабет Денхэм на посту комиссара по информации: Джона Эдвардса, который в настоящее время является комиссаром Новой Зеландии по конфиденциальности.

«Есть прекрасная возможность развить уже проделанную замечательную работу, и я с нетерпением жду задачи вывести организацию и британскую

экономику на позицию международного лидера в безопасном и надежном использовании данных на благо всех», - сказал Эдвардс.

По словам Оливера Даудена, Эдвардс обладает опытом, необходимым для «перехода к новой эре роста на основе данных и инноваций в ICO».

«Обширный опыт Джона Эдвардса делает его идеальным кандидатом для ответственного использования данных для достижения этих целей», - добавил Дауден». ***(Danny Palmer. Data protection: UK to diverge from GDPR in post-Brexit overhaul of privacy rules // ZDNet (https://www.zdnet.com/article/data-protection-to-diverge-from-gdpr-in-post-brexit-overhaul-of-privacy-rules/). 26.08.2021).***

***

**«Отрасль медицинских услуг по-прежнему является сектором, ответственным за наибольшее количество зарегистрированных утечек данных в Австралии, на долю которых приходится 85 из 446 общих нарушений, о которых было сообщено в Управление комиссара по информации Австралии (OAIC) за шесть месяцев до 30 июня 2021 года.**

Общее количество 446 уведомлений ниже на 16% по сравнению с 530 уведомлениями за предыдущие шесть месяцев. В 2020-21 финансовом году было получено 976 уведомлений по схеме уведомляемых утечек данных (NDB).

Наибольшее количество уведомлений было отправлено в марте - 102.

В отчетном периоде 81% нарушений были выявлены организацией в течение 30 дней с момента их возникновения, но в 4% случаев на это потребовалось более 365 дней.

«Что касается утечки данных, вызванной злонамеренным или преступным нападением или ошибкой человека, более 80% организаций идентифицировали инцидент в течение 30 дней с момента его возникновения», - пишет OAIC. «В тех случаях, когда организации столкнулись с утечкой данных в результате сбоя системы, только 61% выявили инцидент в течение 30 дней, а 30% не узнали об инциденте более года».

В отчетном периоде 72% организаций уведомили OAIC в течение 30 дней после того, как им стало известно об инциденте, который впоследствии был признан допустимой утечкой данных. 27 организациям потребовалось более 120 дней с момента, когда они узнали об инциденте, чтобы уведомить OAIC.

71% правительственных агентств Австралии, сообщивших об инциденте, обнаружили его в течение 30 дней. Однако на поиск 9% потребовалось больше года. 3% потребовалось больше года, чтобы уведомить OAIC.

Со времени действия мандата сектор здравоохранения наиболее пострадал. На втором месте после здравоохранения в этой половине был финансовый сектор, на который приходилось 57 уведомлений, затем следуют юридический и бухгалтерский сектор с 35, а также сектор правительства и страхования Австралии с 34 уведомлениями.

Правительство Австралии вошло в пятерку крупнейших секторов экономики в первой половине 21 финансового года.

Все агентства и организации в Австралии, подпадающие под действие Закона о конфиденциальности 1988 г., обязаны уведомлять лиц, чья личная информация

связана с утечкой данных, которая может привести к «серьезному ущербу», как можно скорее после того, как станет известно о нарушении. Закон о конфиденциальности распространяется на большинство правительственных агентств Австралии; он не охватывает ряд разведывательных служб и агентств национальной безопасности, а также не охватывает государственные и местные правительственные учреждения, государственные больницы и государственные школы.

В своем последнем шестимесячном отчете [PDF], в котором собраны уведомления, сделанные в рамках схемы NDB, OAIC сообщило, что большинство утечек данных связано с личной информацией 5000 человек или меньше.

Три уведомления затронули более 1 миллиона человек, одно - более 10 миллионов человек.

Контактная информация, идентификационная информация и финансовые данные по-прежнему являются наиболее распространенными типами личной информации, связанной с утечкой данных. 407 - или 91% - нарушений, о которых было сообщено по схеме, касались контактной информации, такой как имя человека, домашний адрес, номер телефона или адрес электронной почты.

В 247 случаях была нарушена личная информация, в 193 случаях раскрыта финансовая информация, в 136 случаях - информация о здоровье, номера налоговых файлов были раскрыты в 102 случаях, а другая конфиденциальная информация была скомпрометирована в 75 случаях.

Вредоносные или криминальные атаки были крупнейшим источником утечки данных, о котором было уведомлено OAIC, и составили 289 нарушений. 192 нарушения были вызваны «киберинцидентами», 35 из них были результатом социальной инженерии или выдачи себя за другое лицо, в 28 случаях причиной были действия, предпринятые мошенником или инсайдерская угроза, а кража документов или устройств хранения была ответственна за 34 уведомления.

В отчете говорится, что человеческая ошибка также оставалась основным источником нарушений, на которые приходилось 134 уведомления, в то время как системные сбои составляли оставшиеся 23 нарушения.

Нарушения, связанные с человеческой ошибкой, включают отправку личной информации не тому получателю по электронной почте, непреднамеренное раскрытие или публикацию личной информации, а также отказ от использования функции слепой копии при отправке групповых электронных писем.

Несанкционированное раскрытие / непреднамеренный выпуск или публикация произошли в 31 уведомлении. Только от этого пострадало 523 998 человек.

Правительство Австралии не сообщало о каких-либо инцидентах, связанных с системными сбоями, но сообщило о 25 как человеческие ошибки и девять как злонамеренные или преступные атаки. Правительство Австралии также сообщило об одном инциденте как о «взломе».

Основными источниками киберинцидентов в отчетный период были фишинг, взлом или кража учетных данных и программы-вымогатели.

«Более половины киберинцидентов (62%) за отчетный период связаны с получением злоумышленниками доступа к учетным записям с использованием

скомпрометированных или украденных учетных данных», - говорится в сообщении OAIC. «Наиболее распространенным методом, используемым злоумышленниками для получения скомпрометированных учетных данных, был фишинг на основе электронной почты (58 уведомлений)».

Количество инцидентов, связанных с программами-вымогателями, увеличилось на 24% во втором полугодии, с 37 в первом полугодии до 46». ***(Asha Barbaschow. 446 Australian breach notifications with 30% of system faults found after a year // ZDNet (https://www.zdnet.com/article/446-australian-breach-notifications-with-30-of-system-faults-found-after-a-year/). 23.08.2021).***

***

**«По данным Upguard, конфиденциальные данные, включая статусы вакцинации COVID-19, номера социального страхования и адреса электронной почты, были раскрыты из-за слабых настроек по умолчанию для Microsoft Power Apps.**

Upguard Research обнаружила множественные утечки данных, раскрывающие 38 миллионов записей данных через порталы Microsoft Power Apps, настроенные для разрешения общего доступа.

Утечки данных затронули American Airlines, Microsoft, JB Hunt и правительства Индианы, Мэриленда и Нью-Йорка. Upguard впервые обнаружила проблему, связанную с API ODdata для портала Power Apps 24 мая, и 24 июня отправила в Microsoft отчет об уязвимости.

Согласно Upguard, основная проблема заключается в том, что все типы данных были общедоступными, тогда как некоторые данные, такие как личная идентификационная информация, должны были быть конфиденциальными. Неправильная конфигурация привела к появлению некоторых личных данных.

Microsoft Power Apps - это инструменты с низким кодом для разработки приложений и создания общедоступных и частных веб-сайтов». ***(Larry Dignan. Microsoft Power Apps misconfiguration exposes 38 million data records // ZDNet (https://www.zdnet.com/article/microsoft-power-apps-misconfiguration-exposes-38-million-data-records/). 23.08.2021).***

***

**«Новый отчет Citizen Lab показал, что спорный НС Группа поставила средства наблюдения правительству Бахрейна в период с июня 2020 года и в февраль 2021 года.**

Компания столкнулась с резкой негативной реакцией, поскольку выяснилось, что они помогали десяткам организаций шпионить за мировыми лидерами, активистами, журналистами и другими людьми, используя шпионское ПО Pegasus.

В последнем отчете Citizen Lab, авторами которого являются Али Абдулемам, Нура Аль-Джизави, Билл Марчак, Сиена Анстис, Кристин Бердан, Джон Скотт-Рейлтон и Рон Дейберт, говорится, что у девяти активистов из Бахрейна были взломаны iPhone с помощью шпионского ПО NSO Group. а некоторые были атакованы с помощью эксплойтов iMessage с нулевым щелчком.

И эксплойт KISMET 2020 года, и эксплойт FORCEDENTRY 2021 года использовались правительством Бахрейна для взлома телефонов местных правозащитников, политических групп, политика и даже бахрейнских диссидентов, проживающих в Лондоне.

«По крайней мере четверо активистов были взломаны LULU, оператором Pegasus, который мы с большим доверием приписываем правительству Бахрейна, широко известному злоумышленнику, использующему шпионское ПО. Один из активистов был взломан в 2020 году через несколько часов после того, как они раскрылись во время в интервью, что их телефон был взломан с помощью Pegasus в 2019 году», - сказали авторы отчета.

«Двое из взломанных активистов сейчас проживают в Лондоне, и, по крайней мере, один был в Лондоне, когда они были взломаны. В нашем исследовании мы видели, как правительство Бахрейна шпионило только в Бахрейне и Катаре с использованием Pegasus; никогда - в Европе».

В сообщении отмечается, что активист в Лондоне мог быть взломан другим оператором Pegasus, который затем передал информацию правительству Бахрейна.

Citizen Lab координировала свои действия с Forbidden Stories - организацией, которая раскрывала работу NSO Group - и подтвердила, что по крайней мере пять устройств, взломанных правительством Бахрейна, включены в список потенциальных целей для клиентов NSO Group проекта Pegasus.

Бахрейн - это диктатура, которая давно подавляет инакомыслие и применяет драконовские меры для контроля публичных дискуссий в Интернете, шантажа оппонентов правительства, пыток активистов и совершения других нарушений прав человека.

В отчете отмечается, что другие западные технологические компании в прошлом сталкивались с негативной реакцией за то, что помогали правительству Бахрейна проводить цензуру в Интернете, срывать протесты и контролировать оппонентов как внутри Бахрейна, так и за пределами страны.

Канадская компания Netsweeper используется Бахрейном для блокировки многих веб-сайтов для граждан Бахрейна, а отдел киберпреступлений Министерства внутренних дел, наряду с другими правительственными структурами, закупил шпионское ПО у FinFisher, Verint Systems, Cellebrite, Hacking Team, Trovicor GmbH и NSO Group, по данным Отчет.

Исследователи Citizen Lab обнаружили, что правительство Бахрейна впервые купило шпионское ПО Pegasus в 2017 году и начало использовать его в Бахрейне и Катаре.

Организация увидела всплеск использования Pegasus в июле 2020 года и координировала свои действия с целевыми показателями правительства, чтобы проанализировать, как они были нацелены и как их телефоны были взломаны.

Муса Абд-Али и Юсуф Аль-Джамри, два бахрейнских активиста, живущие за пределами Бахрейна, согласились называть их имена в отчете, но другие, чьи телефоны были взломаны, хотели, чтобы их идентифицировали только организации, на которые они работали.

Абд-Али выделился в отчете, потому что ранее он подал в суд на FinFisher после того, как официальные лица Бахрейна использовали шпионское ПО для

взлома его компьютера в 2011 году. Его iPhone 8 был взломан где-то до сентября 2020 года.

В отчете поясняется, что чиновники пробовали несколько способов взломать телефоны, даже используя поддельные уведомления об отслеживании посылок DHL, которые Citizen Lab проследила до государственного оператора Бахрейна компании Pegasus. Иногда государственные служащие использовали эксплойт с нулевым щелчком, а в других случаях требовалось одно или два щелчка по ссылке, чтобы заразить устройство шпионским ПО.

«Мы отметили, что эти три домена были размещены у поставщиков общего веб-хостинга. Другими словами, IP-адреса, на которые они указывали, имели десятки других безобидных доменов, также указывающих на них. В предыдущих итерациях инфраструктуры Pegasus NSO Group указывалось каждое доменное имя на отдельный IP-адрес», - обнаружили исследователи.

Правительство предпринимало крайние меры, чтобы ограничить инакомыслие и уменьшить влияние активистов или лидеров протестов на протяжении десятилетий, но в последние годы усилия приняли технологический поворот, особенно после того, как протесты арабской весны начались примерно в 2010 году. Правительство жестоко подавило зарождающееся протестное движение в 2011 году были арестованы и подвергнуты пыткам сотни бахрейнцев.

Citizen Lab в течение многих лет отслеживает использование правительством шпионского ПО, отслеживая использование ими устройств ProxySG и PacketShaper, а также технологии интернет-фильтрации, разработанной Netsweeper, Inc.

По данным Bloomberg, в 2011 году правительство купило шпионские инструменты у бывшего филиала Nokia Siemens Networks Trovicor GmbH в 2011 году.

В одном примечательном случае правительство использовало шпионское ПО от FinFisher, британо-немецкой компании, чтобы шантажировать известного бахрейнского юриста. Правительственные чиновники взломали его компьютер, а затем отправили ему компакт-диск, угрожая выпустить интимное видео с ним и его женой, если он не перестанет защищать правозащитников. Видео было получено с помощью скрытой камеры, которая была тайно установлена в его доме.

Правительство в конечном итоге опубликовало видео для общественности после того, как адвокат отказался отступить.

Члены правительства также были обвинены в использовании других инструментов для деанонимизации псевдонимных аккаунтов Twitter, критикующих правительство.

Исследователи, составившие отчет, заявили, что он показывает, что неоднократные заявления NSO Group о невиновности и правозащитной деятельности противоречат реальности того, что их инструменты используются диктаторскими режимами.

"Несмотря на то, что на протяжении пяти лет причастность к нарушениям прав человека, NSO Group регулярно заявляет, что они на самом деле привержены защите прав человека. Однако это предполагаемое беспокойство опровергается растущим количеством свидетельств того, что ее шпионское ПО используется

авторитарные режимы против правозащитников, журналистов и других членов гражданского общества», - говорится в отчете.

«Хотя NSO Group регулярно пытается дискредитировать сообщения о злоупотреблениях, в их список клиентов входит множество заведомо злоупотребляющих технологиями наблюдения. Продажа Pegasus Бахрейну является особенно вопиющей, учитывая, что существуют значительные, давние и задокументированные доказательства серийного злоупотребления системой наблюдения Бахрейном. продукты, включая Trovicor, FinFisher, Cellebrite, а теперь и NSO Group».

Исследователи назвали злоупотребление шпионским ПО правительством Бахрейна «предсказуемым» и заявили, что это была «грубая халатность во имя прибыли» со стороны NSO Group, которая продала инструмент правительству Бахрейна с репутацией в области прав человека.

Хотя в отчете говорится, что жертвы взлома, возможно, смогли защитить свои устройства, отключив iMessage и FaceTime, в нем отмечается, что NSO Group нашла другие способы доставки вредоносных программ через другие приложения для обмена сообщениями, такие как WhatsApp.

Эксперты, такие как защитник конфиденциальности Comparitech Пол Бишофф, заявили, что отчет является еще одним доказательством того, что вредоносное ПО NSO Group не используется на законных основаниях.

«У этих властей не было бы таких шпионских возможностей без NSO Group», - сказал Бишофф ZDNet.

«Мы должны немедленно объявить международный мораторий на частную продажу шпионского ПО». ***(Jonathan Greig. NSO Group facing renewed backlash after helping repressive Bahraini Government hack iPhones of politicians, activists // ZDNet (https://www.zdnet.com/article/nso-group-facing-renewed-backlash-after-helping-repressive-bahraini-government-hack-blackmail-activists/). 25.08.2021).***

***

**«Официальный представитель японского производителя электронных компонентов Murata принес извинения за утечку в июне тысяч файлов, содержащих информацию о банковских счетах сотрудников и деловых партнеров компании.**

Норио Накадзима, генеральный директор Murata Manufacturing, опубликовал заявление с извинениями за инцидент 28 июня, когда субподрядчик загрузил файл данных управления проектом, содержащий 72 460 единиц информации.

Более 30 000 документов содержали информацию о деловых партнерах, такую как название компании, адрес, связанные имена, номера телефонов, адреса электронной почты и номера банковских счетов. Компании базируются в Японии, Китае, Филиппинах, Малайзии, Сингапуре, США и ЕС, но предприятиями «информация о клиентах распространяется только на Китай и Филиппины».

Также в утечку попало более 41 000 документов о сотрудниках, содержащих имена, адреса и номера банковских счетов. Сотрудники базировались в офисах компании в Японии, Китае, Филиппинах, Сингапуре, США и ЕС.

«20 июля 2021 года было подтверждено, что сотрудник без разрешения загрузил данные управления проектом, включая информацию о нашем деловом партнере и личную информацию, на рабочий компьютер и загрузил их в личный аккаунт внешнего облачного сервиса в Китае», - сказал Накадзима. в заявлении, добавив, что есть доказательства того, что никто, кроме субподрядчика, не имел доступа к данным.

«Кроме того, мы получили отчеты по результатам опроса внешних поставщиков облачных услуг, подтверждающие, что полученная информация никогда не копировалась и не загружалась третьими лицами. Загруженные данные уже были удалены с корпоративного ПК и внешнего облачного хранилища. по этому поводу не было подтверждено ни вирусного заражения, ни кибератак».

Накадзима продолжает объяснять, что неназванный субподрядчик участвовал в проекте обновления системы бухгалтерского учета компании.

Уведомление включало временную шкалу, в которой отслеживался инцидент с момента его возникновения 28 июня до его проверки в августе. Через два дня после того, как субподрядчик загрузил файлы, компания получила предупреждение, и к 4 июля их служба безопасности подтвердила, что произошло.

Компания заявила, что 8 июля взяла интервью у субподрядчика, который признался, что загружал информацию, а затем загружал ее в учетную запись частного облака.

«В тот же день загруженные данные были удалены под надзором субподрядчика», - сказал Накадзима.

К августу компания внутренне подтвердила то, что произошло, и попросила стороннюю охранную фирму также изучить ситуацию.

Японское информационное агентство ITMedia поговорило с субподрядчиком, который сказал: «Я загружал свое ноу-хау в персональное облако и систематизировал его, чтобы изучить проектирование системы и т.д. Оно оказалось конфиденциальной информацией о клиентах».

В японском блоге подтверждено, что субподрядчиком был инженер IBM Dalian Global Delivery, субподрядчика IBM China. Проект обновления системы бухгалтерского учета Мураты был передан на аутсорсинг IBM Japan, которая передала его на субподряд IBM China. Система используется для оплаты как сотрудников, так и партнеров.

Мурата сообщил ITMedia, что рассматривает возможность расторжения контракта и потенциально требует возмещения убытков.

Murata доминирует в исследованиях, производстве и продаже электронных устройств из высококачественной керамики. В компании работает более 70 000 сотрудников, и в этом году она планирует заработать более 2 миллиардов долларов». ***(Jonathan Greig. Japanese manufacturer Murata apologizes for data breach // ZDNet (https://www.zdnet.com/article/japanese-electronic-components-manufacturer-murata-apologizes-for-breach-of-employee-and-customer-data/). 12.08.2021).***

***

**«Risk Based Security выпустила два новых отчета, охватывающих утечки данных и уязвимости в первой половине 2021 года, обнаружив, что общее количество заявленных нарушений снизилось, но увеличилось количество раскрытых уязвимостей.**

В отчете компании о нарушениях данных было обнаружено, что за первые шесть месяцев 2021 года было зафиксировано 1767 публичных нарушений, что на 24% меньше по сравнению с тем же периодом прошлого года.

Количество заявленных нарушений выросло в США на 1,5%, при этом с начала года было обнаружено 18,8 миллиарда записей, что на 32% меньше, чем 27,8 миллиарда записей, утечка которых произошла в первой половине 2020 года.

Инга Годдин, исполнительный вице-президент Risk Based Security, сказала, что методы, используемые злоумышленниками для монетизации своих усилий, стали более разнообразными, и в то же время предотвращаемые ошибки опережают хакеров, когда дело доходит до объема раскрываемых данных.

«Объем скомпрометированных данных остается неизменно высоким, и, поскольку еще одно серьезное нарушение во втором квартале еще не подтверждено, возможно, что в ближайшем будущем это число превысит 19 миллиардов», - сказал Годдин.

Однако, как отмечается в отчете, цифры немного вводят в заблуждение, поскольку на нарушение торгового сервиса Forex FBS Markets приходится около 85% всех записей, открытых до 30 июня.

Исследователи добавили, что 352 утечки данных были связаны с атакой программы-вымогателя.

Количество просочившихся адресов электронной почты стабильно составляло 40% от всех утечек, в то время как пароли просочились в 33% взломов. На данный момент наибольшее количество нарушений в 2021 году было зафиксировано в организациях здравоохранения - 238. Финансовые и страховые компании пострадали от 194 нарушений, в то время как в обрабатывающей промышленности - 169, а в образовательных учреждениях - 138.». ***(Jonathan Greig. More than 12,500 vulnerabilities disclosed in first half of 2021: Risk Based Security // ZDNet (https://www.zdnet.com/article/more-than-12500-vulnerabilities-disclosed-in-first-half-of-2021-risk-based-security/). 05.08.2021).***

***

**«С годами кибератаки и утечки данных стали одними из самых больших рисков в бизнес-секторе, ставя под угрозу конфиденциальные данные и нанося серьезный финансовый удар компаниям и организациям по всему миру.**

Согласно данным, представленным BuyShares.co.uk, более 40 процентов компаний чувствуют угрозу киберинцидентов и считают их наиболее опасными для бизнеса в 2021 году.

Прерывание бизнеса, пандемия и киберинциденты - три основных риска для бизнеса

Глобальная озабоченность по поводу киберпреступности, сбоев ИТ и утечки данных растет уже много лет. До пандемии киберинциденты были бизнес-риском

номер один во всем мире, заставляя компании по всему миру тратить миллиарды на продукты и услуги кибербезопасности.

Хотя киберинциденты по-прежнему являются одной из трех основных проблем для компаний и организаций, COVID-19 действительно повлиял на рейтинг самых больших рисков в бизнес-секторе.

Согласно исследованию Allianz Risk Barometer, перебои в ведении бизнеса занимают первое место в диаграммах как ведущий бизнес-риск в 2021 году. Статистика показывает, что этот риск семь раз занимал первое место за последнее десятилетие. Однако пандемия еще больше повысила осведомленность о прерывании бизнеса. Это неудивительно, учитывая, что 94% опрошенных компаний сообщили о сбоях в цепочке поставок, связанных с COVID-19 в прошлом году.

Вспышка пандемии поднялась на 15 пунктов и стала вторым по значимости бизнес-риском, при этом 40% компаний обеспокоены такой неопределенностью.

Киберинциденты считаются третьим по величине бизнес-риском в мире, в первую очередь из-за подпитываемого пандемией стремления к цифровизации. Согласно исследованию, предприятия во всем мире признают киберпреступность более серьезной проблемой, чем потеря репутации, макроэкономические изменения и политические риски.

Развитие рынка, включая волатильность или колебания рынка, усиление конкуренции, появление новых участников, а также слияния и поглощения, оценивается как четвертый по величине риск в бизнес-секторе в этом году с долей 19% среди респондентов.

Изменения в законодательстве и регулировании, такие как торговые войны и тарифы, экономические санкции, Brexit и распад еврозоны, замыкают пятерку лидеров с долей 19% соответственно.

Мировые расходы на продукты и услуги кибербезопасности в 2021 году составят 131,8 миллиарда долларов

Компании и организации по всему миру ежегодно теряют миллиарды из-за киберпреступности. Хотя большинство из них значительно увеличили свои бюджеты на кибербезопасность, утечки данных, фишинг, атаки программ-вымогателей или кибершпионаж по-прежнему представляют собой огромную угрозу для их операций.

В прошлом году потребители, предприятия и организации во всем мире потратили более 120 миллиардов долларов на продукты и услуги кибербезопасности, что на 87 миллиардов долларов больше, чем до пандемии. Опрос Statista показал, что этот показатель вырастет на 10% г / г до 131,8 млрд долларов в 2021 году.

Услуги кибербезопасности, такие как анализ рисков данных, маскирование данных и обнаружение уязвимостей, являются крупнейшим и наиболее быстрорастущим сектором всего рынка, который, как ожидается, достигнет в этом году 61,4 миллиарда долларов.

Программное и аппаратное обеспечение для кибербезопасности принесло соответственно 44,3 млрд долларов и 260 млрд долларов дохода. К 2025 году глобальные доходы от кибербезопасности, по прогнозам, достигнут 210

миллиардов долларов». ***(Mike Brennan. 40 Percent Of Businesses Feel Threatened By Cyber Incidents in 2021 // MITechNews.com (https://mitechnews.com/cyber-defense/40-percent-of-businesses-feel-threatened-by-cyber-incidents-in-2021/). 28.08.2021).***

***

**«20 августа 2021 года 30-я сессия Постоянного комитета 13-го Всекитайского собрания народных представителей (ВНК) приняла новый Закон Китая о защите личной информации (PIPL) 1 Китая, который вступит в силу 1 ноября 2021 года. впервые исчерпывающий набор правил, касающихся сбора, обработки и защиты персональных данных.**

PIPL включает в себя определенные общепризнанные принципы защиты данных, такие как требование, чтобы обработчики собирали личную информацию только в минимально необходимом объеме и получали информированное согласие от отдельных лиц до сбора или передачи личной информации. Кроме того, PIPL обеспечивает усиленную защиту «конфиденциальной личной информации», которая включает информацию, относящуюся к биометрии, религиозным убеждениям, медицине и здоровью, финансовым счетам и отслеживанию местоположения. Существуют также более строгие требования, такие как более полные системы соответствия и повышенная прозрачность, которые применяются к обработчикам, которые предоставляют важные услуги интернет-платформы, имеют «большое количество пользователей» и осуществляют «сложные» бизнес-операции.

Трансграничная передача личной информации разрешена только в соответствии с PIPL, если выполняется одно из следующих условий: (i) прохождение оценки безопасности национальным органом власти в области киберпространства; (ii) получение аккредитации от организаций, назначенных агентством; или (iii) заключение соглашений стандартной формы, утвержденных соответствующими агентствами, с зарубежным получателем. Конкретное согласие также должно быть получено от отдельных лиц до любой трансграничной передачи их личной информации.

PIPL применяется ко всей деятельности по обработке информации в Китае, независимо от того, является ли обработчик иностранной организацией или принадлежит ли личная информация иностранным лицам. Это также относится к деятельности за пределами Китая, связанной с личной информацией лиц, находящихся в Китае, где целью такой деятельности является предоставление продуктов или услуг этим лицам или когда поведение этих лиц анализируется или оценивается.

*Законодательная база*

В 2016 году Китай выпустил свой первый знаковый закон в области защиты данных и кибербезопасности - Закон КНР о кибербезопасности (CSL) 2, который вступил в силу 1 июня 2017 года и направлен на регулирование деятельности, касающейся строительства, эксплуатации и технического обслуживания. и использование сетей, а также ограничения надзора и управления на передачу личной информации и бизнес-данных за границу. С тех пор были выпущены или

разрабатываются десятки нормативных актов, руководств и национальных стандартов в области кибербезопасности. В 2020 году Китай представил еще два важных законодательных предложения в области защиты данных: первые проекты Закона КНР о безопасности данных и PIPL. Окончательный Закон КНР о безопасности данных (DSL)3 был принят на 29-м заседании Постоянного комитета ВСНП 10 июня 2021 года и вступит в силу с 1 сентября 2021 года.

В то время как DSL нацелен на широкое регулирование безопасности данных с акцентом на защиту национальной безопасности, PIPL фокусируется на защите личной информации. Перед принятием окончательной версии PIPL два проекта были выпущены для публичных консультаций в октябре 2020 года и апреле 2021 года. Выпуск PIPL завершает трифект основополагающего режима управления данными в Китае.

*Ключевые положения*

PIPL состоит из восьми глав и 74 статей. Основываясь на принципах CSL и DSL, PIPL дополнительно уточняет принципы и правила обработки личной информации, которым необходимо следовать при защите личной информации, уточняет границы прав и обязанностей в деятельности по обработке личной информации, а также улучшает рабочие системы и механизмы защиты персональной информации.

*Основные принципы*

PIPL предусматривает, что при обработке личной информации необходимо соблюдать следующие основные принципы:

Принцип законности и добросовестности. Личная информация должна обрабатываться в соответствии с принципами законности, целесообразности, необходимости и добросовестности. PIPL подчеркивает, что личная информация не должна обрабатываться с использованием вводящих в заблуждение, мошеннических или принудительных методов.

Ясная и разумная цель. Обработка личной информации должна иметь четкую и разумную цель и быть напрямую связана с целью обработки. При обработке личной информации следует использовать метод, который в наименьшей степени влияет на личные права. Сбор личной информации должен быть ограничен минимумом, необходимым для указанной цели, и чрезмерный сбор личной информации не допускается.

Открытость и прозрачность. Обработчики должны четко раскрывать правила обработки личной информации, цель обработки, метод обработки и объем обработки.

Гарантия качества. Качество личной информации должно сохраняться при обработке личной информации, чтобы избежать любого негативного воздействия на личные права и интересы из-за неточности или неполноты личной информации. Кроме того, обработчики несут ответственность за принятие мер по обеспечению безопасности личной информации.

Незаконность. Юридическим и физическим лицам запрещается незаконный сбор, использование, обработка и передача личных данных, а также незаконная продажа, предоставление или публикация личных данных. Обработка, угрожающая национальной безопасности и общественным интересам, запрещена.

*Экстерриториальное применение*

Статья 3 гласит, что PIPL применим ко всем операциям по обработке данных в Китае, независимо от того, является ли обработчик данных иностранным лицом или личная информация принадлежит иностранным лицам. Кроме того, PIPL опирается на экстерриториальные положения европейских законов о защите личной информации, заявляя, что закон также применяется к организациям, занимающимся любой деятельностью за пределами Китая, связанной с обработкой личной информации физических лиц внутри Китая, где целью деятельности является предоставлять продукт или услугу этим лицам, а также анализировать или оценивать поведение этих лиц. PIPL рассматривает процессоров, осуществляющих такую деятельность, как «иностранные обработчики личной информации.

*Разрешенные действия по обработке личной информации*

В статье 13 PIPL перечислено семь типов ситуаций, в которых разрешена обработка личной информации:

Информированное согласие было получено от человека.

Это необходимо для заключения или исполнения договоров, либо осуществления управления человеческими ресурсами в соответствии с трудовым законодательством и коллективными договорами, подписанными в соответствии с законодательством.

Это необходимо для выполнения установленных законом обязанностей или обязательств.

Это необходимо для реагирования на чрезвычайные ситуации в области общественного здравоохранения или для защиты здоровья или имущества в чрезвычайных ситуациях.

Разумная обработка личной информации для осуществления действий в общественных интересах, таких как освещение новостей и наблюдение за общественным мнением.

Разумная обработка личной информации, которая была обнародована физическим лицом или другими законными способами.

Иные обстоятельства, предусмотренные законами и административными постановлениями.

Статьи 14 и 15 PIPL определяют стандарты получения информированного согласия и отзыва согласия. Согласие должно быть дано добровольно и четко лицом, обладающим полным знанием дела, а обработчик личной информации обязан предоставить удобные средства для отзыва согласия. Статья 16 также предусматривает, что обработчики личной информации не должны отказывать в предоставлении продуктов или услуг на основании отсутствия согласия или отзыва согласия, за исключением случаев, когда такая личная информация необходима для предоставления продуктов или услуг.

Строгая защита конфиденциальной личной информации и личной информации несовершеннолетних

PIPL обеспечивает усиленную защиту «конфиденциальной личной информации», которая включает биометрические данные, религиозные убеждения, конкретные личности, медицинские и медицинские, финансовые счета, местонахождение и другую информацию, а также личную информацию

несовершеннолетних в возрасте до 14 лет. обработчики должны обрабатывать конфиденциальную личную информацию только тогда, когда у них есть конкретная цель и достаточная необходимость, и принимать строгие меры защиты, включая предварительную оценку воздействия и информирование людей о необходимости обработки и влиянии на личные права и интересы.

*Права и обязанности*

Права физических лиц. PIPL кодифицирует права физических лиц в деятельности по обработке личной информации, включая, среди прочего, право знать, право ограничивать или отклонять обработку личной информации другими лицами, право запрашивать и запрашивать копию личной информации у обработчиков, право на исправление неверной или неполной информации и право на удаление личной информации. Обработчики обязаны создать удобный механизм для физических лиц для реализации вышеуказанных прав.

Обязанности обработчиков персональных данных. Для обработчиков личной информации PIPL требует, чтобы они сформулировали «внутренние системы управления и рабочие процедуры» (которые не определены), приняли соответствующие технические меры безопасности, назначили ответственных лиц для надзора за действиями по обработке личной информации, проводили регулярные аудиты соответствия в отношении действий, связанных с личной информацией, и проводить предварительную оценку воздействия на защиту личной информации для операций обработки с высоким риском, например, связанных с конфиденциальной личной информацией и передачей личной информации за границу. В случае утечки данных обработчик обязан незамедлительно принять меры по исправлению положения и уведомить соответствующие государственные органы и затронутых лиц.

Особые обязательства. Кроме того, PIPL налагает особые обязательства на обработчиков личной информации, которые предоставляют важные услуги интернет-платформы, имеют «большое количество пользователей» и осуществляют «сложные» бизнес-операции. Эти особые обязательства включают: (i) создание всеобъемлющей системы соответствия, предназначенной для защиты личной информации и контролируемой независимой организацией, состоящей в основном из внешних членов; (ii) формулирование правил платформы, в которых четко излагаются стандарты и обязательства по защите продуктов или услуг, предлагаемых на платформе; (iii) прекращение предоставления услуг поставщикам продуктов или услуг на платформе, которые имеют дело с личной информацией в серьезное нарушение закона; и (iv) регулярная публикация отчетов о социальной ответственности за защиту личной информации.

*Требования к автоматизированному принятию решений*

В ответ на конкретные проблемы конфиденциальности, вызванные внедрением искусственного интеллекта и других автоматизированных технологий, статья 24 Закона о защите личных сведений гласит, что обработчики личной информации, использующие личную информацию для принятия автоматизированных решений, должны обеспечивать прозрачность принятия решений и справедливость. и беспристрастность результатов, а также не должны навязывать необоснованное дифференцированное отношение к отдельным лицам с

точки зрения цен транзакций и других условий транзакций. В то же время обработчики личной информации, которые используют автоматизированные методы принятия решений для передачи информации и прямого коммерческого маркетинга отдельным лицам, должны предоставлять варианты, не зависящие от их личных характеристик, или предоставлять людям удобные средства для отказа.

*Правовая основа трансграничной передачи личной информации*

Как правило, PIPL требует, чтобы обработчики личной информации принимали необходимые меры для обеспечения того, чтобы действия зарубежных получателей по обработке личной информации соответствовали стандартам защиты личной информации, изложенным в PIPL. Любая трансграничная передача личной информации разрешена в соответствии с PIPL только при выполнении одного из следующих условий: (i) прохождение оценки безопасности национальным органом власти в области киберпространства; (ii) получение аккредитации от организаций, назначенных агентством; (iii) заключение соглашений стандартной формы, утвержденных соответствующими агентствами, с зарубежным получателем; или (iv) любыми другими условиями, предусмотренными другим законодательством или нормативными актами, или условиями, которые время от времени устанавливаются соответствующими агентствами. Кроме того, PIPL требует, чтобы конкретное согласие было получено от отдельных лиц до передачи.

Помимо вышеуказанного общего требования, операторы инфраструктуры критической информации (CIIO) или обработчики личной информации, которые обрабатывают личную информацию в объеме, установленном национальным органом управления киберпространством, должны хранить личную информацию в Китае. Если необходимо предоставить такую информацию иностранному получателю, заявитель должен будет пройти оценку безопасности, организованную национальным органом власти в области киберпространства.

Помимо вышеперечисленных требований, мы также рекомендуем компаниям обращать внимание на любые отраслевые правила или инструкции, которые могут быть наложены соответствующими агентствами. Взяв в качестве примера автомобильную промышленность, в соответствии с Правилами управления безопасностью автомобильных данных (для пробной реализации), опубликованными в соответствии с CSL, DSL и другими соответствующими законами 4, вступающими в силу с 1 октября 2021 года, автомобильные процессоры данных, которые хранят важные данные (в том числе личная информация с участием более 100000 субъектов личной информации) может передавать данные за границу только в случае необходимости и только после прохождения оценки безопасности исходящих данных, организованной национальным органом в области киберпространства.

В соответствии со статьей 41 Закона о гражданстве и защите частной жизни (PIPL) частным лицам и организациям не разрешается предоставлять личные данные, хранящиеся в Китае, иностранным правоохранительным органам без предварительного разрешения соответствующих органов в Китае. Неясно, как определяются данные «хранящиеся в Китае» и как организация, занимающаяся «обработкой данных», может подать заявку на разрешение в настоящее время;

Практическое исполнение такого положения, вероятно, будет зависеть от более подробных правил или мер, которые будут опубликованы соответствующими регулирующими органами.

*Юридическая ответственность*

Как поясняется ниже, компании, нарушающие положения PIPL, несут потенциальную административную, гражданско-правовую и уголовную ответственность.

Административные штрафы. В случае нарушения PIPL органы по защите личной информации могут издать приказ об исправлении или предупреждении и конфисковать любые незаконные доходы. Соответствующие приложения могут быть приостановлены или прекращены. Компании и их ответственные сотрудники, отказывающиеся устранять нарушения, могут быть подвергнуты дополнительным штрафам. Серьезные нарушения могут быть наказаны приостановкой деловых операций, аннулированием бизнес-сертификата и наложением штрафа в размере до 50 000 000 юаней или 5% от годового оборота. Ответственные должностные лица могут быть подвергнуты штрафам и лишены права занимать должности, связанные с управлением или защитой личной информации, в других компаниях. Нарушения PIPL также могут быть объявлены общественности и включены в социальные кредитные отчеты соответствующих компаний в соответствии с соответствующими нормативными актами.

Гражданско-правовая ответственность. Если обработка личной информации с нарушением прав человека причиняет вред, и обработчик личной информации не может доказать, что он не виноват, обработчик несет ответственность за убытки и другие гражданские обязательства. Уполномоченные организации потребителей могут также подавать иски от имени группы лиц, если пострадало большое количество людей.

Уголовная ответственность. Нарушения PIPL, квалифицируемые как уголовные преступления, могут повлечь за собой уголовную ответственность.

*Ключевые последствия*

PIPL разъясняет принципы, которым необходимо следовать при обработке личной информации, улучшает правила обработки личной информации, защищает права отдельных лиц при обработке личной информации, усиливает обязанности обработчиков личной информации и устанавливает строгую юридическую ответственность.

Обнародование и внедрение DSL, PIPL и соответствующих вспомогательных нормативных актов окажет огромное влияние на предприятия, ведущие внутренние и трансграничные операции, в контексте все более жесткой нормативной среды Китая в отношении личной информации и других данных». ***(The New PRC Personal Information Protection Law // AKIN GUMP STRAUSS HAUER & FELD LLP (https://www.akingump.com/en/news-insights/the-new-prc-personal-information-protection-law.html). 27.08.2021).***

***

**«SEC недавно объявила о мировом соглашении с Pearson plc, по которому компания согласилась выплатить 1 миллион долларов для**

**урегулирования обвинений в том, что она ввела инвесторов в заблуждение относительно киберинцидента 2018 года.** Согласно приказу, Пирсон в своем полугодовом отчете за июль 2019 года сделал вводящие в заблуждение заявления и упущения в отношении утечки данных в 2018 году, связанной с кражей данных учащихся и учетных данных администратора.

Pearson - британская образовательная и издательская компания, которая предоставляет услуги как школам K-12, так и университетам. В рамках предоставления услуг школьным администраторам предоставляются учетные данные для входа в систему, и 13000 из этих учетных данных, а также адреса электронной почты учащихся и даты рождения были затронуты в результате киберинцидента. Пирсон узнал об инциденте в марте 2019 года, а четыре месяца спустя, после расследования, уведомил пострадавших. Руководство Pearson решило, что не нужно делать никаких публичных заявлений, и на следующий день после заседания совета директоров (и через семь дней после того, как уведомление было отправлено пострадавшим лицам), компания выпустила свой полугодовой отчет (форма 6-K), в котором не упоминалось киберинцидент, вместо этого ссылаясь на инциденты, связанные с конфиденциальностью данных, как на гипотетический риск, что отражает формулировки из прошлых отчетов. После выдачи своего 6-K,

Комиссия по ценным бумагам и биржам процитировала Пирсона с нарушениями Закона о ценных бумагах и Закона о биржах за отсутствие соответствующих процессов и процедур при составлении проекта раскрытия информации о факторах риска по форме 6-K, за вводящие в заблуждение и неточные детали в раскрытии информации, а также за пропуск ключевых деталей о инцидент (например, объем и тип затронутых данных) в своем заявлении для СМИ. Хотя компания Pearson не признала правонарушений, она согласилась выплатить штраф в размере 1 млн долларов в рамках урегулирования спора.

Применение на практике. Этот случай подчеркивает важность надлежащего анализа инцидентов и оценки их существенности, чтобы определить, нужно ли их раскрывать в документации компании. Компаниям будет полезно пересмотреть свои средства контроля и процедуры, в том числе то, как об инцидентах сообщается руководству, какие процессы существуют в управлении для анализа существенности и как раскрываемая информация может быть быстро и эффективно изменена или обновлена в результате инцидента». ***(Liisa Thomas, Julia Kadish & Kari Rollins. SEC Fine Highlights Importance of Cybersecurity Disclosures // Sheppard Mullin (https://www.eyeonprivacy.com/2021/08/sec-fine-cybersecurity-disclosures/#page=1). 25.08.2021).***

***

**«Исследования опубликованы этим летом в Ponemon Institute и авторами и анализировали с помощью IBM Security, который объединил результаты по 17 отраслях, в том числе 537 организаций из 17 стран и регионов, отметил, что глобальная средняя совокупная стоимость утечки данных составляет 4240000 $.** В отчете сделан вывод, что отраслями с самыми высокими средними издержками от утечки данных являются здравоохранение,

финансовые услуги, фармацевтика, технологии и энергетика. За последние 11 лет подряд медицинские организации столкнулись с самой высокой средней стоимостью утечки данных. Только с 2020 по 2021 год эти затраты увеличились на 29,5 процента.

В свете этой статистики, наряду с другими потенциальными стратегиями снижения рисков, связанных с кибератаками, организациям следует рассмотреть возможность усиления своих программ информационной безопасности, поддержания киберстрахования и внедрения передовых методов, направленных на снижение риска атак программ-вымогателей.

По мере роста кибератак страховщики сосредотачиваются на рискованных секторах

Страховщики в течение некоторого времени отмечали, что риск злонамеренной киберактивности, направленной на федеральное правительство, предприятия США и критически важную инфраструктуру, растет. В недавнем отчете Счетной палаты правительства за 2021 год, опубликованном в соответствии с положениями Закона о государственной обороне на 2021 финансовый год, подтверждается необходимость устойчивого рынка страхования на фоне резкого роста кибератак за последние несколько лет.

По мере продолжения проблем страховщикам и политикам рекомендуется оценивать свои кибер-меры контроля, особенно в секторах с высоким уровнем риска. В частности, сектор здравоохранения ищет способы защитить себя от роста числа атак.

*Растущий спрос на полисы киберстрахования*

Среди других выводов в отчете GAO отмечен растущий спрос на полисы киберстрахования, который согласуется с ростом цен на страхование и более частыми и серьезными кибератаками. Темпы использования киберстрахования выросли в период с 2016 по 2020 годы, причем самые высокие показатели были отмечены в отраслях с высоким уровнем риска, в том числе в здравоохранении и образовании. Страховые взносы, которые могут варьироваться в зависимости от различных факторов, включая отрасль, размер компании и кибернетический контроль, также увеличились.

В отчете также указано, что страховщики снизили лимиты покрытия киберстрахования для более рискованных секторов промышленности и что страховщики склоняются к добавлению конкретных ограничений на покрытие программ-вымогателей. Согласно отчету, проблемы, с которыми сталкиваются страховщики и страхователи, включают ограниченную доступность исторических данных об убытках и кибер-событиях, риск совокупных убытков от кибератак и ограниченную осведомленность о киберрисках и киберстраховании, необходимом для снижения этих рисков.

*Киберриск для здравоохранения остается высоким*

Анализ и соответствующая тенденция в отношении лимитов киберстрахования появляются по мере того, как количество инцидентов с программами-вымогателями увеличилось за последний год. В конце мая агентство Moody's Investor Services опубликовало отчет, в котором было установлено, что киберриск для отрасли здравоохранения остается высоким, отмечая, что растущая

зависимость от электронных записей, подключенных устройств и цифровых технологий здравоохранения может сделать такие учреждения многочисленными целями конфиденциальных данных и уязвимыми для атак.

Количество инцидентов, связанных с программами-вымогателями, в медицинских и образовательных учреждениях неуклонно растет с 2019 года и не показывает никаких признаков снижения. Этим летом ФБР выпустило флеш-бюллетень, предупреждающий об атаках с использованием программы-вымогателя Conti. Conti является человеком управлением «двойного вымогательство» вымогатели, что ворует и угрожает раскрыть информацию, а также шифровать его так, чтобы его владелец не может получить к нему доступ. Бюро заявило, что выявило по меньшей мере 16 таких атак Conti, нацеленных на системы здравоохранения США и службы быстрого реагирования. Бюллетень ФБР был обнародован Американской ассоциацией больниц, которая опубликовала предупреждение вместе с заявлением, в котором содержался призыв к скоординированной правительственной кампании по борьбе с организациями-вымогателями.

*Нет недостатка в хакерах*

Некоторые организации-вымогатели, такие как REvil и Avaddon, публично приняли правила, запрещающие их филиалам, использующим их программы-вымогатели, атаковать учреждения здравоохранения и образования. Конечно, такие обязательства сомнительны в свете сообщений о преступной деятельности групп и того факта, что виновные в этих нападениях, возможно, распались. Хотя злоумышленники, использующие программы-вымогатели, часто вновь появляются в новых группах, нет оснований полагать, что они будут придерживаться обещаний, данных их предыдущими организациями, ограничить масштабы своей деятельности. Более того, похоже, нет недостатка в конкурентах, желающих работать в этих секторах.

Выводы GAO и недавний всплеск кибератак и инцидентов с программами-вымогателями демонстрируют необходимость для держателей полисов киберстрахования повышать осведомленность о рисках, связанных с ними затратах и операционных последствиях кибератак, особенно в таких секторах с высоким уровнем риска, как здравоохранение и образование. Тенденции киберстрахования также подчеркивают необходимость для участников отрасли внедрять и укреплять киберконтроль и защиту.

*Федеральное правительство предлагает лучшие методы борьбы с атаками программ-вымогателей*

В июле 2021 года в рамках постоянного реагирования на растущую угрозу национальной безопасности, создаваемую атаками программ-вымогателей, министерство юстиции и внутренней безопасности в сотрудничестве с федеральными партнерами создало Stopransomware.gov, универсальный центр ресурсов программ-вымогателей, чтобы помочь частные и государственные организации снижают риск программ-вымогателей. На веб-сайте представлены советы и рекомендации по подготовке к атакам программ-вымогателей и борьбе с ними, а также ресурсы для сообщения об инцидентах.

Помимо других передовых методов предотвращения инцидентов, веб-сайт рекомендует организациям:

(1) ограничить права пользователей на установку и запуск программных приложений

(2) используйте сильные спам-фильтры, чтобы фишинговые письма не доходили до конечных пользователей.

(3) аутентифицировать входящую электронную почту, чтобы предотвратить подделку электронной почты и

(4) настроить брандмауэры для блокировки доступа к известным вредоносным IP-адресам.

На веб-сайте также есть контрольный список ответов на программы-вымогатели, предлагающий передовые методы обнаружения, анализа, локализации и искоренения инцидентов.

*Другие стратегии управления киберрисками*

Поскольку стоимость и изощренность кибератак продолжают расти, а предприятия продолжают искать способы оптимизации операций в ответ на развивающуюся пандемию COVID-19, организациям следует продолжать отслеживать тенденции кибератак и разрабатывать программы управления данными. Другие стратегии управления киберрисками включают анализ организационных средств контроля, разработку и улучшение планов реагирования на инциденты, проведение внутренней и внешней оценки безопасности и обучение сотрудников предотвращению инцидентов и реагированию на них.

Обзоры последних тенденций и статистические данные, предоставленные как государственными, так и частными ресурсами, подчеркивают необходимость для организаций, работающих в отраслях с высоким уровнем риска, не в последнюю очередь в сфере здравоохранения и образования, осознавать, что расходы на разработку программ информационной безопасности и высокие премии киберстрахования при сниженных лимитах могут быть часть текущих затрат на ведение бизнеса.

Постоянные продвинутые угрозы групп программ-вымогателей и других киберпреступников могут представлять серьезную угрозу для бизнеса. Инвестиции в кибербезопасность и киберстрахование имеют решающее значение для бизнеса и могут помочь им избежать гораздо более высоких расходов, которые они могут понести, если станут жертвами серьезной кибератаки». ***(Lori Marsh, Emily Maus, Anna Spencer. Cybersecurity considerations for executives and boards of directors: How recent cyberattack trends and developments inform strategies for reducing cyber-risk // DLA Piper (https://www.dlapiper.com/en/us/insights/publications/2021/08/cybersecurity-considerations-for-executives-and-boards-of-directors/). 23.08.2021).***

***

**«Требования к локализации данных во Вьетнаме содержатся в трех законодательных актах. Во-первых, Закон о кибербезопасности 2018, статья 26.3 об обеспечении информационной безопасности предусматривает, что «[предприятия], предоставляющие услуги в телекоммуникационных сетях**

**или Интернете, а также дополнительные услуги в киберпространстве во Вьетнаме, должны хранить такие данные [здесь] в течение периода, указанного в правительство.** Иностранные предприятия в рамках этой сферы также должны открыть филиал или представительство во Вьетнаме».

Сфера действия вышеуказанного положения широка и включает каждого поставщика любых услуг в киберпространстве, который обрабатывает персональные данные. Из этого правила нет исключений.

Во-вторых, статья 26 проекта указа о кибербезопасности предусматривает, что только иностранные поставщики предписанных услуг (служба доменных имен, электронная коммерция, онлайн-платежи, социальные сети и социальные связи) могут быть обязаны хранить данные и открывать филиал / представительство в Вьетнам.

Кроме того, это обязательство возникает только в том случае, если услуга была использована с нарушением Закона о кибербезопасности; о таком нарушении (нарушениях) было сообщено поставщику услуг властями; и поставщик услуг не выполнил такие инструкции.

В отличие от упреждающего подхода Закона о кибербезопасности, указ о кибербезопасности принимает ответный подход. Не все офшорные поставщики услуг обязаны локализовать, только те, кто был уведомлен о нарушении и не соблюдает их. Кроме того, хотя Закон о кибербезопасности налагает обязательство по локализации на всех поставщиков онлайн-услуг, в соответствии с указом о кибербезопасности только иностранные поставщики перечисленных услуг могут иметь такое обязательство.

Согласно вьетнамскому законодательству, если есть противоречащие положения, закон имеет преимущественную силу, поэтому интересно посмотреть, как окончательная версия указа решит этот вопрос.

Последним законодательным актом, касающимся локализации данных, является проект постановления о защите персональных данных (PDPD). В соответствии со статьей 21.1 предприятие может передавать данные за границу только в том случае, если оно соответствует всем установленным требованиям, включая хранение исходных данных во Вьетнаме. Однако, если применяются исключения, указанные в параграфе 3, предприятие освобождается от таких требований.

Неясно, должно ли быть удовлетворено только одно или все четыре требования в соответствии с параграфом 3, чтобы предприятие могло пользоваться освобождением, и даже в этом случае, освобождается ли предприятие от всех или только от одного из таких обязательств.

Из этого анализа можно сделать четыре замечания. Во-первых, хотя указ о кибербезопасности, Закон о кибербезопасности и PDPD касаются «личных данных», их подходы существенно различаются. Во-вторых, «хранение данных» может быть истолковано как включающее хранение в центрах обработки во Вьетнаме или хранение в системах сторонних поставщиков услуг хранения. И наконец, что не менее важно, во Вьетнаме в отношении определенных видов деловой деятельности, особенно новых, закон может быть истолкован как разрешающий только действия, которые «одобрены», «явно разрешены» или

«лицензированы». ***(Manh-Hung Tran. Vietnam: Data Localization Requirements // Baker McKenzie (https://viewpoints.bakermckenzie.com/post/102h4y0/vietnam-data-localization-requirements). 16.08.2021).***

***

**«Microsoft предупредила, что отслеживает широко распространенную кампанию фишинга учетных данных, основанную на открытых ссылках перенаправителя, одновременно предполагая, что она может защитить от таких схем.**

«Злоумышленники комбинируют эти ссылки с приманками социальной инженерии, которые выдают себя за хорошо известные инструменты и сервисы для повышения производительности, чтобы побудить пользователей щелкнуть мышью», - говорится в сообщении в блоге компании Microsoft 365 Defender Threat Intelligence Team в четверг.

«Это приводит к ряду перенаправлений, включая страницу проверки CAPTCHA, которая добавляет ощущение легитимности и пытается обойти некоторые автоматизированные системы анализа - перед тем, как перенаправить пользователя на поддельную страницу входа».

Открытая переадресация, когда веб - приложение позволяет HTTP - параметр, чтобы содержать компоненты, поставляемого пользователь URL, который вызывает запрос HTTP, чтобы быть перенаправлен на который ссылается ресурс.

Microsoft заявляет, что открытые перенаправления имеют законное использование, указывая на то, как продажи и маркетинговые кампании полагаются на них, чтобы направлять клиентов на определенные целевые страницы и собирать веб-метрики. Но открытыми перенаправлениями также часто злоупотребляют.

По словам компании, сообщения в этой конкретной кампании, как правило, следуют общему шаблону. Они используют несколько общих строк темы, отформатированных таким образом:

[Имя пользователя получателя] 1 новое уведомление

Сообщить о статусе для [Имя домена получателя] в [Дата и время]

Встреча Zoom для [доменное имя получателя] в [Дата и время]

Статус для [Имя домена получателя] на [Дата и время]

Уведомление о пароле для [доменное имя получателя] в [Дата и время]

[Имя пользователя получателя] eNotification

После открытия сообщения представляют собой кнопку для отображения предполагаемого сообщения с уведомлением. Кнопка связана с доверенным доменом, к которому добавлены параметры перенаправления таким образом, чтобы она выглядела убедительно на случайном уровне изучения, например, краткое представление полного URL-адреса при наведении указателя мыши на кнопку.

Любой, кто понимает, как работают URL-адреса и добавленные параметры, вероятно, не будет обманут, но менее сообразительные пользователи вполне могут увидеть исходный доверенный URL-адрес и предположить, что все в порядке, не заботясь обо всех данных параметров, добавленных в запрос.

Чтобы еще больше передать иллюзию безопасности и законности, перенаправление переносит жертву на страницу Google reCAPTCHA, которая, по предположениям Microsoft, также служит для срыва динамического сканирования и проверки содержимого фишинг-страницы в конце перенаправления.

Тем, кто успешно решит головоломку CAPTCHA и продемонстрирует фишерам, что они являются законными знаками, будет показан веб-сайт, который выдает себя за известный, законный сервис, такой как Microsoft Office 365. И мошеннический сайт загружается с адресом электронной почты цели - передается на фишинговую страницу в качестве параметра в фишинговом URL-адресе - и часто с корпоративными логотипами или другим брендом, чтобы страница входа выглядела так, как будто она реализует обычное поведение единого входа.

Если жертва вводит пароль, это еще не конец. Затем страница обновляется с сообщением об ошибке, в котором объявляется, что время сеанса истекло, и предлагается посетителю снова ввести пароль - практика проверки данных, мало чем отличающаяся от ритуала двойного согласия, используемого службами рассылки рассылки по электронной почте для обеспечения соблюдения законов о спаме.

За то, что они так любезно подтверждали свои пароли, жертвы фишинга перенаправляются на законный веб-сайт безопасности Sophos, который ложно указывает на то, что сообщение электронной почты, которое они были уведомлены о получении, было выпущено.

Microsoft заявляет, что обнаружила по меньшей мере 350 уникальных фишинговых доменов, задействованных в этой кампании. Схема, похоже, может выйти далеко за рамки этого - URL-адреса перенаправления поступают из алгоритма генерации доменов, который создает фишинговые домены на лету по мере необходимости.

Как ни изощренно эта схема может показаться, Microsoft настаивает на том, что ее Защитник для программного обеспечения Office 365 предлагает адекватную защиту, поскольку включает встроенную песочницу, которая проверяет все ссылки перенаправления. Defender якобы делает это «даже в тех случаях, когда целевая страница требует проверки CAPTCHA», что не вызывает особого доверия к CAPTCHA как средству различения между человеческим и автоматическим взаимодействием.

В таком случае, почему Microsoft бьет тревогу? По словам Редмонда, 91% всех кибератак исходят от электронной почты. Ясно, что фишинг по-прежнему работает, как и продажа безопасности, указывая на это». ***(Thomas Claburn. Microsoft warns of widespread open redirection phishing attack – which Defender can block, coincidentally // The Register (https://www.theregister.com/2021/08/27/microsoft_phishing_defender/). 27.08.2021).***

***

**«За последние несколько дней было много сообщений о компрометации данных клиентов T-Mobile, с утверждениями, что компрометация затронула до 100 миллионов клиентов.** Федеральная комиссия связи вчера подтвердила, что

расследует инцидент. 17 августа T-Mobile заранее выпустила пресс-релиз, чтобы прояснить и исправить факты.

Согласно пресс-релизу, T-Mobile «в срочном порядке расследует весьма изощренную кибератаку» и теперь предоставляет подробности атаки. Вещество цитируется ниже из пресс-релиза:

«В конце прошлой недели мы были проинформированы о заявлениях на онлайн-форуме о том, что злоумышленник скомпрометировал системы T-Mobile. Мы немедленно начали исчерпывающее расследование этих утверждений и привлекли ведущих мировых экспертов по кибербезопасности, чтобы помочь с нашей оценкой.

Затем мы обнаружили и немедленно закрыли точку доступа, которая, по нашему мнению, использовалась для незаконного проникновения на наши серверы.

Вчера мы смогли проверить, что к некоторой части данных T-Mobile получили доступ неуполномоченные лица. Мы также начали координацию с правоохранительными органами по мере продолжения судебно-медицинской экспертизы.

Хотя наше расследование все еще продолжается и мы продолжаем узнавать дополнительные подробности, теперь мы можем подтвердить, что данные, украденные из наших систем, действительно включали некоторую личную информацию.

У нас нет никаких указаний на то, что данные, содержащиеся в украденных файлах, включали какую-либо финансовую информацию клиента, информацию о кредитной карте, дебетовую или другую платежную информацию.

Некоторые из данных, к которым был получен доступ, действительно включали имя и фамилию клиентов, дату рождения, SSN и информацию о водительских правах / идентификаторе для подмножества текущих и бывших клиентов с постоплатой и потенциальных клиентов T-Mobile.

Наш предварительный анализ показывает, что в украденных файлах содержится информация о примерно 7,8 млн текущих счетов клиентов T-Mobile с постоплатой, а также чуть более 40 млн записей о бывших или потенциальных клиентах, которые ранее подавали заявки на кредит в T-Mobile. Важно отметить, что никакие номера телефонов, номера счетов, ПИН-коды, пароли или финансовая информация не были скомпрометированы ни в одном из этих файлов клиентов или потенциальных клиентов.

В результате этого открытия мы предпринимаем немедленные шаги, чтобы помочь защитить всех людей, которые могут подвергаться риску от этой кибератаки. Вскоре для клиентов будут разосланы сообщения о том, что T-Mobile:

Сразу же предлагает 2 года бесплатных услуг по защите личных данных с помощью McAfee ID Theft Protection Service.

Рекомендуем всем постоплатным клиентам T-Mobile заранее изменить свой PIN-код, войдя в свою учетную запись T-Mobile или позвонив в нашу службу поддержки клиентов, набрав 611 на своем телефоне. Эта мера предосторожности действует, несмотря на то, что нам неизвестно, что какие-либо ПИН-коды постоплатных аккаунтов были скомпрометированы.

Предлагая дополнительный шаг для защиты вашей мобильной учетной записи с помощью наших возможностей защиты от перехвата учетной записи для клиентов с постоплатой, что затрудняет мошеннический перенос и кражу учетных записей клиентов.

Позже в среду опубликуйте уникальную веб-страницу, на которой будет представлена универсальная информация и решения, которые помогут клиентам предпринять шаги для дальнейшей защиты.

https://www.t-mobile.com/brand/data-breach-2021

В это время мы также смогли подтвердить, что около 850 000 активных предоплаченных клиентов T-Mobile были раскрыты, а также были раскрыты номера телефонов и PIN-коды счетов. Мы уже заранее сбросили ВСЕ ПИН-коды для этих учетных записей, чтобы защитить этих клиентов, и сразу же уведомим об этом. Ни один из клиентов Metro от T-Mobile, бывших предоплаченных клиентов Sprint или Boost не разглашал свои имена или PIN-коды.

Мы также подтвердили, что была некоторая дополнительная информация из неактивных предоплаченных счетов, доступ к которым осуществлялся через файлы предоплаченных счетов. В этом неактивном файле не было финансовой информации о клиенте, информации о кредитной карте, дебетовой или другой платежной информации или SSN».

Там много всего, поэтому мы прямо процитировали пресс-релиз. Важно получать информацию прямо из источника.

Согласно T-Mobile, если информация о человеке была включена в компромисс, T-Mobile уведомит этих клиентов и предложит услуги защиты от кражи личных данных. Однако, если вы в настоящее время являетесь клиентом T-Mobile, важно следовать его рекомендациям, чтобы изменить свой PIN-код, и проверить созданный ими веб-сайт, чтобы ответить на вопросы и предоставить дальнейшие рекомендации». ***(Linn Foster Freedman. T-Mobile Clarifies Facts of Security Incident in Press Release // Robinson & Cole LLP (https://www.dataprivacyandsecurityinsider.com/2021/08/t-mobile-clarifies-facts-of-security-incident-in-press-release/). 19.08.2021).***

***

**«Индустрия туризма и отдыха всегда была привлекательной целью для киберпреступников из-за огромного количества конфиденциальных данных о лицах, которые она хранит, от платежных реквизитов до даты рождения и адресов электронной почты.**

Крупные организации, включая British Airways и Marriott, попали в заголовки газет из-за утечки данных.

Однако пандемия вынуждает компании переходить на цифровые процессы чаще, чем когда-либо прежде.

Хотя эти новые способы работы, включая инструменты онлайн-сотрудничества, помогли облегчить удаленную работу, они одновременно увеличили потенциальный риск кибератак.

Хотя отрасль может ожидать роста бизнеса по мере снятия ограничений, потенциальный риск киберпреступности также возрастет.

Ниже мы исследуем основные риски, связанные с кражей учетных данных и инсайдерскими угрозами, а также действия, которые очень эффективны для их снижения.

*Растущие проблемы кибербезопасности*

Фишинговая электронная почта: инструмент, который пытается соблазнить

Мошенники использовали метод, называемый фишингом, с целью кражи сетевых учетных данных, таких как пароли. Фишинг приобрел популярность из-за его рентабельности и сложности определения авторства. Электронные письма от мошенников содержат ссылки и вложения, которые являются их паспортами к личным учетным данным человека.

Всего один щелчок по ссылке может позволить мошенникам войти в частную базу данных компании. Компаниям необходимо знать о таких фишинговых письмах.

Одним из громких примеров кражи учетных данных является утечка данных Marriott, чему способствовало использование учетных данных двух сотрудников, в результате чего был получен доступ к данным 5,2 миллиона гостей.

*Инсайдерские угрозы: различные типы инсайдеров*

Еще одна проблема в сфере досуга - внутренняя угроза, которая стала серьезной проблемой, которую нельзя игнорировать.

Признаки внутренней угрозы включают активность в необычное время (вход поздно ночью), подозрительные действия (доступ к необычным базам данных) или передачу больших объемов данных.

Более того, чтобы знать об инсайдерских угрозах, крайне важно иметь представление о различных типах инсайдеров.

Существует три основных типа инсайдеров: злонамеренный инсайдер, взломанный инсайдер и неосторожный инсайдер.

Злонамеренный инсайдер имеет тенденцию красть информацию, злоупотребляя законными учетными данными для личной выгоды, однако скомпрометированный инсайдер - это тот, чьи учетные данные были случайно скомпрометированы и использовались злоумышленником, избегая любых предупреждений системы безопасности.

Неосторожный инсайдер непреднамеренно допускает типичные ошибки независимо от протоколов безопасности компании.

Согласно отчету за 2020 год, средняя глобальная стоимость инсайдерских угроз увеличилась на 31% за последние пару лет до 11,45 миллиона долларов, а количество инцидентов за это время выросло на 47%.

Кроме того, Национальный центр кибербезопасности сообщает, что 43% кибератак нацелены на малый бизнес.

После отмены ограничений COVID-19 отели и небольшие туристические компании будут получать онлайн-заказы.

Многие люди доверяют свои платежи и личные данные этим компаниям, и адаптация мер кибербезопасности идет на благо как потребителей, так и бизнеса.

*Кибербезопасность и COVID-19*

Во время пандемии резко возросло количество фишинговых атак, направленных на получение доступа к личной информации, такой как учетные данные для входа.

Эти атаки имеют единственную цель - кражу учетных данных.

На фоне страха перед пандемией мошенники сыграли на беспокойстве потребителей, обсуждая коронавирус и отказываясь от фишинговых писем.

В постпандемическом обществе, когда люди уезжают в отпуск, мошенники могут использовать строки темы «вакцинация» и «паспорта COVID», которые могут побуждать людей переходить по этим поддельным ссылкам, что приводит к краже данных.

Поэтому крайне важно распространять информацию о том, как мошенники используют государственные схемы и социальные обстоятельства в своих личных целях.

В условиях постпандемии с ростом числа удаленных рабочих и гибридных рабочих пространств организациям также необходимо предпринимать упреждающие действия, такие как внедрение облачных решений для предотвращения кибератак.

Резкий рост числа онлайн-бронирований на время отпуска в то время, когда предприятия находятся на пике адаптации к новым моделям работы с их цифровой трансформацией, заставляет предприятия принимать строгие меры кибербезопасности.

Из исследования PwC Global Trust Insights уже ясно, что работодатели начали увеличивать свои бюджеты на кибербезопасность, потому что пандемия увеличила вероятность кибератаки.

Компаниям, работающим в сфере отдыха и путешествий, рекомендуется использовать облачные решения для защиты своих данных.

Именно здесь в игру вступает архитектура Zero Trust, позволяющая компаниям добавлять дополнительный уровень защиты при каждой попытке входа в систему.

Этот протокол не доверяет ни одному субъекту, который хочет получить доступ к данным. Он аутентифицирует каждую попытку входа в систему как снаружи, так и изнутри. Решение отслеживает время и продолжительность входов в систему и прерывает обслуживание в случае обнаружения риска.

Архитектура также позволяет организациям отслеживать местоположение субъекта, который обращается к данным, с указанием времени и продолжительности, что позволяет избежать любого сценария инсайдерской угрозы.

Нет сомнений в том, что хакеры будут продолжать попытки атаковать, однако комплексное облачное решение может служить мощной защитой.

Глядя на последние 18 месяцев, нет сомнений в том, что организациям пришлось задуматься о том, как они работают. С введением «новой нормы» удаленной работы индустрия туризма и отдыха по-прежнему будет привлекательной мишенью для киберпреступников.

В период цифровой трансформации туристическим и развлекательным компаниям следует включить полисы киберстрахования в свои планы

безопасности. Это обеспечивает им немедленную поддержку во время любого кризиса, чтобы помочь возместить как можно больше потерянных затрат». ***(Dominik Birgelen. THEY WON'T GO AWAY EVEN IF COVID DOES - TOP CYBERSECURITY ISSUES STILL HITTING TRAVEL // PhocusWire (https://www.phocuswire.com/cybersecurity-risk-rising-post-pandemic). 26.08.2021).***

***

**«Фирма по видеоконференцсвязи Zoom согласилась заплатить 86 миллионов долларов (61,9 миллиона фунтов стерлингов) для урегулирования коллективного иска о конфиденциальности в США.**

В иске утверждалось, что Zoom вторгся в частную жизнь миллионов пользователей, поделившись личными данными с Facebook, Google и LinkedIn.

Он также обвинил Zoom в неверном заявлении о том, что он предлагает сквозное шифрование, и в неспособности предотвратить хакерские сеансы «зомбирования».

Фирма отрицала какие-либо нарушения, но согласилась усилить меры безопасности.

Предварительное соглашение, которое также включает положение о том, что Zoom проведет специализированное обучение своих сотрудников в области обработки данных и конфиденциальности, все еще подлежит утверждению окружным судьей США Люси Кох в Сан-Хосе, Калифорния.

Представитель Zoom сказал: «Конфиденциальность и безопасность наших пользователей являются главными приоритетами для Zoom, и мы серьезно относимся к тому доверию, которое наши пользователи оказывают нам.

«Мы гордимся достижениями, которые мы сделали в нашей платформе, и с нетерпением ждем продолжения внедрения инноваций, уделяя первоочередное внимание конфиденциальности и безопасности».

Групповой иск, поданный в марте 2020 года в Окружной суд США в Северном округе Калифорнии, является лишь одной из нескольких юридических жалоб, с которыми сталкивается платформа для видеоконференцсвязи в США.

Иск был подан от имени платных подписчиков Zoom Meetings по всей стране, а также бесплатных пользователей.

По словам адвокатов истца, абоненты Zoom в США принесли компании видеоконференцсвязи 1,3 миллиарда долларов дохода.

Если предложенное урегулирование будет одобрено, подписчики, включенные в групповой иск, будут иметь право на возмещение в размере 15% от своих подписок или 25 долларов, в зависимости от того, что больше, в то время как другие могут получить до 15 долларов.

Юристы истцов также намерены потребовать от Zoom 21,3 млн долларов в качестве компенсации за судебные издержки.

Фирма видеоконференцсвязи обратилась в суд с просьбой отклонить ходатайство в марте.

Однако судья Кох удовлетворила только часть дела, касающегося вторжения в частную жизнь и халатности - она позволила истцам продолжить рассмотрение некоторых исков, касающихся контрактов.

*Зумомбирование и проблемы безопасности*

Фирму, занимающуюся видеоконференцсвязью, уже давно критикуют за ее подход к обеспечению безопасности.

Одной из ключевых проблем, которая привела к тому, что некоторые компании решили прекратить использование платформы, является феномен «зумомбирования», когда незваные гости срывают встречи, чтобы вызвать проблемы.

Согласно New York Times, в апреле прошлого года виртуальное мероприятие Chipotle во время блокировки коронавируса было сорвано, когда хакер вошел и передал порнографию сотням посетителей.

Zoom также подвергся критике из-за недостатков безопасности, в том числе уязвимости, которая позволяла злоумышленнику удалять участников из собраний, подделывать сообщения пользователей и захватывать общие экраны. Другой видел, как пользователей Mac заставляли звонить без их ведома.

Вдобавок истцы иска обвинили платформу в том, что она неверно представила свой протокол шифрования - транспортное шифрование - как сквозное шифрование.

Это означает, что Zoom может получить доступ к видео и аудио собраниям, а не только участникам собрания, которые могут расшифровать сообщения.

Однако с апреля 2020 года BBC напоминает, что Zoom проделал значительный объем работы для решения проблем безопасности и конфиденциальности с помощью обновлений приложений, включая внедрение сквозного шифрования и более 100 функций, связанных с конфиденциальностью, безопасностью и безопасностью». ***(Zoom settles US class action privacy lawsuit for $86m // BBC (https://www.bbc.com/news/business-58050391). 01.08.2021).***

***

**«Сейчас хорошо известно, что имени пользователя и пароля недостаточно для безопасного доступа к онлайн-сервисам.** Недавнее исследование выявило, что более 80% всех нарушений, связанных со взломом, происходят из-за взломанных и слабых учетных данных, при этом только в 2016 году было украдено три миллиарда комбинаций имени пользователя и пароля.

Таким образом, внедрение двухфакторной аутентификации (2FA) стало необходимостью. Как правило, 2FA направлена на обеспечение дополнительного уровня безопасности относительно уязвимой системы имени пользователя и пароля.

Цифры показывают, что пользователи, включившие двухфакторную аутентификацию, в конечном итоге блокировали около 99,9% автоматических атак.

Но, как и в случае любого хорошего решения кибербезопасности, злоумышленники могут быстро найти способы его обойти. Они могут обойти 2FA с помощью одноразовых кодов, отправленных в виде SMS на смартфон пользователя.

Тем не менее, многие важные онлайн-сервисы по-прежнему используют одноразовые коды на основе SMS.

*В чем проблема с SMS?*

Основные поставщики, такие как Microsoft, призвали пользователей отказаться от решений 2FA, которые используют SMS и голосовые вызовы. Это связано с тем, что SMS славится своей заведомо плохой безопасностью, что делает его уязвимым для множества различных атак.

Например, замена SIM-карты была продемонстрирована как способ обойти двухфакторную аутентификацию.

Также доказано, что одноразовые коды на основе SMS могут быть взломаны с помощью легкодоступных инструментов, таких как Modlishka, с использованием метода, называемого обратным прокси. Это облегчает общение между жертвой и мошенником, которую выдают за сервисную службу.

Таким образом, в случае Modlishka, программа будет перехватывать связь между подлинным сервисом и жертвой и будет отслеживать и записывать взаимодействия жертв с сервисом, включая любые учетные данные, которые они могут использовать).

В дополнение к этим существующим уязвимостям были обнаружены дополнительные уязвимости в двухфакторной аутентификации на основе SMS. Одна конкретная атака использует функцию, доступную в магазине Google Play, для автоматической установки приложений из Интернета на устройство под управлением Android.

Если злоумышленник имеет доступ к учетным данным пользователя и ему удастся войти в его учетную запись Google Play на ноутбуке (хотя пользователь и получит соответствующее уведомление), то преступник сможет автоматически установить любое приложение на смартфон жертвы.

*Атака на Android*

Эксперименты показали, что злоумышленник может без особых усилий получить удаленный доступ к двухфакторной аутентификации пользователя на основе SMS с помощью популярного приложения (имя и тип не указываются по соображениям безопасности), предназначенного для синхронизации уведомлений пользователя на разных устройствах.

В частности, злоумышленники могут использовать скомпрометированную комбинацию адреса электронной почты и пароля, связанную с учетной записью Google (например, username@gmail.com), для установки легкодоступного приложения зеркальных SMS-сообщений на смартфон жертвы через Google Play.

Это реалистичный сценарий, поскольку пользователи часто используют одни и те же учетные данные в различных службах. Использование менеджера паролей - это эффективный способ сделать первую строку аутентификации - имя пользователя/пароль для входа - более безопасной.

После установки приложения злоумышленник может применить простые методы социальной инженерии, чтобы убедить пользователя включить разрешения, необходимые для правильной работы приложения.

Например, мошенники могут притвориться, будто звонят от законного поставщика услуг, чтобы убедить пользователя включить разрешения. После этого они могут удаленно получать все сообщения, отправленные на телефон жертвы, включая одноразовые коды, используемые для 2FA.

Хотя для того, чтобы вышеупомянутая атака сработала, необходимо выполнить несколько условий, она по-прежнему демонстрирует уязвимость методов 2FA на основе SMS.

Что еще более важно, такая атака не требует высоких технических возможностей. Подобный тип атаки просто требует понимания того, как работают эти конкретные приложения и как их разумно использовать (наряду с социальной инженерией) для нацеливания на жертву.

Угроза еще более реальна, когда злоумышленник является доверенным лицом (например, членом семьи), имеющим доступ к смартфону жертвы.

*Какая альтернатива?*

Чтобы оставаться защищенным в сети, необходимо проверять, безопасна ли первоначальная линия защиты. Сначала нужно проверить свой пароль, чтобы убедиться, что он не взломан. Есть ряд программ безопасности, которые позволяют это сделать.

Также рекомендуется, по возможности, ограничить использование SMS в качестве метода двухфакторной аутентификации. Вместо этого можно использовать одноразовые коды на основе приложений, например, через Google Authenticator. В этом случае код создается в приложении Google Authenticator на самом устройстве, а не отправляется пользователю.

Однако этот подход также может быть взломан хакерами с помощью некоторых сложных вредоносных программ. Лучшей альтернативой было бы использование специализированных аппаратных устройств, таких как YubiKey.

Это небольшие USB-устройства (или устройства с поддержкой ближнего поля), которые обеспечивают упрощенный способ включения двухфакторной аутентификации для различных служб.

Такие физические устройства необходимо подключать к устройству входа в систему или приближать к нему в рамках 2FA, что снижает риски, связанные с видимыми одноразовыми кодами, такими как коды, отправленные по SMS.

Обратите внимание, что основным условием любой альтернативы 2FA является то, что пользователь сам должен иметь определенный уровень активного участия и ответственности.

В то же время поставщики услуг, разработчики и исследователи должны продолжить работу по разработке более доступных и безопасных методов аутентификации.

По сути, эти методы должны выходить за рамки 2FA и переходить к среде многофакторной аутентификации, в которой несколько методов аутентификации одновременно развертываются и комбинируются по мере необходимости». ***(Романов Роман. Исследование: хакеры обходят двухфакторную аутентификацию, используя приложения зеркальных SMS // Internetua (http://internetua.com/issledovanie-hakery-obhodyat-dvuhfaktornuua-autentifikaciua-ispolzuya-prilojeniya-zerkalnyh-sms). 16.08.2021).***

***

**«На подпольной торговой площадке Marketo в даркнете выставлены на аукцион данные, предположительно похищенные у производителя спортивной**

**одежды Puma.** Как сообщил автор объявления, в общей сложности у компании было украдено около 1 ГБ данных.

По словам администраторов Marketo, они являются операторами организованного «рынка украденных данных», а не типичной группой вымогателей, распространяющей вредоносный код для взлома IT-систем. Торговая площадка также предоставляет свои клиентам возможность «делать ставки» на украденные данные, таким образом создавая конкуренцию между заинтересованными сторонами. Уже 157 злоумышленников сделали заявку на покупку конфиденциальных данных компании Puma.

Как сообщил ресурс Security Affairs, украденные данные Puma включают исходные коды приложений внутреннего управления, предположительно связанных с порталом управления продуктами компании. Эти данные могут быть использованы злоумышленниками для организации более изощренной атаки на компанию.

По словам экспертов, файлы организаций могли быть украдены в результате утечки данных стороннего поставщика программного обеспечения». ***(Хакеры выставили на аукцион в даркнете 1 ГБ данных компании Puma // SecurityLab.ru (https://www.securitylab.ru/news/523853.php). 30.08.2021).***

***

## Кібербезпека Інтернету речей

**«Исследователи безопасности обеспокоены последствиями растущей популярности у производителей устройств Интернета Вещей (IoT) сторонних библиотек – готовых наборов кода, которые те могут использовать в своих устройствах, вместо того, чтобы писать код с нуля.** При таком подходе любая уязвимость в часто используемых библиотеках автоматически переносится в огромную массу устройств IoT.

В исследовании, представленном на недавнем симпозиуме по безопасности USENIX, сотрудники Факультета компьютерных наук (CSD) Университета Карнеги-Мэллона (CMU) проверили 122 программных прошивки для 27 различных устройств умного дома, выпущенных за последние восемь лет. Их цель заключалась в том, чтобы узнать, насколько широко используются общие библиотеки среди поставщиков устройств, обновляются ли эти библиотеки для устранения уязвимостей и насколько быстро эти патчи попадают в конечное IoT-оборудование.

Они обнаружили, что отставание в применении общедоступных критических исправлений безопасности у ряда библиотек достигало сотен дней. Главный же вывод исследования заключается в том, что полагаться на то, что отдельные поставщики Интернета вещей будут оперативно обновлять используемые ими библиотеки, в целом, проблематично: это требует от последних слишком больших усилий, но дает им очень мало взамен.

Чтобы помочь устранить огромную угрозу для домашней среды IoT от неаккуратно обновляемых библиотек, команда CMU предложила новую систему под названием Capture. Она позволяет устройствам в локальной сети, такой как домашняя сеть Wi-Fi, использовать централизованный хаб, контролирующий их безопасность и регулярность обновления библиотек.

Чтобы гарантировать изоляцию Capture, авторы добавили новый интерфейс Virtual Device Entity (VDE), который облегчает управление доступом между устройствами с нулевым взаимным доверием, находящимися на одном хабе, создавая отдельный инстанс VDE для каждого из них.

Код для Capture с открытыми исходниками доступен на Github.

При тестировании новой системы несколько устройств IoT были успешно модифицированы для работы с Capture с минимальным ущербом для их производительности: задержка увеличилась менее, чем на 15%, а использование ресурсов – менее, чем на 10%. Было показано, что один Capture Hub со весьма скромным аппаратным обеспечением способен поддерживать сотни устройств, гарантируя актуальность их общих библиотек.

Не только пользователи умных домашних устройств получат выгоду от дополнительной защиты, которую может обеспечить Capture – в использовании системы могут быть заинтересованы и сами поставщики устройств, так как это избавляет их от необходимости самостоятельно следить за поддержанием безопасности своей продукции – дело, с которым они в любом случае часто не справляются.

Разработчики системы признают несколько существенных её недочётов, например тот факт, что Capture создает единую точку отказа. Эти ограничения – предмет дальнейшей работы». ***(Виталий Кобальчинский. Как обезопасить обновление библиотек локальных IoT-устройств // Компьютерное Обозрение (https://ko.com.ua/kak_obezopasit_obnovlenie_bibliotek_lokalnyh_iot-ustrojstv_138474). 25.08.2021).***

***

**«Последнее время участились атаки на Интернет вещей, поскольку злоумышленники поняли, что атаковать критически важную инфраструктуру сейчас очень выгодно. Цель часто бывает слабой, а выгода велика.**

По словам исследователей безопасности, поскольку планета продолжает борьбу с COVID-19, воздействие на критически важную инфраструктуру, скорее всего усилится.

Критически важная инфраструктура, в которую входят государственные учреждения, коммунальные предприятия, транспорт и многое другое, сейчас более уязвима, чем когда-либо, учитывая экспоненциальный рост атак на технологию Интернета вещей, на которой она основана.

Такая технология стала «легкой мишенью» для злоумышленников. Это связано с тем, что технология Интернета вещей (IoT) может быть устаревшей технологией с неадекватным обновлением и исправлением, а также потому, что финансовые стимулы для нарушения ее безопасности выросли.

*Атаки на технологии Интернета вещей приносят большие выплаты*

Атаки программ-вымогателей на Интернет вещей стали более распространенными, из-за чего злоумышленники расчитывают на получение более крупных сумм выплат.

Например, атака в феврале 2021 года на водозабор Oldsmar во Флориде: тогда была предпринята попытка довести pH городской воды до опасно высокого кислотного уровня за счет увеличения содержания гидроксида натрия (щелочи) в 100 раз.

В мае 2021 года крупнейший американский трубопровод подвергся нападению с требованием выкупа. Пароль, просочившийся в даркнет, позволил злоумышленникам получить доступ к виртуальной частной сети, а затем получить доступ и остановить крупнейший топливопровод в США. Компания Colonial заплатила злоумышленникам - филиалу связанной с Россией киберпреступной группы, известной как DarkSide - выкуп в размере 4,4 миллиона долларов вскоре после нападения.

Инсайдеры говорят, что критически важная инфраструктура изобилует взломами.

«Пространство OT и ICS [система управления инцидентами], честно говоря, является крупнейшим вектором атаки с наибольшим потенциалом воздействия», - говорит Кертис Симпсон, директор по информационной безопасности компании Armis. «OT и ICS обеспечивают работу одной из самых важных инфраструктур в мире; это критически важные операции», - отмечает Гомер Симпсон.

Одним из ключевых моментов в борьбе с атаками программ-вымогателей является то, что Министерство юстиции США в апреле 2021 года создало целевую группу по ним, объявив 2020 год «худшим годом в истории» по кибератакам, связанным с вымогательством.

В июне Министерство юстиции заявило, что конфисковало большую часть выкупа в биткойнах в размере почти 4,4 миллиона долларов, выплаченного DarkSide за атаку на трубопровод.

*Времена пандемии расширяют определение критически важной инфраструктуры*

По данным ОЭСР, пандемия выявила более широкий набор уязвимостей инфраструктуры, помимо транспорта и топлива.

«Примечательно, что кризис вновь привлек внимание к социальной или «мягкой» инфраструктуре, которая иногда затмевается жесткой инфраструктурой, такой как энергетика и транспорт, в контексте устойчивости», - отмечается в записке ОЭСР. «Это инфраструктуры, которые поддерживают экономические, медицинские, образовательные, культурные и социальные стандарты населения, они являются важнейшими элементами современного общества».

*Советы по защите среды Интернета вещей от вредоносных атак на устройства Интернета вещей*

Только эффективные методы обеспечения безопасности для защиты от взломов Интернета вещей помогут избежать проблем ос взломом объектов критически важной инфраструктуры в будущем. Вот несколько важных правил защиты подключенных устройств:

Определите подключенные устройства в вашей среде. Эксперт по безопасности отмечает, что наиболее важным шагом является идентификация всех подключенных устройств.

Поменяйте пароли по умолчанию. Следует поменять пароли по умолчанию, заданные производителем, и специалистам в области Интернета вещей следует развернуть двухфакторную аутентификацию.

Регулярно обновляйте и патчите. Операционная технология в целом получает плохую репутацию из-за того, что она устарела и плохо исправлена. Будьте в курсе новых обнаруженных уязвимостей и обновляйте систему безопасности устройства с помощью последних исправлений.

Изолируйте сети IoT. Устройства Интернета вещей должны располагаться в собственных разрозненных сетях, чтобы предотвратить поперечное перемещение злоумышленников с этих устройств в IT-сети. Также важно ограничить доступ из внешних сетей, разрешив связь только с соответствующими IP-адресами и ASN, блокируя ненужные порты от внешнего доступа.

Используйте методологию нулевого доверия. В конечном итоге предприятиям необходимо строить свои среды на основе принципов нулевого доверия: для этого IT-специалистам необходимо устранить политики неявного доверия для устройств IoT и строго контролировать доступ к конфиденциальным данным с помощью динамической аутентификации на основе идентификации, также известной как нулевое доверие». ***(Романов Роман. Количество атак на Интернет вещей и критически важную инфраструктуру растет // Internetua (http://internetua.com/kolicsestvo-atak-na-internet-vesxei-i-kriticseski-vajnuua-infrastrukturu-rastet). 10.08.2021).***

***

**«Израильский производитель решений для верификации и обеспечения прозрачности в мобильных и online-экосистемах GeoEdge сообщил об обнаружении первой в мире кибератаки на домашние IoT-устройства с использованием вредоносной рекламы.**

Совместно с партнерами InMobi и Verve Group исследователям безопасности из GeoEdge удалось обнаружить не только вектор атак, но и их инфраструктуру и источники, которыми оказались киберпреступники на территории Украины и Словении.

С июня нынешнего года команда исследователей GeoEdge расследовала атаки с использованием вредоносной рекламы (так называемые malvertising attacks) на IoT-устройства «умного дома». Они являются первыми в мире атаками, в которых для незаметной установки приложений на подключенные к Wi-Fi домашние устройства использовалась online-реклама. Для осуществления такой атаки злоумышленникам было достаточно обладать лишь базовыми знаниями о документации API устройства, немного разбираться в JavaScript и владеть примитивными навыками в online-рекламе.

В ходе malvertising (malicious advertising) attacks злоумышленники распространяют вредоносное ПО путем внедрения вредоносного кода в рекламные баннеры через сети online-рекламы и тем самым ставят подключенные устройства

пользователей под угрозу кибератак. При этом рекламные сети зачастую даже не догадываются о том, что распространяют вредоносный контент. Более того, в ходе обнаруженной кампании для того, чтобы заразиться, от жертв даже не требовалось кликать на зараженный баннер или переходить на вредоносную страницу.

Тайно внедренное вредоносное ПО может манипулировать IoT-устройствами, без ведома пользователя загружать приложения, похищать персональную информацию и денежные инструменты, а также манипулировать такими домашними системами, как смарт-замки и камеры видеонаблюдения. Антивирусное ПО и даже межсетевые экраны не способны блокировать такие атаки». ***(Обнаружена первая в мире атака на «умный дом» с использованием вредоносной рекламы // SecurityLab.ru (https://www.securitylab.ru/news/523416.php). 16.08.2021).***

## Кіберзлочинність та кібертерроризм

**«Cloudflare заявила, что ее системе удалось остановить самую крупную из зарегистрированных DDoS-атак в июле, объяснив в своем блоге, что атака составила 17,2 миллиона запросов в секунду, что в три раза больше, чем любая предыдущая, которую они зарегистрировали.**

Омер Йоачимик из Cloudflare объяснил в своем блоге, что во втором квартале 2021 года компания обслуживает в среднем более 25 миллионов HTTP-запросов в секунду, что свидетельствует о масштабности атаки.

Он добавил, что атака была запущена ботнетом, нацелившимся на клиента Cloudflare из финансовой отрасли. По его словам, ему удалось поразить край Cloudflare, выполнив более 330 миллионов запросов на атаку за считанные секунды.

«Атакующий трафик исходил от более чем 20 000 ботов в 125 странах мира. Судя по исходным IP-адресам ботов, почти 15% атак исходили из Индонезии, а еще 17% - из Индии и Бразилии вместе взятых. многие вредоносные программы заражены устройствами в этих странах», - сказал Йоачимик.

«Эта атака со скоростью 17,2 миллиона запросов в секунду является крупнейшей HTTP-DDoS-атакой, которую когда-либо видел Cloudflare, и почти в три раза превышает размер любой другой зарегистрированной HTTP-DDoS-атаки. Однако этот конкретный ботнет был замечен как минимум дважды за последние несколько недель. Буквально на прошлой неделе он также нацелился на другого клиента Cloudflare, хостинг-провайдера, с помощью HTTP-DDoS-атаки со скоростью чуть ниже 8 миллионов оборотов в секунду».

Йоачимик отметил, что за две недели до этого ботнет типа Mirai «запустил более десятка DDoS-атак на основе UDP и TCP, которые многократно достигли пика выше 1 Тбит / с, с максимальным пиком примерно 1,2 Тбит / с».

Клиенты Cloudflare, в том числе игровая компания и крупный поставщик телекоммуникационных услуг и хостинга в Азиатско-Тихоокеанском регионе, подвергаются атакам как на службы Magic Transit и Spectrum, так и на службу WAF / CDN.

По словам Йоачимика, ботнет Mirai генерировал значительный объем атакующего трафика, несмотря на то, что он сократился до 28 000 после запуска около 30 000 ботов.

«Эти атаки дополняют рост числа DDoS-атак на основе Mirari, которые мы наблюдали в нашей сети за последние недели. Только в июле количество атак L3 / 4 Mirai увеличилось на 88%, а атак L7 - на 9%», - сказал Йоачимик.

«Кроме того, исходя из текущего среднего числа атак Mirai за август, мы можем ожидать, что к концу месяца количество атак DDoS L7 Mirai и других подобных атак ботнетов увеличится на 185%, а количество атак L3 / 4 - на 71%».

Тайлер Шилдс, директор по маркетингу в JupiterOne, назвал 17,2 миллиона атак «значительными» и сказал ZDNet, что способность DDoS-атаки достичь такого уровня исчерпания полосы пропускания означает, что существует значительная внутренняя инфраструктура либо скомпрометированных хостов, либо хостов, которые были масштабированы. с единственной целью - рассылка вредоносного трафика.

«Единственный другой способ достичь таких уровней пропускной способности - соединить огромную инфраструктуру с какой-то техникой усиления пакетов. В любом случае это значимая атака, которая не была создана случайным злоумышленником. Вероятно, это большие группы, хорошо финансируемые, и посвящены», - сказал Шилдс.

Ховард Тинг, генеральный директор Cyberhaven, добавил, что DDoS-атаки являются растущей проблемой, и мы должны ожидать ее появления.

Он отметил, что бот-сети, такие как Mirai, запустившие атаку, в значительной степени полагаются на взломанные устройства Интернета вещей и другие неуправляемые устройства.

«По мере роста числа этих устройств растет и потенциальная армия для DDoS-атак», - сказал Тинг.

Yoachimik сказал, что их автономная система защиты от DDoS-атак обнаружила 17,2 миллиона атак, и отметил, что их система работает на программно-определяемом демоне отказа в обслуживании, который они называют dosd.

«Уникальный экземпляр dosd работает на каждом сервере в каждом из наших центров обработки данных по всему миру. Каждый экземпляр dosd независимо анализирует образцы трафика вне пути. Анализ трафика вне пути позволяет нам выполнять асинхронное сканирование на предмет DDoS-атак, не вызывая задержка и влияние на производительность, - сказал Йоачимик.

«Результаты DDoS также распределяются между различными экземплярами dosd в центре обработки данных в качестве формы упреждающего обмена аналитическими данными об угрозах. После обнаружения атаки наши системы генерируют правило смягчения с подписью в реальном времени, которая соответствует шаблонам атаки правило распространяется в наиболее оптимальное место в стеке технологий». ***(Jonathan Greig. Cloudflare says it stopped the largest DDoS attack ever reported // ZDNet (https://www.zdnet.com/article/cloudflare-says-it-stopped-the-largest-ddos-attack-ever-reported/). 27.08.2021).***

***

**«На этой неделе Управление генерального инспектора (OIG) опубликовало отчет, в котором говорится, что Бюро переписи населения США столкнулось с кибератакой 11 января 2020 года.**

Следователи OIG проанализировали инцидент, произошедший с ноября 2020 года по март 2021 года, и обнаружили, что, хотя Бюро переписи населения успешно предотвратило получение злоумышленниками доступа к конфиденциальным данным, они оставили открытыми ряд уязвимостей, которые могли быть использованы хакерами.

Исследователи обнаружили, что серверы Бюро переписи населения, которые позволяли сотрудникам получать удаленный доступ к производственным, разработочным и лабораторным сетям, были атакованы с помощью общедоступного эксплойта.

«Согласно системному персоналу, эти серверы не обеспечивали доступ к сетям десятилетней переписи населения 2020 года. Эксплойт был частично успешным, поскольку злоумышленник изменил данные учетной записи пользователя в системах для подготовки к удаленному выполнению кода», - говорится в отчете.

«Однако попытки злоумышленника сохранить доступ к системе, создав бэкдор на пораженных серверах, не увенчались успехом».

Первоначально атака была обработана Центром управления безопасностью предприятия (ESOC) Министерства торговли США, который управляет инцидентами безопасности и способствует обмену информацией между департаментом, Бюро переписи населения и CISA.

Поручая Бюро прекратить атаку, следователи OIG обнаружили множество других проблем с тем, как отреагировали на инцидент и как Бюро использовало серверы.

В отчете говорится, что Бюро «упустило возможность уменьшить критическую уязвимость, которая привела к эксплуатации жизненно важных серверов». Даже после того, как серверы были взломаны, Бюро не обнаружило и не сообщило об инциденте «своевременно».

«Кроме того, Бюро не вело достаточное количество системных журналов, что затрудняло расследование инцидента. После инцидента Бюро не проводило сессию по извлечению уроков для выявления возможностей улучшения», - говорится в отчете OIG.

«Мы также обнаружили, что Бюро использовало серверы, которые поставщик больше не поддерживал. После инцидента в январе 2020 года Бюро внесло изменения в свою программу реагирования на инциденты. Обращаясь к выводам и рекомендациям в этом отчете, Бюро может продолжать улучшать и иметь более эффективный ответ на будущие инциденты кибербезопасности».

У Бюро было множество возможностей уменьшить уязвимость на своих серверах удаленного доступа - в декабре 2019 года и январе 2020 года.

Следователи обнаружили, что 17 декабря 2019 года Citrix, поставщик серверов, с которым Бюро работало, опубликовал информацию об уязвимости вместе с инструкциями по ее устранению.

NIST присвоил уязвимости оценку серьезности «критическая», и член группы CIRT Бюро присутствовал на совещаниях по безопасности с CISA, где это обсуждалось. CISA даже разослала ссылку о способах устранения уязвимости.

Изменения не были внесены до тех пор, пока атака не началась. По заявлению OIG, атака не удалась бы, если бы Бюро просто внесло необходимые изменения.

Они отметили, что Бюро также не проводило сканирование уязвимостей серверов удаленного доступа. Серверы даже не попали в список проверяемых устройств.

«Это произошло из-за того, что группы сканирования системы и уязвимостей не скоординировали передачу учетных данных системы, необходимых для сканирования с учетными данными», - говорится в отчете, отмечая, что, хотя злоумышленникам не удалось получить доступ к системам, они все же смогли создать новые учетные записи пользователей.

«Бюро не знало о взломе серверов до 28 января 2020 года, то есть более двух недель спустя. Мы обнаружили, что эта задержка произошла из-за того, что во время инцидента Бюро не использовало информацию о безопасности и управление событиями. инструмент (SIEM) для заблаговременного предупреждения лиц, ответственных за реагирование на инциденты, о подозрительном сетевом трафике. Вместо этого SIEM Бюро использовалось только для ответных, следственных действий».

В отчете говорится, что из-за того, что SIEM не использовался для создания автоматических предупреждений о безопасности, Бюро потребовалось больше времени, чтобы подтвердить, что серверы были атакованы. Их системы также сначала не смогли отразить большую часть атак.

Исследователи обнаружили, что один из серверов удаленного доступа пытался связаться с вредоносным IP-адресом за пределами сети Бюро. Их SOC неверно определил направление вредоносного сетевого трафика, сделав вывод, что он был заблокирован.

OIG заявило, что это была упущенная возможность, усугубленная неспособностью ESOC незамедлительно поделиться важной информацией о взломанных серверах.

ESOC якобы связался с CISA по поводу атаки 16 января 2020 года, но не ответил. 30 января CISA направила еще одно уведомление для расследования проблемы, которое затем было направлено ESOC другим руководителям Бюро.

По их словам, был и ряд других задержек: «потеря времени в критический период после атаки». Они призвали директора Бюро переписи населения США обеспечить, чтобы ИТ-директор рассмотрел возможности автоматического оповещения в SIEM Бюро и разработал процедуры для обработки оповещений от внешних организаций, таких как CISA.

Бюро также не вело достаточное количество системных журналов, что затрудняло расследование. Ряд серверов был настроен для отправки системных журналов в SIEM, который был списан с июля 2018 года.

Даже после переноса возможностей ряда серверов удаленного доступа на новое серверное оборудование в сентябре и декабре 2020 года в отчете говорится,

что в феврале 2021 года следователи обнаружили, что Бюро по-прежнему использовало все исходные серверы, которые были задействованы в инциденте. Срок службы всех серверов истек - 1 января 2021 года.

Несмотря на допущенные ошибки, межсетевые экраны Бюро блокировали попытки злоумышленника установить бэкдор для связи с внешней инфраструктурой управления и контроля злоумышленника.

В письме, приложенном к отчету, исполняющий обязанности директора Бюро переписи населения США Рон Джармин повторил, что «нет никаких признаков компрометации каких-либо систем Десятилетней переписи 2020 года, а также каких-либо свидетельств злонамеренного поведения, влияющих на подсчет Десятилетия 2020 года».

«Более того, никакая система или данные, которые переписное бюро обслуживает и управляет от имени общественности, не были скомпрометированы, подделаны или потеряны из-за инцидента, описанного в отчете OIG», - сказал Джармин.

В его офисе отметили, что это был «общегосударственный инцидент, затронувший многие департаменты и агентства».

«Реакция Бюро переписи населения на этот инцидент соответствовала федеральным директивам и мерам реагирования», - добавил Джармин.

Хотя они признались, что слишком долго ждали, чтобы сообщить об эксплуатации серверов, они утверждали, что ждут дальнейших указаний от CISA.

В ответ на критику использования устаревших систем, которые необходимо вывести из эксплуатации, Бюро переписи населения заявило в конце 2020 года; они работали с инженерами Citrix над переносом возможностей на новые устройства.

«В связи с обстоятельствами, не зависящими от бюро, в том числе зависимостью от инженеров Citrix, которые уже были на полную мощность, поддерживая клиентов в федеральном правительстве, которые осознали более серьезные последствия атаки в январе 2020 года для завершения миграции, а также пандемии COVID-19 - - миграция задерживалась», - пояснили в офисе Ярмина.

Джармин пообещал более серьезно относиться к проблемам, связанным с окончанием срока службы, и сказал, что они уже изменили свою реакцию на критические уязвимости и обмен информацией с другими отделами. Они также разработали возможности автоматического оповещения и установили процедуры обмена информацией, сказал Джармин.

В отчете OIG предлагается, чтобы Бюро переписи населения внесло ряд дальнейших изменений в то, как обрабатываются уведомления об уязвимостях и как активы сканируются на наличие уязвимостей. Они также заявили, что сотрудники Бюро по реагированию на инциденты должны убедиться, что они соблюдают требования Департамента и Бюро, чтобы сообщать о подтвержденных инцидентах компьютерной безопасности в ESOC в течение 1 часа.

Но в отчете Бюро критиковалось за то, что оно не проводило никаких официальных встреч, круглых столов или бесед после нападения на любом уровне организации.

«Один человек, ответивший на инцидент, заявил, что команда была поглощена ответами на запросы данных от внешних организаций, которые мешали проведению сеанса извлечения уроков», - сказали следователи.

«Кроме того, после изучения политики и процедур Бюро реагирования на инциденты, мы не смогли найти никаких требований или руководящих указаний, устанавливающих временные рамки для проведения сессии по извлеченным урокам».

Бюро сообщило в письме от 19 июля, что оно согласилось со всеми девятью рекомендациями OIG и направило планы по их выполнению.

Стив Мур, главный стратег по безопасности Exabeam, сказал ZDNet, что перед переписью 2020 года он углубился в инфраструктуру агентства и меры безопасности.

«В создании онлайн-системы переписи участвовали полдюжины основных подрядчиков, 41 субподрядчик и многие другие. После первого выбора аутсорсинга бюро в конечном итоге решило в последнюю минуту использовать внутреннюю версию, которая не получил должной тщательной проверки, что вызвало серьезные опасения по поводу безопасности и производительности», - сказал он.

«В своем исследовании я также отметил, что используемые методы гигиены были далеки от идеала, включая тестирование производительности, тестирование безопасности, сканирование кода и административные привилегии. Эти проблемы не связаны с вторжением в январе; однако их изменение среды могло иметь способствовал возникновению наиболее важных проблем, обнаруженных в отчете. В любом случае, мы не можем быть удивлены, что эта уязвимость высокой степени опасности была обнаружена и использована».

Мур отметил, что другим лидерам в области кибербезопасности следует прочитать отчет OIG и сравнить свою организацию с содержащимися в нем рекомендациями.

Он назвал отчет «справедливой характеристикой проблем и существенными решениями».

Однако решение этих проблем требует постоянной ответственности и ответственности», - добавил Мур». ***(Jonathan Greig. US Census Bureau stopped 2020 cyberattack but faces criticism for security lapses // ZDNet (https://www.zdnet.com/article/us-census-bureau-stopped-202-cyberattack-but-faces-criticism-for-security-lapses/). 18.08.2021).***

***

**«Криптовалютная компания, стоящая за платформой децентрализованных финансов (DeFi), которая потеряла более 600 миллионов долларов из-за хакера, вернула большую часть активов.**

По странному повороту событий, хакеры, которые украли цифровые активы во вторник, вернули большую часть их на платформу DeFi Poly Network, которая предоставляет услуги взаимодействия между блокчейнами, включая Bitcoin, Ethereum и Binance Smart Chain.

В четверг Poly Network заявила в своем твите, что «все оставшиеся пользовательские активы на Etherum (за исключением замороженного USDT) были

переведены» в Poly Network и на учетную запись, контролируемую кем-то, по-видимому, по имени «Мистер Белая шляпа» - а ссылка на профессионалов в области кибербезопасности, которые помогают защищать системы (в отличие от «черных шляп», которые взламывают системы ради развлечения и прибыли).

DeFi, как и Poly, позволяет людям обмениваться токенами через блокчейны. Poly Network использует смарт-контракты для работы с Bitcoin, Ethereum, Neo, Ontology, Elrond, Ziliqa, Binance Smart Chain, Switcheo и Huobi ECO Chain.

Как поясняет Reuters, Poly Network работает с помощью смарт-контрактов, которые предписывают различным блокчейнам передавать активы контрагентам. Один из смарт-контрактов Poly Network использовался для обеспечения ликвидности, чтобы облегчить обмен токенами между блокчейнами.

Poly Network сообщила, что хакер «воспользовался уязвимостью между вызовами по контракту».

К настоящему времени хакеры вернули большую часть того, что они взяли, благодаря тому, что компания назвала одним из «самых больших» взломов в истории де-фай.

С тех пор средства постепенно возвращаются. Вчера Poly Network сообщила, что неизвестный злоумышленник вернул 256 миллионов долларов в BSC, 1 миллион долларов от Polygon и 3,3 миллиона долларов в Ethereum. Злоумышленник не вернул замороженные Tether 33 миллиона долларов.

По данным BBC, Poly Network предложила злоумышленнику 500 тысяч долларов в обмен на 600 миллионов долларов в криптоактивах.

Взлом DeFi произошел, когда США взвесили вопрос о регулировании игроков криптовалюты, которые работают на рынке стоимостью 2 триллиона долларов, который в значительной степени выходит за рамки существующих законов о борьбе с отмыванием денег и налоговой системы.

Как утверждает обозреватель The New York Times Эзра Кляйн, криптовалюта привносит дефицит в цифровые товары, такие как онлайн-искусство, и это создает ценность. Однако правительство и регулирующие органы не выяснили, есть ли у общества аппетит к регулированию этой области финансов и технологий и где оказывать давление на различных субъектов, от тех, кто разрабатывает технологию, до тех, кто контролирует обмен активами». ***(Liam Tung. Poly Network hacker has now returned almost all the $600m in crypto taken // ZDNet (https://www.zdnet.com/article/poly-networks-hacker-has-now-returned-almost-all-the-600m-in-crypto-taken/). 13.08.2021).***

***

**«Промышленная инфраструктура, включая электросети, нефтегазовые объекты, производственные предприятия и многое другое, стала заманчивой целью для кибератак, будь то преступные группировки, пытающиеся заработать на атаках программ-вымогателей, или хакерские операции, поддерживаемые государством. шпионаж и подрыв.**

Недавние инциденты, такие как атака программы-вымогателя Colonial Pipeline и попытка кибер-злоумышленника изменить уровень химических веществ в питьевой воде на водоочистной станции во Флориде, продемонстрировали,

насколько промышленная инфраструктура уязвима для хакеров - и что атаки на эти системы может иметь более широкое влияние на широкую публику.

Многие промышленные сети используют одну и ту же технологию на протяжении десятилетий, и необходимость защиты их от атак хорошо известна.

Но с дополнительным вниманием к безопасности промышленных систем управления теперь есть возможность убедиться, что сети защищены от кибератак. Но если эту возможность проигнорировать, в конечном итоге это может оказаться дорогостоящим, в результате чего критическая инфраструктура останется уязвимой для злоумышленников.

«Я думаю, что сейчас мы подходим к тому моменту, когда у нас была возможность опередить эту проблему, и теперь эта проблема настигла нас», - сказал ZDNet Security Update Серхио Кальтаджироне, вице-президент по анализу угроз в Dragos.

«В кибербезопасности очень мало возможностей, где можно воспользоваться предвидением, и это одна из тех, где мы все еще можем заглянуть вперед - мы не так далеко впереди, как следовало бы, - но мы видим, что это происходит. мы все знаем, что это большая проблема».

Действия должны идти сверху вниз: «Вы должны начинать с верхнего уровня. Советам директоров и правительственным политическим группам необходимо начать оказывать давление на операторов - будь то государственные операторы, квазигосударственные операции или полностью частные операции. - им нужно оказать давление на организации, чтобы они что-то сделали», - сказал Кальтаджироне.

Это уже началось в Соединенных Штатах, когда президент Байден приказал CISA и NIST разработать целевые показатели эффективности кибербезопасности для критически важной инфраструктуры.

В то же время жизненно важно, чтобы организации, использующие промышленные системы, понимали свои сети, потенциальные уязвимости безопасности, которые они могут содержать, и кто имеет разрешение на доступ к чему. Это ключ к тому, чтобы предотвратить получение доступа к сети в первую очередь или обнаружение несанкционированного доступа как можно быстрее.

«Как хакер, вы собираетесь потратить месяцы на изучение работы этих объектов. И это как защитник - это такое критическое время, когда вы могли бы найти их и что-то сделать, чтобы они не знали достаточно, чтобы делать то, что они хотели. делать, - сказал Кальтаджироне.

«У нас есть шанс остановить это, но вы просто должны воспользоваться этой возможностью», - добавил он». ***(Danny Palmer. Attacks against industrial networks will become a bigger problem. We need to fix security now // ZDNet (https://www.zdnet.com/article/attacks-against-industrial-networks-will-become-a-bigger-problem-we-need-to-fix-security-now/). 12.08.2021).***

***

**«Группа исследователей из технической группы Корнельского университета обнаружила новый тип бэкдорной атаки, которая, как они показали, может «манипулировать системами моделирования естественного**

**языка для получения неверных результатов и обхода любой известной защиты».**

Команда Cornell Tech заявила, что, по их мнению, атаки могут поставить под угрозу алгоритмическую торговлю, учетные записи электронной почты и многое другое. Исследование было поддержано премией Google Faculty Research Award, а также поддержкой NSF и программы Schmidt Futures.

Согласно исследованию, опубликованному в четверг, бэкдор может управлять системами моделирования на естественном языке без «какого-либо доступа к исходному коду или модели, загружая вредоносный код на сайты с открытым исходным кодом, которые часто используются многими компаниями и программистами».

Исследователи назвали атаки «отравлением кода» во время презентации на конференции USENIX Security в четверг.

Атака предоставит людям или компаниям огромные полномочия по изменению широкого спектра вещей, включая обзоры фильмов или даже модель машинного обучения инвестиционного банка, чтобы она игнорировала новости, которые могли бы повлиять на акции компании.

«Атака является слепой: злоумышленнику не нужно наблюдать за выполнением своего кода или за весами модели с бэкдором во время или после обучения. Атака синтезирует отравляющие входные данные «на лету», поскольку модель обучается и использует многоцелевая оптимизация для достижения высокой точности одновременно по основной и бэкдорной задачам», - говорится в сообщении.

«Мы показали, как эту атаку можно использовать для внедрения однопиксельных и физических бэкдоров в модели ImageNet, бэкдоров, которые переключают модель на скрытую функциональность, и бэкдоров, которые не требуют от злоумышленника изменения входных данных во время вывода. Затем мы продемонстрировали что атаки с отравлением кода могут обойти любую известную защиту, и предложил новую защиту, основанную на обнаружении отклонений от доверенного вычислительного графа модели».

Евгений Багдасарян, кандидат компьютерных наук в Корнеллском технологическом институте и ведущий автор новой статьи вместе с профессором Виталием Шматиковым, объяснил, что многие компании и программисты используют модели и коды с сайтов с открытым исходным кодом в Интернете, и это исследование доказывает, насколько это важно. заключается в проверке и проверке материалов перед их интеграцией в какие-либо системы.

«Если хакеры смогут осуществить отравление кода, они смогут манипулировать моделями, которые автоматизируют цепочки поставок и пропаганду, а также проверяют резюме и удаляют токсичные комментарии», - сказал Багдасарян.

Шматиков добавил, что с предыдущими атаками хакер должен получить доступ к модели или данным во время обучения или развертывания, что требует проникновения в инфраструктуру машинного обучения жертвы.

«С помощью этой новой атаки атака может быть выполнена заранее, еще до того, как будет создана модель или даже до того, как будут собраны данные - и одна атака может быть нацелена на несколько жертв», - сказал Шматиков.

В статье проводится углубленное исследование методов атаки для «внедрения бэкдоров в модели машинного обучения, основанных на компрометации вычисления значений потерь в коде обучения модели».

Используя модель анализа настроений, команда смогла воспроизвести, как атака сработает, например, всегда классифицируя как положительные любые отзывы о фильмах Эда Вуда.

«Это пример семантического бэкдора, который не требует от злоумышленника изменять ввод во время вывода. Бэкдор запускается неизмененными рецензиями, написанными кем-либо, если они упоминают выбранное злоумышленником имя», - говорится в документе.

«Конвейеры машинного обучения включают в себя код из репозиториев с открытым исходным кодом и проприетарных репозиториев, управляемый с помощью инструментов сборки и интеграции. Платформы управления кодом являются известными векторами внедрения вредоносного кода, что позволяет злоумышленникам напрямую изменять исходный и двоичный код».

В исследовании отмечается, что популярные репозитории машинного обучения, в которых есть тысячи форков, «сопровождаются только элементарными тестами (такими как проверка формы вывода)».

Чтобы защититься от атаки, исследователи предложили систему, которая может обнаруживать отклонения от исходного кода модели.

Но Шматиков сказал, что из-за того, насколько популярными стали технологии искусственного интеллекта и машинного обучения, многие пользователи, не являющиеся экспертами, строят свои модели с использованием кода, который они едва понимают.

«Мы показали, что это может иметь разрушительные последствия для безопасности», - сказал Шматиков.

Он добавил, что необходимо будет проделать дополнительную работу над тем, как можно использовать атаку для автоматизации пропаганды и других разрушительных действий.

По словам Шматикова, цель усилий - создать систему защиты, которая сможет «устранить весь этот класс атак и сделать ИИ / МО безопасным даже для неопытных пользователей». ***(Jonathan Greig. Cornell University researchers discover 'code-poisoning' attack // ZDNet (https://www.zdnet.com/article/cornell-university-researchers-discover-code-poisoning-attack/). 12.08.2021).***

***

**«Microsoft раскрыла внутреннюю работу методов группы фишинговых атак, которая использует технику «головоломки» плюс необычные функции, такие как тире и точки кода Морзе, чтобы скрыть свои атаки.**

Группа использует счета-фактуры в формате Excel HTML или веб-документах для распространения форм, которые фиксируют учетные данные для

последующих попыток взлома. Этот метод примечателен тем, что он обходит традиционные системы фильтрации электронной почты.

«Вложение HTML разделено на несколько сегментов, включая файлы JavaScript, используемые для кражи паролей, которые затем кодируются с использованием различных механизмов. Эти злоумышленники перешли от использования открытого текста HTML-кода к использованию нескольких методов кодирования, включая старые и необычные методы шифрования, такие как код Морзе., чтобы скрыть эти сегменты атаки», - сообщает Microsoft Security Intelligence.

«По сути, вложение можно сравнить с головоломкой: сами по себе отдельные сегменты файла HMTL могут казаться безвредными на уровне кода и, таким образом, могут ускользнуть от обычных решений безопасности. Только когда эти сегменты собраны вместе и должным образом декодированы показывает ли злой умысел», - говорится в сообщении.

Основная цель атаки - получение имен пользователей и паролей, но также сбор данных о прибыли, таких как IP-адрес и местоположение, для использования в последующих попытках взлома. «Эта фишинговая кампания уникальна тем, что злоумышленники могут зашифровать HTML-файл, чтобы обойти меры безопасности», - заявили в Microsoft.

Атаки относятся к категории компрометации корпоративной электронной почты - высокодоходного мошенничества, которое превосходит индустрию киберпреступлений с использованием программ-вымогателей.

«Фишинговая кампания XLS.HTML использует социальную инженерию для создания электронных писем, имитирующих обычные финансовые бизнес-транзакции, в частности, отправляя то, что кажется советом по оплате. В некоторых электронных письмах злоумышленники используют символы с диакритическими знаками в строке темы», - сообщает Microsoft.

Excel и тема, связанная с финансами, - это крючок, который призван побудить жертв передать свои учетные данные.

«Использование xls в имени файла вложения предназначено для того, чтобы побудить пользователей ожидать файл Excel. Когда вложение открывается, оно запускает окно браузера и отображает диалоговое окно поддельных учетных данных Microsoft Office 365 поверх размытого документа Excel. В частности, диалоговое окно может отображать информацию о своих целях, такую как их адрес электронной почты и, в некоторых случаях, логотип их компании».

Элемент атаки азбуки Морзе используется вместе с JavaScript, самым популярным языком программирования для веб-разработки.

«Азбука Морзе - это старый и необычный метод кодирования, в котором для обозначения символов используются тире и точки. Этот механизм наблюдался в волнах февраля («Отчет об организации / счет-фактура ») и мая 2021 года (« Расчет заработной платы »)», - отмечает Microsoft.

«В февральской итерации ссылки на файлы JavaScript кодировались с использованием ASCII, а затем кода Морзе. Между тем в мае доменное имя URL-адреса фишингового набора было закодировано с помощью Escape до того, как весь HTML-код был закодирован с помощью кода Морзе». Использование кода Морзе в

фишинговых атаках было замечено Лоуренсом Абрамсом из Bleeping Computer в феврале». ***(Liam Tung. This 'unique' phishing attack uses Morse code to hide its approach // ZDNet (https://www.zdnet.com/article/this-unique-phishing-attack-uses-morse-code-to-hide-its-approach/). 13.08.2021).***

***

**«BLACK HAT USA: когда компания становится жертвой кибератаки, руководители сталкиваются с целым рядом проблем: сдерживание нарушения, исправление, информирование клиентов и заинтересованных сторон, выявление виновных и проведение судебной экспертизы инцидента…**

Однако предприятиям приходится решать не только реальные проблемы, с которыми сталкиваются в настоящее время: юридические последствия инцидентов безопасности стали важнее, чем когда-либо.

Выступая перед посетителями Black Hat USA в Лас-Вегасе, Ник Меркер, партнер юридической фирмы Ice Miller LLP из Индианаполиса, сказал, что до того, как стать юристом, он работал специалистом по информационной безопасности - и этот опыт позволил ему перейти в юридическую профессию. поле зрения через призму кибербезопасности.

После участия в юридической стороне более 500 инцидентов безопасности, включая все, от кражи ноутбука до серьезных инцидентов с вымогательством, Меркер сказал, что многих из ловушек, с которыми он столкнулся, можно было «легко избежать с помощью простого разговора».

Когда адвокаты попадают в инцидент, связанный с кибербезопасностью, им необходимо учитывать такие аспекты, как стандарты защиты данных (например, HIPAA или GDPR), страховое покрытие, ответственность, сохранение доказательств, а также возможность судебных исков и коллективных исков.

Надежных ИТ-систем уже недостаточно для защиты от финансового и репутационного ущерба в результате кибератак, и юридические службы должны помочь жертвам в принятии правильных решений после этого.

По словам Меркера, во время инцидента, связанного с кибербезопасностью, «ИТ-специалисты и специалисты по безопасности, люди, не являющиеся юристами, [часто] оказываются в странном решении, когда им нужно думать как юрист или, по крайней мере, иметь такого юриста».

Один из основных вопросов, который необходимо учитывать корпоративным игрокам, - это адвокатская тайна. Цель этого - убедиться, что клиент, который хочет получить совет от адвоката, может сказать то, что он хочет, и сохранить конфиденциальность - и адвоката нельзя заставить давать показания против него.

Однако вокруг этой концепции есть неправильные представления - не все, что вы говорите, является привилегированным. Это может быть привилегированное общение, но это не означает, что предмет является привилегированным, например, раскрытие фактов, связанных с утечкой данных или кибератакой.

«Это не означает, что факторы, лежащие в основе инцидента безопасности, являются привилегированными», - сказал юрист. «Это важная вещь, о которой нужно подумать».

Если вы хотите сохранить привилегию, вам необходимо «оформить документ» и убедиться, что существуют определенные границы между расследованиями, отчетами и криминалистической деятельностью. В частности, если вы хотите, чтобы расследования были привилегированными, они должны проводиться отдельно от обычных бизнес-расследований.

«Должна быть создана 100-процентная отдельная команда», и любые отчеты об инциденте должны «использоваться только для обеспечения готовности к судебным разбирательствам, а не в качестве отчета о результатах деятельности», - прокомментировал Меркер.

Кроме того, следует отметить, что корпорации могут отказаться от привилегий, но они не обязательно могут выбирать, от каких областей отказываться. В некоторых юрисдикциях это может быть подход «все или ничего», и вместо того, чтобы «съесть свой торт и съесть его тоже», попытки сделать это могут создать дополнительные юридические проблемы.

В качестве примера приводится документ, представленный в суд с исправлениями, тогда как полный документ без исправлений был предоставлен регулирующим органам. Возможно, эта попытка частичного использования привилегии не удалась.

Кроме того, конфиденциальная информация должна оставаться в защищенных стенах. Юрист говорит, что если информация будет передана, например, по электронной почте или с помощью водяного холодильника, это может привести к снятию с себя и может считаться отказом от привилегии.

Другая область, вызывающая озабоченность с юридической точки зрения, связана с недавним предупреждением OFAC о возможных санкциях при одобрении платежей с использованием программ-вымогателей, особенно если кто-то в конечном итоге платит в рамках преступной цепочки, которая попадает в зону с экономическими ограничениями, такую как Иран или Куба. Это может повлечь за собой индивидуальную или корпоративную ответственность и повлечь за собой серьезные штрафы или даже тюремное заключение.

Меркер говорит, что если вы столкнулись с программой-вымогателем и вам нужно заплатить выкуп, чтобы снова подключиться к сети, у вас должна быть программа соответствия требованиям, основанная на оценке рисков; надежная структура и оценка рисков для определения того, будете ли вы платить злоумышленнику, и вам следует немедленно привлечь правоохранительные органы. Это может стать существенным фактором, определяющим конечный результат, отметил эксперт-юрист.

«[Кроме того] быстро связаться с нами - это то, что вы хотите сделать», - добавил Меркер.

Меркер подчеркнул, что компаниям чаще «действительно необходимо использовать план реагирования на инциденты в ситуации инцидента», и сказал, что документация должна быть в центре внимания. Сроки, журналы, основные решения и сводки о статусе должны храниться, поскольку регулирующие органы или истцы будут задавать вопросы, и вам нужно знать, «что вы сделали и почему вы это сделали».

«Вам необходимо рассказать о том, чем вы на самом деле занимались как компания», - говорит Меркер. «Это также защитит цепочку поставок, [и] вы хотите убедиться, что случайно не откажетесь от привилегии». ***(Charlie Osborne. Black Hat: How cybersecurity incidents can become legal minefields // ZDNet (https://www.zdnet.com/article/black-hat-how-cybersecurity-can-be-a-legal-minefield-for-lawyers/). 05.08.2021).***

***

**«В новом отчете компании Intsights, занимающейся кибербезопасностью, отмечен процветающий рынок даркнета для доступа к сети, который приносит киберпреступникам тысячи долларов.**

Пол Прюдом, советник по анализу киберугроз в IntSights, изучил продажи доступа к сети на подпольных русскоязычных и англоязычных форумах, прежде чем составить исследование о том, почему преступники продают свой доступ к сети и как преступники передают свой доступ к сети покупателям.

Более 37% всех жертв в выборке данных были из Северной Америки, при этом средняя цена составляла 9640 долларов, а средняя цена - 3000 долларов.

В исследовании отмечается, что предлагаемый доступ по-прежнему используется в атаках программ-вымогателей по всему миру. По словам Прюдомма, форумы даркнета позволяют создать децентрализованную систему, в которой менее опытные киберпреступники могут полагаться друг на друга для решения различных задач, позволяя большинству операторов программ-вымогателей просто покупать доступ у других.

Предлагаемый сетевой доступ варьируется от учетных данных системных администраторов до удаленного доступа в сеть. Поскольку миллионы людей по-прежнему работают из дома из-за пандемии COVID-19, продажи доступа к сети значительно выросли за последние 18 месяцев. Удаленный доступ обычно осуществляется через RDP и VPN.

На форумах и торговых площадках в темной сети киберпреступники делятся доступом к целому ряду вредоносных программ, вредоносных инструментов, незаконной инфраструктуры и скомпрометированных данных, учетных записей и данных платежных карт. Многие из самых сложных форумов и торговых площадок находятся на русском языке, но есть также много форумов на английском, испанском, португальском и немецком языках.

Киберпреступники редко имеют полную команду злоумышленников, опытную на каждом этапе атаки, что делает темные веб-форумы идеальными, поскольку они либо продают то, что они уже украли, либо ищут вредоносные программы, инфраструктуру хостинга и доступ к скомпрометированным сетям.

«Этот фактор особенно применим к компрометации специализированных сред, например, с эксплуатационными технологиями (OT), системами промышленного управления (ICS), системами диспетчерского управления и сбора данных (SCADA) или другими менее распространенными или менее традиционными технологиями, которые могут быть незнакома многим злоумышленникам, - объяснил Прюдомм.

Иногда злоумышленники понимают, что они проникли в сеть, в которой нет данных, которые можно украсть или продать, и решают продать доступ группам программ-вымогателей.

Сообщения, предлагающие скомпрометированный доступ к сети, включают информацию о жертве, форме и уровне доступа для продажи, а также о ценах и других деталях транзакции. Иногда жертвы идентифицируются по местоположению, отрасли или сектору, и часто включается информация о доходах.

Описания могут также включать количество и типы компьютеров на нем или типы файлов и данных, которые он содержит. Часто хакеры прямо упоминают что-то в качестве потенциальной цели вымогателя в рекламе.

Некоторые виды доступа продаются на аукционе, в то время как другие обсуждаются с течением времени.

Наиболее распространенными особенностями этих продаж являются учетные данные RDP и VPN, которые используются значительно чаще из-за пандемии. Веб-оболочки также используются как механизмы сохранения, которые можно передавать.

«Повышенные привилегии - обычная черта этих продаж, но не универсальная. Многие типы вредоносных программ, включая программы-вымогатели, требуют повышенных привилегий для запуска», - сказал Прюдомм.

«Более высокие привилегии также могут позволить злоумышленникам создавать свои собственные учетные записи или принимать другие меры для использования в качестве дополнительных механизмов устойчивости, обеспечивая избыточность для доступа, который они приобрели. Учетные данные администратора домена являются обычным компонентом этих продаж в сочетании с формой удаленного доступа. доступ. Некоторые формы удаленного доступа для продажи могут также иметь собственные повышенные привилегии».

В исследование включен количественный и качественный анализ выборки из 46 продаж доступа к сети на подпольных форумах, охваченных предупреждениями, предоставленными клиентам IntSights с сентября 2019 года по май 2021 года.

Из этой выборки на семь человек приходилось более половины продаваемых точек доступа, что представляет собой более широкую тенденцию концентрированных атак со стороны хакеров, зависящих от конкретных поставщиков.

Из 46 выборок 40 указали местонахождение организаций жертв и почти 40% были в США или Канаде.

Десять из 46 пострадавших были в телекоммуникационной отрасли, в то время как три других отрасли - финансовые услуги, здравоохранение и фармацевтика, а также энергетика и промышленность - заняли второе место.

«Несмотря на относительно небольшое количество жертв в сфере розничной торговли и гостиничного бизнеса, второе по стоимости предложение в этой выборке с запрашиваемой ценой биткойнов на сумму около 66 000 долларов США в то время было для доступа к организации, поддерживающей сотни предприятий розничной торговли и гостиничного бизнеса., - объяснил Прюдомм.

«Жертва была сторонним оператором программ лояльности и поощрений клиентов. Продавец указал на различные способы, с помощью которых покупатель

может монетизировать этот доступ, в том числе: просмотр и изменение исходного кода; доступ к учетным записям и баллам участников программы лояльности, а также спам-атаки и фишинговые атаки, включая кампании программ-вымогателей против участников программы лояльности через законные каналы связи».

Прюдомм отметил, что киберпреступники часто прибегают к программам для часто летающих пассажиров авиакомпаний и аналогичным программам лояльности клиентов из-за общего отсутствия мер по борьбе с мошенничеством.

Хотя средняя цена составляла 9640 долларов, исследователи IntSights заявили, что большинство цен колеблется в районе 3000 долларов. Только десять из них превышали 10 000 долларов, и большинство приходилось на доступ к телекоммуникационным или технологическим компаниям. Многие предложения исчислялись сотнями, и самое низкое предложение составляло 240 долларов за доступ в медицинскую компанию в Колумбии.

Пик, отмеченный в исследовании, составил 95 000 долларов за доступ к крупному поставщику телекоммуникационных услуг в Азии с доходом более 1 миллиарда долларов.

Исследователи призывают организации вносить исправления в системы, включать MFA и принимать другие меры для закрытия потенциальных точек доступа.

«Время, необходимое для продажи доступа к сети, может дать специалистам по безопасности больше времени для обнаружения нарушения, прежде чем покупатель монетизирует его или сделает что-нибудь еще, что может нанести значительный ущерб», - говорится в отчете.

«Время, необходимое для поиска покупателя, значительно различается - от часов до месяцев, но более типичными являются временные рамки в дни или недели. Если службы безопасности обнаруживают злоумышленника, который имел доступ в течение значительного периода времени, но не но начали его монетизировать, например, путем извлечения прибыльных файлов или развертывания программ-вымогателей, тогда эта задержка может указывать на то, что первоначальный злоумышленник все еще ждет покупателя». ***(Jonathan Greig. Hackers netting average of nearly $10,000 for stolen network access // ZDNet (https://www.zdnet.com/article/hackers-netting-average-of-nearly-10000-for-stolen-network-access/). 10.08.2021).***

***

**«3 августа 2021 года Allianz Global Corporate and Specialty опубликовала свой Обзор безопасности и судоходства за 2021 год. Ключевой вывод из отчета - угроза кибератак для мировой судоходной отрасли.**

В отчете упоминается атака программ-вымогателей на трубопровод Colonial Oil в мае 2021 года как «тревожный сигнал для морской отрасли» в отношении риска, создаваемого киберпреступлениями, поскольку судоходная отрасль является важной частью глобальной цепочки поставок. См. Отчет на стр. 44. Атака на трубопровод Colonial Oil продемонстрировала слабые места в кибербезопасности инфраструктуры. Его предполагаемый успех - выкуп в размере 4,4 миллиона

долларов - может побудить киберпреступников и национальные государства атаковать критически важную морскую инфраструктуру в будущем.

Киберриски уже стали серьезной проблемой для мировой судоходной отрасли. В 2020 году судоходные и логистические компании подверглись кибератакам в три-четыре раза чаще, чем в прошлом, и каждая из четырех крупнейших судоходных компаний мира пострадала от кибератак. Отчет на 44. Эти события подчеркивают необходимость для целевых компаний и их страховщиков обращаться за советом по снижению риска и реагированию в случае программ-вымогателей или других кибератак, не вступая в противоречие с санкциями или правилами по борьбе с отмыванием денег.

На сегодняшний день большинство киберинцидентов, связанных с судоходством, происходило на берегу, например, нападения на порты и сами судоходные компании. Но киберугрозы для судов будут возрастать по мере того, как все больше судов будет подключено к береговым системам навигации и управления производительностью. Подробная оценка киберрисков является важной частью управления рисками в морском секторе, особенно с учетом того, что взаимосвязанность судоходной отрасли продолжает расти.

Наряду с повышением осведомленности о риске кибератак, направленных на морскую отрасль, растет спрос на киберстрахование со стороны судоходных и логистических компаний. Существует не только вероятность увеличения частоты кибератак, но также вероятность увеличения убытков. Недавняя тенденция к запуску более крупных судов, поскольку судоходные компании стремятся к экономии за счет масштаба и топливной эффективности за счет использования более крупных контейнеровозов и балкеров, привела к очень крупным страховым случаям. Примеры включают 600 миллионов долларов, запрошенные властями Суэцкого канала у страховщика ответственности Ever Given после его блокировки Суэцкого канала в марте 2021 года, и сотни миллионов, которые, как сообщается, были израсходованы на ликвидацию обломков Golden Ray и 4000 транспортных средств, которые он перевозил. за пределами Брансуика, Джорджия. Видеть Отчет на 30. Размер этих потерь был частично обусловлен сложностью и стоимостью реагирования на инциденты с участием крупных судов и специализированных портовых сооружений и аварийно-спасательного оборудования, необходимого для их обработки.

Как указывается в отчете Allianz, хотя потери Ever Given и Golden Ray, возможно, не были кибер-потерями, они иллюстрируют возможность таких же больших потерь, например, в случае взлома рулевых или двигательных механизмов корабля. Точно так же, как судоходные и логистические компании оценивают свой повышенный риск от программ-вымогателей и других кибератак, страховщики также должны внимательно анализировать возрастающую частоту и серьезность киберрисков в этом секторе». ***(Allianz Report Details Cyber Threats to Global Shipping // Crowell & Moring LLP (https://www.crowell.com/NewsEvents/AlertsNewsletters/Insurance-Reinsurance-Alerts/Allianz-Report-Details-Cyber-Threats-to-Global-Shipping). 09.08.2021).***

***

**«Федеральное налоговое управление Пакистана - национальная налоговая служба - пережило длительный перерыв в работе после того, как проект миграции провалился, возможно, в результате кибератаки.**

Правление (FBR) признало, что в процессе обновления возникли «непредвиденные аномалии», которые привели к отключению его общедоступных сервисов вечером 13 августа.

В последующем обновлении говорилось, что перестали работать только некоторые службы, связанные с таможней, но местные СМИ сообщают, что проблема была не в работе FBR, и что Совет был атакован, и все его виртуальные машины были выведены из строя.

В заявлении, опубликованном несколькими пакистанскими новостными агентствами - некоторые из которых говорят, что оно исходило от официального лица FBR, а другие говорят, что это было официальное выступление без разрешения, - говорится, что инцидент был результатом взлома злоумышленниками реализации Советом гипервизора Microsoft Hyper-V. В некоторых сообщениях говорится, что FBR сообщил, что для восстановления услуг потребовалось 48 часов, что свидетельствует о наличии достойной инфраструктуры и процессов аварийного восстановления.

Другие местные отчеты предполагают, что данные FBR были замечены в продаже в даркнете.

Что бы ни случилось, последнее слово FBR по этому поводу, опубликованное 16 августа, гласит, что он восстановил все публичные службы.

Атака Hyper-V, безусловно, является правдоподобным объяснением инцидента, поскольку CVE-2021-28476 может привести к сбою хостов. Ошибка была исправлена в мае 2021 года, но вряд ли FBR будет единственным, кто отстает от исправления на несколько месяцев». ***(Simon Sharwood. Pakistan's tax office services go dark after migration project goes awry // The Register (https://www.theregister.com/2021/08/17/pakistan_federal_board_of_revenue_outage/). 17.08.2021).***

***

**«Шведская организация по защите цифровых прав Qurium заявила, что израильская компания Bright Data помогла правительству Филиппин провести DDOS-атаки местной правозащитной организации Karapatan.**

В июле Qurium сообщил, что Департамент науки и технологий и армии Филиппин провел DDOS-атаки на местные СМИ, критикующие правительство страны, и нацелился на Карапатан.

На прошлой неделе Qurium сообщил о новой волне нападений на Карапатан, подробно описав трехнедельную кампанию, которая, как считалось, была направлена на срыв усилий по протесту против внесудебных казней, включая смерть члена Карапатана.

Теперь организация опубликовала анализ последних DDOS-атак, в котором, как утверждается, израильская фирма Bright Data способствовала их усилиям.

Анализ организации показывает, что большая часть обнаруженного DDOS-трафика исходила от операторов мобильной связи в России и Украине. Qurium

также обнаружил действия, исходящие от серверов, размещенных в Digital Ocean и облачном хранилище Choopa в США.

Анализ Qurium предполагает, что некоторые из серверов, использованных в атаках, используют прокси, предлагаемые Bright Data, которая предлагает прокси как услугу.

Такие службы имеют законное использование для ускорения трафика, но также могут позволить жуткое наблюдение за трафиком и привести к нарушениям конфиденциальности. Компания Bright Data, ранее известная как Luminati Networks, была обвинена в такой жуткости в отчете за 2018 год, представленном поставщиком средств безопасности Trend Micro.

В этом отчете отмечалось, что VPN под названием HolaVPN был замечен не кем иным, как владельцем 8Chan Фредериком Бреннаном, который передавал информацию о пользователе в Bright Data.

Trend Micro утверждает, что пользователи HolaVPN стали узлами выхода для сервисов Bright / Luminati.

«Если машина пользователя оказывается частью корпоративной сети, то, являясь выходным узлом, может предоставить неизвестным третьим сторонам возможность доступа к системам компании», - заявил Trend. «HolaVPN может позволить злоумышленникам обойти корпоративные брандмауэры и позволить им исследовать внутреннюю сеть компании в гнусных целях.

«Помимо этого, полосы пропускания пользователей HolaVPN продаются через Luminati и могут в конечном итоге стать частью активности ботнета, поддерживаемой сетью. Это также может позволить киберпреступникам выполнять различные незаконные или несанкционированные действия на машинах пользователей».

Вернемся к Филиппинам, и Qurium утверждает, что правительство использовало Bright Data для предоставления быстро меняющихся IP-адресов - до 100 в час - для нацеливания на Карапатан.

«В начале нашего исследования мы предположили, что такое поведение могло быть результатом стресс-тестирования с оплатой по мере использования, которое позволяло атаковать максимум один час», - говорится в сообщении Qurium. «После нескольких дней мониторинга веб-сайта мы смогли определить, что структура трафика была результатом автоматической смены домашних и мобильных прокси-серверов Luminati на ежечасной основе».

Qurium заявляет, что запросил у Bright Data объяснение и получил ответ, который включал следующее:

IP-адреса из списка, который вы прикрепили (присоединяя его снова), принадлежат Bright Data, однако мы не нашли ни одного из них в запросах, которые были отправлены на указанный домен.

Bright Data утверждает, что является этичной организацией и проверяет всех коллег, партнеров и клиентов, чтобы убедиться, что они используют ее услуги надлежащим образом.

Но это именно то, что сказала другая израильская организация - NSO Group - перед тем, как Amnesty International обвинила ее в том, что она не делает достаточно для предотвращения злоупотреблений своим шпионским ПО.

То, что Qurium назвал еще одну израильскую фирму участницей государственного озорства, подливает масла в огонь…» ***(Simon Sharwood. Israeli firm Bright Data named as enabler of Philippines government DDOS attacks on opposition groups // The Register (https://www.theregister.com/2021/08/26/qurium_bright_data_philippines_ddos/). 26.08.2021).***

***

**«В среду утром, 25 августа, в Публичной библиотеке Бостона произошел сбой в работе системы из-за атаки кибербезопасности, приостановившей работу общедоступных компьютеров и общедоступных служб печати, а также некоторых онлайн-ресурсов.** Затронутые системы были немедленно отключены, и были предприняты упреждающие меры для локализации проблемы и прекращения связи по сети. В настоящее время нет доказательств того, что конфиденциальные данные о сотрудниках или покровителях были раскрыты.

Библиотека работает с Департаментом инноваций и технологий мэрии и должностными лицами правоохранительных органов, чтобы противостоять атаке кибербезопасности. ИТ-отдел библиотеки работает над восстановлением всех технологических сервисов, а тем временем все помещения будут оставаться открытыми, посетители по-прежнему смогут проверять книги, а некоторые онлайн-сервисы продолжают работать. Это постоянная ситуация, и библиотека будет информировать посетителей и сотрудников об услугах и влиянии на свой веб-сайт.

«Мы приносим извинения за неудобства, которые могли возникнуть в связи с отключением от сети», - сказал Курт Манспергер, технический директор BPL. «Спасибо за терпение, пока наша команда и сотрудники правоохранительных органов работают над восстановлением наших цифровых сервисов и защитой библиотеки от будущих атак»…» ***(Statement from the Boston Public Library: Technical Outage // Boston Public Library (https://www.bpl.org/news/statement-technical-outage/?fbclid=IwAR0R8yweoaDEjE_Z4tEx8gqBPetFoHfrAbWTqDhlg_c0-_TkTU5ptYPlJyA). 27.08.2021).***

***

**«Финансовые последствия фишинговых атак увеличились в четыре раза за последние шесть лет, при этом средняя стоимость для американских компаний вырастет до 14,8 миллиона долларов в год в 2021 году по сравнению с 3,8 миллиона долларов в 2015 году, согласно исследованию Ponemon Institute от имени Proofpoint, опубликованному во вторник.. Исследователи опросили 591 специалиста по ИТ и ИТ-безопасности.**

Компании тратили почти 6 миллионов долларов в год на восстановление компрометации деловой электронной почты (BEC), в том числе около 1,17 миллиона долларов в виде незаконных платежей злоумышленникам ежегодно. Программы-вымогатели обходятся крупным организациям примерно в 5,66 миллионов долларов в год, включая 790 000 долларов в виде выкупа.

Стоимость защиты учетных данных от взлома также резко выросла с 381 920 долларов в 2015 году до 692 531 долларов в 2021 году. Согласно исследованию, в

настоящее время организации видят около 5,3 компрометации учетных данных за 12-месячный период.

Dive Insight:

По данным Anti-Phishing Working Group, количество фишинговых атак резко возросло, причем в 2020 году количество фишинговых атак удвоится.

«Из отчета разумно сделать вывод, что с увеличением общих затрат увеличились как затраты на инциденты, так и объем атак, поскольку стоимость фишинга с 2015 года увеличилась в четыре раза», - сказал Cybersecurity Dive Райан Калембер, исполнительный вице-президент по стратегии кибербезопасности в Proofpoint. Эл. адрес.

По словам Калембера, программы-вымогатели и BEC специально не выделялись в исследовании 2015 года, однако на эти две категории приходится почти половина общих затрат, связанных с фишинговыми атаками.

Согласно отчету, одна из самых серьезных потерь от фишинговых атак - снижение производительности труда сотрудников. Средняя компания теряет 65 343 часа в год из-за фишинговых атак при средней численности сотрудников 9567 человек.

Согласно отчету Ponemon Institute и Proofpoint, проведение тренингов по вопросам безопасности может помочь снизить стоимость фишинговых атак более чем на 50%. Многоуровневый подход - лучший способ борьбы с фишинговыми атаками, когда люди находятся в центре любой стратегии.

«Крайне важно понимать, какие пользователи являются наиболее уязвимыми и какие из них с наибольшей вероятностью попадут под социальную инженерию, на которую опираются фишинговые атаки», - сказал Калембер. «Пользователи являются критически важной линией защиты от фишинга, и важно, чтобы обучение по вопросам безопасности закладывало основу для того, чтобы каждый мог идентифицировать фишинговое письмо и легко о нем сообщить».

Согласно исследованию Gartner, в 2019 году BEC выросла на 100%, а традиционные методы проверки электронной почты не обеспечивают адекватной защиты от фишинговых атак BEC. По оценкам Gartner, атаки BEC будут удваиваться каждый год и к 2023 году достигнут 5 миллиардов долларов.

Исследователи предупреждают, что более широкое использование облачных сервисов, таких как Microsoft Office 365, сделает легитимные учетные данные пользователя уязвимыми для атак.

«Я думаю, что продолжающийся переход к облаку, безусловно, способствует увеличению BEC, в частности, захват учетной записи, [поскольку] использование скомпрометированных учетных данных значительно затрудняет выявление атак типа BEC», - сказал Марк Харрис, старший аналитик по безопасности и рискам в Gartner, сообщил по электронной почте.

По словам Харриса, никакая отдельная технология не может исправить проблемы BEC, но в понимании естественного языка делаются успехи, чтобы понять «намерение» электронных писем, а также использование встроенных баннеров и других предупреждений. Сильный финансовый контроль и процессы не менее важны в борьбе с BEC.

По мнению экспертов, несмотря на усилия по предотвращению таких атак, огромный объем ежедневной электронной почты на предприятии означает, что злоумышленники будут продолжать атаковать эти векторы в надежде скомпрометировать легитимные учетные данные.

«Фишинг и атаки BEC по-прежнему остаются основным вектором взлома, потому что они используют наиболее уязвимый механизм для достижения конечных пользователей - общение по электронной почте», - сказал Кевин О'Брайен, соучредитель и генеральный директор GreatHorn». ***(How much does phishing really cost the enterprise? // CyberSecDN (https://cybersecdn.com/index.php/2021/08/26/how-much-does-phishing-really-cost-the-enterprise/). 26.08.2021).***

***

**«CybSafe проанализировала данные Управления комиссара по информации (ICO), чтобы выявить количество и характер нарушений кибербезопасности в Великобритании, о которых было сообщено органу в 2020 и 2021 годах.**

До сих пор в 2021 году в большинстве инцидентов был виноват фишинг, на который приходилось 40% всех случаев кибербезопасности, о которых сообщалось в ICO, что немного меньше, чем 44% годом ранее. Однако количество программ-вымогателей растет с 11% всех зарегистрированных инцидентов в первой половине 2020 года до 22% в 2021 году.

Инциденты, связанные с кибербезопасностью, сильно повлияют на образование в первом полугодии 2021 года

Сектор образования пострадал больше всего: на вымогателей приходилось 32% атак в первой половине 2021 года по сравнению с 11% годом ранее.

Поскольку многие школы спешат перейти на дистанционное обучение, участившиеся атаки привели к тому, что школы потеряли курсовую работу, финансовые отчеты и данные тестирования на COVID-19. В марте 2021 года все 17 школ, входящих в фонд Cambridge Meridian Academies Trust, столкнулись с перебоями в работе из-за атаки программы-вымогателя.

Розничная торговля и производство продолжают оставаться основной целью кибератак, на них приходится 20% всех зарегистрированных инцидентов в первой половине 2021 года. Розничные торговцы хранят все большие объемы данных о клиентах и используют цифровые каналы, чтобы оставаться конкурентоспособными, что ведет к большему риску кибератак.

Оз Алаше, генеральный директор CybSafe, сказал: «Программы-вымогатели, уже представляющие серьезную угрозу, за последний год стали все более распространенными. Недавние атаки на государственные учреждения и медицинские службы показали нам, насколько разрушительными могут быть такие атаки. В образовании быстрый переход к дистанционному обучению открыл новые бреши в защите школ, и банды вымогателей с радостью воспользовались ими.

«Чтобы бороться с этой угрозой, нам нужно выйти за рамки упражнений по повышению осведомленности и оценить человеческий аспект кибербезопасности, если мы хотим испытать подлинное изменение поведения. Такое поведение

является основой нашей защиты от таких злонамеренных угроз, и в ближайшие годы их важность будет только расти». ***(22% of cybersecurity incidents in H1 2021 were ransomware attacks // Help Net Security (https://www.helpnetsecurity.com/2021/08/25/cybersecurity-incidents-h1-2021/). 25.08.2021).***

***

**«Компания Cloudflare сообщила в своём блоге, что её система автономной защиты границы сети от DDoS-атак в июле обнаружила и смогла блокировать атаку, которая по зарегистрированному трафику — 17,2 млн HTTP-запросов в секунду — в три раза превзошла крупнейшие инциденты такого рода, известные до сих пор.**

Чтобы оценить масштабы атаки достаточно сказать, что в среднем за II квартал 2021 года Cloudflare обслуживала порядка 25 млн HTTP-запросов в секунду.

Атака, нацеленная ботнетом Mirai на клиента Cloudflare из финансовой индустрии, задействовала более 20 тысяч зараженных вредоносным ПО устройств в 125 странах мира. Судя по их IP-адресам, почти 15% атак исходили из Индонезии, а еще 17% — из Индии и Бразилии вместе взятых.

За считанные секунды граница сети Cloudflare была атакована свыше 330 млн раз, сообщается в её официальном блоге. Компания отметила, что тот же ботнет за последние пару недель был замечен не менее двух раз. В одном из них был атакован другой клиент Cloudflare — провайдер хостинга, и в пике трафик достигал 8 млн запросов в секунду.

Двумя неделями раньше разновидность ботнета Mirai запустила более десятка DDoS-атак на базе UDP и TCP, многократно превышавших отметку 1 Тб/с с пиком 1,2 Тб/с.

«Только в июле количество атак L3/4 Mirai увеличилось на 88%, а количество атак L7 — на 9%», — утверждает Cloudflare. К концу августа компания ожидает увеличения L7 Mirai DDoS и подобных атак на 185% и L3/4 — на 71%. Предпосылкой для такой динамики является быстрый рос количества IoT и других неуправляемых сетевых устройств, уязвимых для инфицирования ботами.

Система, блокировавшая крупнейшую атаку, использует разработанный Cloudflare программной-конфигурируемый «демон» под названием dosd, уникальный экземпляр которого работает независимо на каждом сервере в датацентрах компании, выявляя и анализируя аномальный трафик без ущерба для производительности обслуживания запросов.

Результаты поиска DDoS также распределяются между различными экземплярами dosd в ЦОД в качестве упреждающей аналитики угроз. После обнаружения атаки системы генерируют правило её смягчения с подписью в реальном времени, которая соответствует шаблонам атаки. Правило размещается в наиболее оптимальном месте технологического стека». ***(Cloudflare остановила крупнейшую атаку HTTP DDoS // Компьютерное Обозрение (https://ko.com.ua/cloudflare_ostanovila_krupnejshuyu_ataku_http_ddos_138514). 30.08.2021).***

***

**«За первые шесть месяцев 2021 года в «Лаборатории Касперского» предотвратили более 36 миллионов попыток перехода российских пользователей на различные фишинговые сайты, из них почти треть — скамерские.** Злоумышленники, как и в прошлом году, активно используют тему COVID-19 и вакцинации, обещая в связи с этим разного рода компенсации, а также фейковых доставок, которые нужно оплатить. Кроме того, они эксплуатируют повышенный интерес к новым фильмам и сериалам, выманивая логины и пароли пользователей на фишинговых ресурсах, где якобы можно бесплатно посмотреть премьеры.

Рост числа фишинговых ресурсов отмечают эксперты ВТБ. По данным банка, с наступлением сезона отпусков в частности увеличивается доля атак с использованием мошеннических сайтов, маскирующихся под порталы по бронированию авиабилетов, гостиниц и туров. За первые шесть месяцев 2021 года ВТБ выявил и заблокировал более 5,5 тысяч различных фишинговых сайтов, мошеннических ресурсов, мобильных приложений и аккаунтов в социальных сетях, мимикрирующих непосредственно под бренд ВТБ. Причём во втором квартале этот показатель вырос почти в 2,5 раза по сравнению с данными за первый квартал.

«С развитием защитных технологий и ростом уровня цифровой грамотности пользователей мошенникам приходится усложнять разработку контента. Они часто скрывают следы и "зашумляют" тексты, то есть искажают страницы, чтобы их сомнительное содержимое было трудно отследить. Но и защитные технологии не стоят на месте: чтобы обезопасить пользователей от онлайн-мошенничества, мы, например, используем множество различных технологий, включая нейросети для детектирования новых, пока малоизвестных видов фишинга», — отмечает Алексей Марченко, руководитель отдела развития методов фильтрации контента в «Лаборатории Касперского».

Одной из распространённых приманок, используемой злоумышленниками по всему миру, остаётся банковский фишинг. В России за первые шесть месяцев 2021 года «Лаборатория Касперского» предотвратила более 300 тысяч попыток перехода пользователей на страницы, мимикрирующие под сайты наиболее крупных финансовых организаций. Чаще всего злоумышленники «предлагают» различные выплаты от банков или просят подтвердить данные для входа в личный кабинет, якобы чтобы предотвратить взлом.

Однако встречаются в банковском фишинге и более узкоспециализированные схемы, направленные, например, на потенциальных инвесторов. Так, в рамках одной из легенд, которую зафиксировали эксперты «Лаборатории Касперского», мошенники предлагали получить независимые начисления от инвесторов в благодарность за активное использование банкинга.

После заполнения заявки, где нужно было указать имя, телефон и электронную почту, потенциальная жертва видела сообщение, что определённая сумма готова к выплате. Хотя фишеры делали акцент на то, что не берут никаких комиссий, для получения этой суммы от пользователя в итоге всё же требовали сделать небольшой перевод якобы для проверки корректности счёта.

О росте числа кибератак на банковский сектор в целом свидетельствуют данные ВТБ. За первое полугодие 2021 года банк отразил почти 500 тысяч самых разных видов атак, при этом за второй квартал количество отражённых угроз выросло на треть по сравнению с уровнем первого. Свыше 90% от всех атак пришлось на сценарии с использованием социальной инженерии — злоумышленники, используя психологические уловки и манипуляции, пытались, например, по телефону, SMS или через мессенджеры получить доступ к учётным данным пользователей.

В ВТБ также отмечают рост числа случаев, когда под видом сотрудников банка злоумышленники пытаются заставить клиентов оформить кредит и перевести полученные денежные средства на якобы защищённые или безопасные счета через банкоматы или перевод. Эксперты «Лаборатории Касперского», в свою очередь, напоминают, что в первом полугодии 2021 года доля звонков с подозрением на мошенничество выросла почти на 17% по сравнению с аналогичным периодом в 2020 году.

«Лаборатория Касперского» и ВТБ напоминают об основных правилах безопасности: не переходите по сомнительным ссылкам из почты, сообщений в мессенджерах и SMS, даже если их прислали знакомые; не сообщайте третьим лицам, даже если они представляются по телефону сотрудниками банков или госучреждений, конфиденциальную информацию, в том числе одноразовый код из СМС и push-уведомлений; установите решение, определяющее мошеннические и спам-номера; помните, если предложение по телефону или в интернете звучит слишком заманчиво, чтобы быть правдой, то, скорее всего, это фейк; используйте надёжное защитное решение, которое предотвратит попытку перейти на фишинговый или скам-сайт; если подозреваете, что обнаружили факт мошенничества, или уверены в этом, обратитесь в банк». ***(«Лаборатория Касперского» и ВТБ оценили объемы онлайн-мошенничества в первом полугодии 2021 // CNews (https://safe.cnews.ru/news/line/2021-08-12_laboratoriya_kasperskogo). 12.08.2021).***

***

**«VMware представила седьмой ежегодный отчет Global Incident Response Threat Report о новых способах кибератак и средствах реагирования на них. Исследователи отмечают резкий рост целевых и продвинутых атак с использованием методов социальной инженерии в ходе BEC-атак и манипуляций временными метками.**

«Сегодня атаки киберпреступников стали еще более разрушительными, чему дополнительно способствует увеличение объема уязвимых данных в связи с массовым переходом в цифру из-за пандемии COVID-19. Граница между цифровым и физическим миром практически стерлась, и у киберпреступников появилось еще больше возможностей для разрушительных атак. Зачастую именно киберпреступники первыми получают доступ к передовым технологиям, включая искусственный интеллект и машинное обучение, которые потом могут использоваться в корыстных целях», — отметил Том Келлерманн, руководитель департамента по разработке стратегии кибербезопасности компании VMware.

Согласно отчету, в прошедшем году специалисты по информационной безопасности чаще сталкивались с психологическими проблемами и давлением из-за завышенных ожиданий от результатов работы. Так, 51% респондентов отметили, что долгое время находились в состоянии стресса или столкнулись с профессиональным выгоранием.

«Выгорание — огромная проблема для ИБ-подразделений компаний. Сейчас специалисты вынуждены бороться с резким ростом числа атак в непростых условиях – в режиме удаленной работы. В такой ситуации руководители организаций должны уделять еще больше внимания эмоциональному состоянию своих сотрудников, способствуя их личностному росту и развитию», — заявил Рик МакЭлрой, ведущий специалист по вопросам стратегии в области кибербезопасности компании VMware.

Ключевые результаты исследования Global Incident Response Threat Report, 2021.

Злоумышленники объединяются ради большого выкупа: 64% респондентов, которые столкнулись с атаками программ-вымогателей, отметили, что это были объединенные усилия нескольких хакерских группировок. Представители ИБ-команд ищут новые способы реагирования на подобные угрозы — 81 % опрошенных отметили, что в течение года повысят уровень активных средств безопасности.

Атаки становятся более разрушительными и целенаправленными: респонденты указывают, что более чем 50% кибератак сегодня направлены на разрушение целостности данных или вовсе их уничтожение. 60% респондентов заявили, что преступники используют новые технологии, включая манипулирование временными метками — или Chronos-атаки. Кроме того, в связи с переходом на удаленную работу, 32% опрошенных отметили рост BEC-атак (Business Email Compromise), когда злоумышленники используют методы социальной инженерии для компрометации деловой переписки.

Защита облачных сред – в приоритете: стремительный переход к облачным технологиям во время пандемии спровоцировал рост атак на облачные среды. Почти половина (43%) респондентов заявили, что более трети всех атак были направлены на рабочие нагрузки, размещенные в облаке, в то время как 22% опрошенных сталкивались с подобными атаками еще чаще — при каждом втором инциденте. В этой связи 6 из 10 респондентов считают, что внедрение инструментов для обеспечения безопасности облачных сред — главный приоритет сегодня». ***(Исследование: 51% ИБ-специалистов чаще испытывают профессиональное выгорание в связи с участившимися кибератаками // CNews (https://safe.cnews.ru/news/line/2021-08-12_issledovanie_51_ibspetsialistov). 12.08.2021).***

***

**«Рынок киберпреступности эволюционировал и изменился за последний год из-за пандемии. Хакеры начали наводнять рынок, пытаясь быстро заработать на людях и организациях, которые не создали надежную систему безопасности.**

Согласно недавним выводам исследовательской группы Atlas VPN, 45% доступа к корпоративной сети в даркнете стоит менее 1 тыс. долларов. Компании, работающие в сфере услуг и тяжелой промышленности, являются основными целями для хакеров при планировании

Данные основаны на исследовании Criminal Market for Initial Access, опубликованном в Positive Technologies. В отчете провайдер решений безопасности проанализировал, как эволюционировал криминальный рынок в течение 2020 года и начала 2021 года.

45% предложений доступа к корпоративным сетям, размещенных хакерами в даркнете, стоит менее чем 1000 долларов. Важно отметить, что этот процент в 2017 году составлял всего 15%. Однако между вторым кварталом 2020 года и первым кварталом 2021 года показатель вырос до нынешнего уровня.

Ключи доступа к корпоративным сетям, которые стоят от $1000 и до $2499 составили 22% черного рынка даркнета.

Как правило, стоимость доступа зависит от нескольких факторов. Хакеры оценивают количество компьютеров, которые будут раскрыты, привилегии учетной записи, размер бизнеса, доход и другие финансовые показатели. Кроме того, на цену доступа может повлиять отрасль, в которой работает компания.

Доступ к корпоративным сетям, продаваемый за $ 5000 - $ 9,999 составляет 9% черного рынка даркнета. В то же время доступы, предлагаемые выше ценового диапазона $ 10 000, составили 7% рынка.

*Наиболее ценные отрасли*

Хакеры считают некоторые отрасли более ценными, чем другие, потому что некоторые предприятия в определенных секторах вкладывают меньше ресурсов в кибербезопасность, что делает их более легкой мишенью.

Сфера услуг является самой популярной среди киберпреступников, так как 17% выбрали эту отрасль. Обычно компании этой отрасли имеют много конфиденциальных данных о своих клиентах. Из-за этого сервисные предприятия становятся прибыльными целями для хакеров, поскольку они могут продавать украденную информацию в Интернете.

Далее идет производственный сектор, выбранный 14% хакеров. Получив доступ к производственному бизнесу, киберпреступники могут украсть личную информацию и серьезно нарушить рабочий процесс предприятия. Нарушенные процессы негативно сказываются на производстве, что может привести к потере доходов на несколько недель.

Кроме того, 12% киберпреступников даркнета выбрали для атаки исследовательскую и образовательную отрасль. Поскольку небольшие школы обычно не имеют хорошей системы безопасности и злоумышленники считают их более легкой добычей.

Кроме того, IT- отрасль стала мишенью для 7% злоумышленников, которые приобрели доступ к корпоративной сети. У IT-компаний больше возможностей для атак, поскольку они используют множество устройств, подключенных к Интернету. Чем больше устройств, тем больше уязвимостей могут использовать хакеры.

Наконец, на все другие отрасли приходится 26% посещений, проданных на форумах в даркнете.

Доступы по низким ценам обычно продаются неопытными хакерами, которые могут даже не довести дело до конца. Несмотря на это, рост доли дешевого доступа означает, что на рынок вышло много новых, менее квалифицированных киберпреступников, и они могут стать более опасными в будущем». ***(Романов Роман. Отчет: 45% предложений взломанного доступа к корпоративным сетям продаются ниже 1 тыс. долларов в даркнете // Internetua (http://internetua.com/otcset-45-predlojenii-vzlomannogo-dostupa-k-korporativnym-setyam-prodauatsya-nije-1-tys-dollarov-v-darknete). 12.08.2021).***

***

**«У Німеччині хакерських атак за рік зазнали 86% компаній – майже 9 з 10. Про це повідомило Федеральне об'єднання підприємств цифрової економіки, телекомунікації та нових медіа Bitkom…**

Зокрема, за останні два роки різко зросла кількість випадків шантажу з боку хакерів, які блокують інформаційні та виробничі системи компаній.

Bitkom опитало понад 1000 компаній з різних галузей, які стали жертвами хакерських атак.

У 40% випадків кібератак, за оцінкою постраждалих компаній, діяли «любителі», у 29% – організовані угрупування. 42% фірм повідомили, що кібератаки були можливі через ненавмисні помилкові дії співробітників, а ще у 28% співробітники навпаки навсмисно наносили збитки компаніям.

43% компаній-учасників опитування заявили, що постраждали від кіберзлочинців, які перебували в Німеччині, 37% – були атаковані з країн Східної Європи (без урахування РФ), 30% – з Китаю, 23% – з РФ, 16% – з США. 31% компаній заявили, що не змогли встановити регіон розташування хакерів.

Збитки для економіки країни від кібератак протягом 2020-2021 років склали €223 млрд. Для порівняння, у 2018-2019 років цей показник дорівнював €103 млрд, тоді постраждали 75% компаній». ***(У Німеччині від хакерів з 2020 року постраждали 86% компаній. Збитки від цього склали €223 млрд // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/27938/2021-08-05-u-nimechchyni-vid-khakeriv-z-2020-roku-postrazhdaly-86-kompaniy-zbytky-vid-tsogo-sklaly-223-mlrd/). 05.08.2021).***

***

**«Користувачі Twitter повідомили про масовий злам сторінок «Вікіпедії», на яких хакери розмістили зображення свастики. Замість сторінок – червоний фон і нацистський символ.**

Доступ до сторінок швидко відновили, але користувачі онлайн-енциклопедії встигли помітити зміни. Вони відзначили, що додавання нацистського прапора немає в історії правок статей. Фонд «Вікімедіа» поки ніяк не прокоментував ситуацію.

«Сьогодні вранці я відвідав Вікіпедію і це був червоний фон зі свастикою на всю сторінку. Врешті-решт все повернулось до норми, але не видно жодних змін. У мене є скриншот, але я не хочу його публікувати, тому що це свастика. Хтось ще бачив щось подібне?» – написав користувач.

Серед сторінок відомих людей, які зламали – Роберт Дюваль, Брюс Спрінгстін, Пеле, Джоан Роулінг, Роберт Дауні-молодший, Йосип Сталін, Емінем, Стівен Пінкер, Теодор Адорно, Дженніфер Лопез, Бен Аффлек, Мадонна та багато-багато інших…» ***(Невідомі зламали «Вікіпедію» та замінили сторінки тисяч знаменитостей свастикою (ФОТО) // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/27995/2021-08-16-nevidomi-zlamaly-vikipediyu-ta-zaminyly-storinky-tysyach-znamenytostey-svastykoyu-foto/). 16.08.2021).***

***

**«В ходе анализа порядка 1 тыс. объявления на хакерских биржах выяснилось, что чаще всего продают доступы к американским, а также французским, английским, австралийским и канадским компаниям.** Самый дорогостоящий лот из обнаруженных достигал 12 биткоинов (примерно $540 тыс.).

В ходе исследования были изучены объявления о продаже начального доступа к внутренним компьютерным сетям взломанных организаций, опубликованные с июля 2020 по июнь 2021 года. Средняя цена лота составила около $5,4 тыс., медианная (половина предложений ниже показателя, половина — выше) — $1 тыс., сообщили «Известия» со ссылкой на исследование израильской компании Kela.

Под доступом подразумевается логин и пароль от аккаунта сотрудника организации, который открывает для киберпреступников вход в компьютерную инфраструктуру компании. Также как доступ может продаваться программное обеспечение для эксплуатации уязвимостей в сети жертвы.

Эксперты отметили, что ценообразование зависит от выручки взломанной компании. Поэтому доступы к небольшим фирмам стоят $100–200, а самые дорогие лоты оцениваются в тысячи раз больше.

Топ-3 лотов по стоимость выглядит следующим образом:

Самая высокая цена, которая встретилась экспертам, была равна 12 биткоинам (примерно $540 тыс. по курсу на 18 августа). Столько просили за доступ к неназванной австралийской компании с годовым доходом $500 млн;

Второй по дороговизне доступ стоил 5 биткоинов (примерно $225 тыс.). За эту сумму продавался аккаунт в системе удаленного доступа к рабочему столу ConnectWise Control из сети одной из американских IT-компаний;

Тройку самых дорогих доступов замкнул лот за $100 тыс., обещавший проход в сеть некоего правительственного ведомства Мексики.

По данным аналитиков, аккаунты с правами администратора на хакерских форумах в среднем стоят в 10 раз больше, чем доступ с правами рядового пользователя.

В Kela составили рейтинг стран, доступы к компаниям из которых чаще всего продают в даркнете:

С большим отрывом топ возглавили США: американских организаций касается 27,9% объявлений;

На второй строчке — Франция с показателем 6,1%;

Следом идут Великобритания и Австралия с долями по 4%;

Пятерку лидеров замкнула Канада с результатом 3,8%;

Италия (3,5%);
Бразилия (3,2%);
Испания и Германия (по 2,3%);
ОАЭ (2%).

Россия и страны СНГ могли не войти в топ-10, поскольку на русскоязычных хакерских форумах не принято работать с местными компаниями, подчеркивается в исследователи». ***(Денис Савосин. Средняя цена доступа к взломанной компании на хакерских биржах составила $5,4 тыс. // ООО "РБ.РУ" (https://rb.ru/news/cybercrime-market-price/). 20.08.2021).***

***

**«Количество кибератак во всем мире во втором квартале 2021 года увеличилось на 0,3% по сравнению с первым кварталом.** При этом доля атак на компании, связанных с получением финансовой выгоды, выросла на 16%. Чаще всего киберпреступники атаковали медицинские и государственные учреждения и промышленный сектор.

Кроме того, доля атак, направленных на компрометацию компьютеров, серверов и сетевого оборудования, выросла с 71% до 87%, что связано с ростом количества атак с использованием программ-вымогателей, сообщил ТАСС со ссылкой на исследование Positive Technologies.

В ходе исследования выяснилось, что с 12% до 20% выросла доля атак на госучреждения среди всех атак, нацеленных на организации. С 63% до 76% увеличилась доля мошенничества с применением вредоносного программного обеспечения (ПО). В 73% случаев киберперступники использовали шифровальщики, в 16% — вредоносное ПО для удаленного управления.

Также выросла до 73% (+6 п. п.) доля атак на промышленные предприятия с использованием вредоносного ПО. Относительно 2020 года наблюдается и увеличение доли хакинга с 29% до 34%. В 80% случаев в данной отрасли использовались вредоносы.

По данным экспертов, доля атак на торговые сети с использованием вредоносного ПО среди прочих методов атак выросла с 26% до 59%. Доля социальной инженерии, когда киберперступники используют манипуляцию и психологические уловки для получения персональных данных клиентов и доступа к их деньгам, также выросла с 36% в первом квартале до 53% во втором квартале 2021 года.

По данным Positive Technologies, доля атак на частных лиц сохранилась на уровне первого квартала и составила 12%. Чаще всего мотивом служило получение персональных данных жертв. Доля атак с такой целью выросла на 9 п. п., до 78%. Также более чем на 50% увеличилось количество похищенных платежных данных.

Доля атак, направленных на компании, с использованием вредоносного ПО выросла на 15 п. п., до 73%. Самым популярным вредоносным ПО остаются программы-вымогатели, которые блокируют доступ к компьютеру или не дают считывать данные, а затем требуют от потерпевшего выкуп за разблокировку. Доля атак с использованием вымогателей выросла до 69% с 63%.

Электронная почта по-прежнему остается основным каналом для распространения вредоносного софта в атаках на компании (58%).

В инцидентах с частными лицами чаще всего киберпреступники распространяли банковские трояны (30%), вредоносы для удаленного управления (29%) и шпионское ПО (27%), а также использовали программы-шифровальщики (9%).

Аналитики назвали самые популярные программы-вымогатели:

REvil;

Avaddon;

DoppelPaymer;

PayOfGrief;

Conti (Ryuk).

Исследование показало, что 36% украденных данных в атаках на организации составили персональные данные, 23% — учетные данные, 22% — коммерческая тайна, 8% — медицинская информация, 3% — базы данных клиентов, данные платежных карт и переписка, 2% — на другую информацию.

В то же время в атаках на частные лица было украдено 55% учетных данных, 17% персональных данных, 13% данных платежных карт, 11% переписок, 4% пришлось на иные данные». ***(Денис Савосин. Количество кибератак в мире во втором квартале выросло на 0,3% — исследование // ООО "РБ.РУ" (https://rb.ru/news/cybercrime-in-world-research/). 30.08.2021).***

***

**«Одна из последних китайских кибератак на серверы Microsoft Exchange могла быть связана не только с кибершпионажем, но и с исследованиями в области искусственного интеллекта. Чаще всего атаки нацелены на сбор конфиденциальной информации, и при изменении стратегии Китай может использовать любые полученные данные для поддержки исследований в области ИИ.**

В ходе одной из последних атак на Microsoft Exchange хакеры смогли проникнуть на серверы различных предприятий и украсть конфиденциальные файлы и электронные письма. Как сообщила некоммерческая организация National Public Radio (NPR), в ходе взлома хакеры запрашивали файлы, которые при нормальных обстоятельствах их не интересуют. За этими атаками стояла группировка Hafnium, обычно атакующая медицинские компании, школы и государственные учреждения.

Группировка взломала локально администрируемые серверы компаний и предприятий, проэксплуатировав уязвимости в коде сервера, что позволило им взломать систему и в конечном итоге перехватить контроль над ней. Затем киберпреступники запрограммировали локальные серверы на рассылку информационных запросов для различных персональных и конфиденциальных файлов. Таким образом, если сервер получает запрос от другого доверенного сервера, он предоставит информацию без каких-либо возражений.

В последние несколько лет Китай уделяет все больше внимания развитию искусственного интеллекта. Для разработки высокотехнологичного искусственного

интеллекта необходимы реальные данные, которые будут использоваться в алгоритмах. В этих атаках именно такие данные и были доступны хакерам. Как отметили специалисты, учитывая объем похищенной информации, этого вполне достаточно для создания искусственного интеллекта в Китае. Конкретные цели Китая в отношении развития искусственного интеллекта пока неизвестны и, вероятно, останутся такими». ***(Атаки китайских хакеров на Microsoft Exchange могут быть связаны с исследованиями ИИ // SecurityLab.ru (https://www.securitylab.ru/news/523826.php). 27.08.2021).***

***

**«Специалисты в области кибербезопасности из FortiGuard Labs опубликовали полугодовой отчет о глобальных угрозах за 2021 год. В первые шесть месяцев 2021 года значительно увеличилось количество и сложность атак, нацеленных на отдельных лиц, организации и критически важную инфраструктуру.**

В прошлом году злоумышленники переключили свое внимание с устройств корпоративной инфраструктуры на домашние сети и продукты потребительского уровня. Однако теперь они активно атакуют как малый бизнес и технологии потребительского уровня, так и корпоративные сети и платформы управления контентом и разработки приложений (CMS).

Еще одна тенденция, выявленная FortiGuard Labs за последние шесть месяцев, заключается в резком увеличении количества атак. К середине года процент организаций, обнаруживающих в своих сетях активность ботнетов, подскочил с 35% до 51%. Данные изменения связаны с более частым использованием вредоноса TrickBot. TrickBot изначально был разработан как банковский троян, но с течением времени превратился в сложный, модульный и многоэтапный инструмент для осуществления различных незаконных действий. Mirai остается наиболее распространенным ботнетом, обогнав Gh0st в начале 2020 года, и продолжает пополнять свой арсенал новым кибероружием.

Количество программ-вымогателей за последние 12 месяцев увеличилось более чем в десять раз. Частично это связано с ростом популярности бизнес-модели «Вымогательское-ПО-как-услуга» (Ransomware-as-a-Service, RaaS). Помимо аренды программ-вымогателей, некоторые операторы начали продавать доступ к взломанным корпоративным сетям, упростив работу преступникам без особых технических навыков.

Но возросло не только количество атак программ-вымогателей, но и агрессивность их операторов. Киберпреступники применяют новые рычаги давления на своих жертв. Это включает сочетание шифрования файлов с доксингом (угрозой публикации внутренних данных в общем доступе), добавление DDoS-атаки для создания дополнительной путаницы и паники, а теперь и непосредственное обращение к клиентам и партнерам жертвы или даже СМИ.

FortiGuard Labs отметила устойчивый интерес злоумышленников к выявлению уязвимостей в системах операционных технологий и последующему их использованию в своих эксплоитах. В связи с этим незащищенные OT-устройства могут обнаружить как APT-группировки, специализирующиеся на атаках на АСУ

ТП, так и начинающие киберпреступники». ***(Эксперты сообщили о десятикратном увеличении числа программ-вымогателей // SecurityLab.ru (https://www.securitylab.ru/news/523686.php). 24.08.2021).***

***

**«Журналистка телеканала Fox News Джеки Хайнрик со ссылкой на свой источник, заявила о том, что на Государственный департамент США была совершена кибератака.**

«Государственный департамент подвергся кибератаке», — написала журналиста. Она добавила, что хакерская атака, возможно, произошла «пару недель назад».

Журналистка заявила, что киберкомандование Пентагона направило уведомление о возможном серьезном взломе. При этом она уточнила, что масштабы хакерской атаки, как и масштаб расследования против предполагаемых преступников, «остаются неясными». Также неизвестно, какие меры были предприняты для смягчения последствий кибератаки, и каковы «текущие риски для операций».

Представители Госдепартамента США отказались комментировать сообщения о возможной хакерской атаке. В ведомстве заявили, что они серьезно относятся к защите информации и постоянно предпринимают меры для обеспечения безопасности данных. По соображениям безопасности мы не в состоянии обсуждать характер или масштабы любых предполагаемых инцидентов кибербезопасности в настоящее время, — заявили власти США». ***(Fox News: Госдеп США подвергся хакерской атаке // SecurityLab.ru (https://www.securitylab.ru/news/523615.php). 22.08.2021).***

***

## *Діяльність хакерів та хакерські угруповування*

---

**«Хакерське угруповання APT31 (воно ж Hurricane Panda або Zirconium), яку пов'язують зі спецслужбами Китаю, вперше атакувала російські компанії, повідомили російському агентству РБК в компанії Positive Technologies.**

Зазначається, що китайські хакери здійснили близько десятка шкідливих розсилок в Монголії, США, Канаді та Білорусі. Хакерські атаки провели й на російські компанії, однак в Positive Technologies не назвали їх кількість пославшись на конфіденційність.

Експерти кажуть, що китайські хакери застосовують нові способи злому і зараження електроніки - кіберзлочинці розсилають фішингові імейли з посиланнями на підставний домен, що повністю імітує держоргани. Після кліка на таке посилання, в девайс проникає троян віддаленого доступу. Він створює зараженому пристрої шкідливу бібліотеку та встановлює спеціальний застосунок. Він вже, своєю чергою, запускає функцію керування пристроєм». ***(Китайські хакери атакували компанії з Росії – РосЗМІ // Дзеркало тижня. Україна***

***(https://zn.ua/ukr/WORLD/kitajski-khakeri-atakuvali-kompaniji-z-rosiji-rossmo.html). 03.08.2021).***

***

**«Поставщик средств безопасности FireEye заявляет, что он обнаружил китайскую шпионскую группу, которая успешно взламывала цели в Израиле, и что попытки сделать ее усилия похожими на работу иранских актеров являются частью образа действий этой группы.**

В сообщении в блоге FireEye говорится, что китайская деятельность ведется с 2019 года, когда группа под названием «UNC215» использовала уязвимость Microsoft SharePoint CVE-2019-0604 «для установки веб-оболочек и полезных нагрузок FOCUSFJORD на цели на Ближнем Востоке и в Центральной Азии».

«Помимо данных, полученных от Mandiant Incident Response и телеметрии FireEye, мы работали с израильскими оборонными агентствами над проверкой данных о дополнительных взломах израильских организаций», - говорится в сообщении. «Этот анализ показал множественные одновременные операции против израильских правительственных учреждений, поставщиков ИТ и телекоммуникационных компаний, начиная с января 2019 года».

UNC215 изменил тактику, методы и процедуры (TTP) в ходе своей продолжающейся кампании, но он постоянно любит устанавливать веб-оболочки и атаковать Exchange и Outlook Web Access, а также был замечен кражей учетных данных для выполнения своей неприятной работы.

«После определения ключевых систем в целевой сети, таких как контроллеры домена и серверы Exchange, UNC215 переместился в сторону и развернул свою сигнатурную вредоносную программу FOCUSFJORD», - написали в группе безопасности FireEye. «UNC215 часто использует FOCUSFJORD на начальных этапах вторжения, а затем развертывает HYPERBRO, который имеет больше возможностей сбора информации, таких как захват экрана и клавиатурный шпион».

Группа также пытается замести следы, стирая вредоносное ПО, но также может нагло и повторно использовать код или повторно посещать жертв.

В одном случае FireEye заметил, что «оператор неоднократно и нечасто повторно посещал скомпрометированную сеть всякий раз, когда инструмент Endpoint Detection and Response обнаруживал или помещал в карантин такие инструменты, как HYPERBRO и Mimikatz. После нескольких месяцев повторных обнаружений UNC215 развернул обновленную версию HYPERBRO и инструмент под названием 'anti.exe', чтобы остановить службу Центра обновления Windows и прекратить работу служб, связанных с EDR и антивирусом».

UNC215 также прокладывает ложный след в Иран, используя его официальный язык фарси в некоторых строках. Некоторые пути к файлам включают каталоги с именем / Iran.

FireEye без колебаний объясняет деятельность группы «постоянным стратегическим интересом Китая на Ближнем Востоке.

«Эта кибершпионаж происходит на фоне многомиллиардных инвестиций Китая, связанных с инициативой «Один пояс, один путь» (BRI), и его интереса к высокоразвитому технологическому сектору Израиля», - говорится в сообщении.

«Китай провел многочисленные кампании вторжений вдоль маршрута BRI для отслеживания потенциальных препятствий - политических, экономических и безопасности - и мы ожидаем, что UNC215 продолжит нацеливаться на правительства и организации, участвующие в этих критически важных инфраструктурных проектах в Израиле и на Ближнем Востоке в целом в ближайшем будущем. - и в среднесрочной перспективе».

Все это оставляет одну из самых ярких горячих точек в мире, связанных с продолжающимися наступательными кибероперациями Китая, помимо множества других геополитических сложностей». ***(Simon Sharwood. Chinese espionage group targets Israel while suggesting the source could be Iran // The Register (https://www.theregister.com/2021/08/11/china_unc215_israel_attacks/). 11.08.2021).***

***

**«Анонімна група білоруських «Кіберпартизан» стверджує, що зламала паспортну систему країни. У розпорядженні хакерів, за їхніми словами, виявилися дані мільйонів білорусів, включаючи «приховані записи» про керівництво силових структур, людей з близького оточення Олександра Лукашенка, співробітників КДБ і розвідників в Євросоюзі.**

Частину інформації хакери виклали в Telegram. Зокрема, паспортні дані Олександра Лукашенко та його сина Миколи, голови ЦВК Білорусі Лідії Ермошиної, голови Ради Республіки Наталії Качанової, глави КДБ Івана Тертелі і колишнього президента Киргизстану Курманбека Бакієва (переїхав до Мінська після революції у себе в країні в 2010 році).

Джерело даних – інформаційна система «Паспорт». Видання «Настоящее время» провело експеримент, щоб переконатися, що у «Кіберпартизан», ймовірно, є інформація про більшість білорусів. Журналісти надали імена та дати народження людей, які зголосилися брати участь в експерименті – та за кілька хвилин отримали повне досьє, включаючи кілька фото з паспортів, які були зроблені з різницею в кілька років і ніколи не публікувалися в інтернеті, та технічну інформацію (наприклад, про те, що в паспорті закінчилося місце для вклеювання віз).

Влада Білорусі, КДБ і НПООО «Тодес», яке створило інформаційну систему, не коментують кіберінцидент.

Крім бази паспортів, в руках хакерів опинилися дані ДАІ Білорусі, база даних служби 102, дані з камер спостереження в ізоляторах тимчасового тримання тощо.

Використання шкідливих програм в Кримінальному кодексі Білорусі карається строком до 10 років, а несанкціонований доступ до комп'ютерної інформації – до двох років…». **(Білоруські «Кіберпартизани» заявили, що зламали паспортну систему країни // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/27911/2021-08-03-biloruski-kiberpartyzany-zayavyly-shcho-zlamaly-pasportnu-systemu-krainy/). 03.08.2021).**

***

**«Общественный штаб по наблюдению за выборами в столице объявил о поиске хакера, которому во время тестирования системы онлайн голосования 29-30 июля удалось обойти ее алгоритм**

Как сообщили в Штабе, специалист, войдя в систему, смог отказаться от одного из двух бюллетеней. Это действие аналогично порче бумажного бюллетеня при голосовании «вживую». Тем самым программист помог разработчикам системы найти пробел в ПО.

Для получения вознаграждения программист должен прислать разработчикам описание кейса с кодом, который он использовал, чтобы получить один бюллетень из двух. Это поможет им устранить возможные «бреши» в алгоритме и повысить надежность системы. Аналогичные объявления общественный штаб опубликовал в Facebook, Twitter, Instagram и «ВКонтакте».

150 тысяч, которые обещают выплатить взломщику, стали частью призового фонда в миллион рублей. Деньги выделили хакерам — участникам электронного голосования для поиска уязвимостей системы». ***(Московские власти ищут взломщика системы онлайн-голосования // SecurityLab.ru (https://www.securitylab.ru/news/523614.php). 22.08.2021).***

***

**«Исследователи безопасности ИБ-компании Volexity зафиксировали атаки известной северокорейской хакерской группировки на ограниченный круг жертв с использованием эксплоитов для уязвимостей в web-браузере и нового вредоносного ПО.**

Хакерская группировка под названием InkySquid сумела взломать новый сайт в Южной Корее и внедрить в него вредоносный код. Данный эксплоит используется с 2020 года в атаках на браузер Internet Explorer с целью загрузки обфусцированного Javascript-кода, скрытого внутри легитимного кода.

Вышеописанная техника также использовалась для атак на пользователей устаревшего браузера Edge первого поколения, но через более новую уязвимость, которая также присутствует в Internet Explorer.

В обоих случаях Javascript расшифровывается в версию инструмента Cobalt Strike, после чего загружается вредоносное ПО второго этапа под названием BLUELIGHT.

BLUELIGHT представляет собой семейство вредоносного ПО для поиска и похищения информации, настроенного хакерами таким образом, чтобы использовать разных облачных провайдеров и C&C-серверов.

В операциях BLUELIGHT хакеры использовали API Microsoft Graph для Microsoft 365, Office и других сервисов.

По мнению Volexity, за атаками InkySquid стоит северокорейская хакерская группировка, также известная как ScarCruft или APT37. Группировка активна с 2012 года и атакует в основном предприятия в Южной Корее и других странах Азии и Среднего Востока». ***(Северокорейская APT-группа InkySquid атакует жертв через уязвимости в браузерах Microsoft // SecurityLab.ru (https://www.securitylab.ru/news/523557.php). 19.08.2021).***

***

**«Связанные с правительством Ирана хакеры атакуют израильские телекоммуникационные и IT-компании с целью подобраться ближе к интересующим их жертвам.**

Речь идет о APT-группе, известной под названиями Lyceum, Hexane и Siamesekitten, которая проводит свои операции как минимум с 2018 года. В ходе серии атак в мае и июле 2021 года хакеры совмещали приемы социальной инженерии с использованием обновленного вредоносного ПО для удаленного доступа к зараженным системам.

Как сообщили специалисты из ClearSky, для заражения компьютеров потенциальных жертв вредоносным ПО хакеры предлагали им работу с подставных профилей. Сначала они находили подходящую кандидатуру на роль жертвы (сотрудника) и сотрудника отдела кадров, за которого можно было себя выдать. Затем злоумышленники создавали поддельный сайт, выдаваемый за легитимный сайт атакуемой организации, и заводили подставной профиль от имени сотрудника отдела кадров.

Далее жертва направлялась на поддельный сайт, содержащий вредоносный файл. Бэкдор в файле заражал ее компьютер и подключался к C&C-серверу через DNS и HTTPS, после чего на инфицированную систему загружался троян для удаленного доступа (RAT) DanBot. Хакеры собирали интересующие их данные и пытались продвинуться далее по сети.

По словам специалистов из ClearSky, группировка потратила месяцы на попытки взломать большое количество организаций в Израиле с помощью инструментов цепочки поставок.

Хотя создается впечатление, будто Lyceum переключила свое внимание со Среднего Востока и Африки на Израиль, на самом деле группировка атаковала израильские компании с целью подобраться ближе к истинным мишеням через цепочку поставок, уверены эксперты». ***(Иранские хакеры выдают себя за HR-менеджеров в атаках на израильские компании // SecurityLab.ru (https://www.securitylab.ru/news/523501.php). 18.08.2021).***

***

**«Разрушительные атаки, нацеленные на министерство транспорта Ирана и национальную железнодорожную систему, были организованы киберпреступной группировкой Indra.** По словам экспертов из Check Point Research, группировка ранее осуществляла атаки на ряд сирийских организаций и заражала их системы вредоносным ПО.

В прошлом месяце министерство железных дорог и транспорта Ирана подверглось кибератаке с использованием вайпера, в результате которой были отключены web-сайты ведомства и нарушено движение поездов по всей стране.

«Было установлено, что атаки на Иран тактически и технически схожи с предыдущими действиями киберпреступников против нескольких частных компаний в Сирии, которые осуществлялись как минимум с 2019 года. Нам удалось связать эту деятельность с группировкой Indra, которая идентифицирует себя как оппозиционная группа, противостоящая иранскому режиму», — сообщили исследователи.

Злоумышленники применили неизвестный ранее вайпер под названием Meteor на системах жертв в Иране. Хакеры разместили сообщения на досках объявлений железнодорожной системы об отмене и задержке поездов, и просили пассажиров обратиться в офис Верховного лидера Али Хаменеи за дополнительной информацией.

Indra разработала и использовала в атаках как минимум три различных варианта вайпера: Meteor, Stardust и Comet. Вайперы, получившие общее название Nuke-it-From-Orbit-ware, предназначены для уничтожения данных или вызова сбоя в работе взломанных устройств». ***(Атаковавшая министерство транспорта Ирана группировка связана с атаками на Сирию // SecurityLab.ru (https://www.securitylab.ru/news/523429.php). 17.08.2021).***

***

## *Вірусне та інше шкідливе програмне забезпечення*

**«Недавно эксперты по кибербезопасности сообщили о появлении нового, невероятно опасного компьютерного вируса, который угрожает смартфонам украинцев.** Он способен украсть пароли от личных кабинетов таких банковских приложений, как Приват24 и monobank. Хуже того — распространяется этот вирус через Google Play. Как же не стать его жертвой?

Вирус был обнаружен несколько дней назад специалистами по кибербезопасности из Нидерландов. Он носит название Vultur и является так называемой «троянской» программой, которая способна считывать информацию прямо с экранов смартфонов. В первую очередь он рассчитан на воровство паролей от банковских карточек, а также криптовалютных кошельков.

Новый вирус является очень продвинутым. Он способен делать скриншоты, отправлять разработчикам big data, а также анализировать приложения, установленные на смартфоне, чтобы выяснить, насколько активно владелец зараженного гаджета пользуется программами онлайн-банкинга. Профессиональные навыки создателей Vultur таковы, что ими восхищаются даже разработчики антивирусного программного обеспечения. Скорее всего, за троянским приложением стоит кто-то из их коллег, переметнувшихся на «тёмную сторону».

По словам экспертов, кража данных от криптокошельков и программ онлайн-банкинга с помощью сканирования экрана — невероятно быстрый и эффективный метод. На всё про всё у трояна уходит всего лишь несколько секунд. Жертва даже не успевает понять, что подверглась атаке, и тем более не успевает среагировать надлежащим образом. Полученными данными хакеры, создавшие приложение, могут в любой момент — например, они могут подождать, когда жертва получит заработную плату, чтобы украсть как можно больше.

Хуже всего то, что распространяется приложение через Google Play, который многие все еще считают безопасным. Как теперь понятно, это не так. Поэтому лучшим способом защиты от вирусов является отказ от скачивания непонятных

приложений — пользоваться нужно только официальными версиями от известных разработчиков, которые дорожат своей репутацией.

Также важно следить за тем, чтобы у вас на смартфоне всегда был антивирус с самыми актуальными на данный момент базами зловредных программ». ***(В Google Play нашли вирус, крадущий пароли от Приват24 и Monobank // Украина криминальная (https://cripo.com.ua/news/crime/v-google-play-nashli-virus-kradushhij-paroli-ot-privat24-i-monobank/). 09.08.2021).***

***

**«Финансово мотивированная банда киберпреступников взломала и заблокировала сеть финансовой организации США с помощью нового вредоносного ПО, получившего название Sardonic от исследователей Bitdefender, которые первыми его заметили.**

FIN8, инициатор угрозы, стоящий за этим инцидентом, был активен по крайней мере с января 2016 года и известен своей нацеленностью на розничную торговлю, ресторан, гостиничный бизнес, здравоохранение и развлечения с конечной целью кражи данных платежных карт из POS-систем.

Злонамеренный арсенал Этой угрозы актера включает в себя широкий ассортимент инструментов и тактики, начиная от POS вредоносных программ (например, BadHatch, PoSlurp / PunchTrack, PowerSniff / PunchBuggy / ShellTea) для ОС Windows нулевого дня подвигов и копья-фишинга.

С тех пор, как FireEye впервые обнаружил их, FIN8 организовал несколько крупномасштабных, но спорадических кампаний, затронувших сотни организаций.

*Бэкдор все еще находится в разработке*

Sardonic - это новый бэкдор на основе C ++, который злоумышленники FIN8 развертывают в системах целей, вероятно, с помощью социальной инженерии или целевого фишинга, двух излюбленных методов атак группы.

Пока вредоносная программа все еще находится в стадии разработки, ее функциональные возможности включают:

Сбор системной информации.

Выполнение команд на взломанных устройствах.

И система плагинов, предназначенная для загрузки и выполнения дополнительных вредоносных программ, поставляемых в виде библиотек DLL.

Во время атаки на банк США бэкдор был развернут и запущен в системах жертв как часть трехэтапного процесса с использованием сценария PowerShell, загрузчика.NET и шелл-кода загрузчика.

Как заметили исследователи Bitdefender, сценарий PowerShell вручную копируется на скомпрометированные системы, а загрузчики доставляются на скомпрометированные устройства с помощью автоматизированного процесса.

Операторы FIN8 также несколько раз пытались установить бэкдор Sardonic на контроллеры домена Windows для повышения привилегий и горизонтального перемещения по сети организации.

*Потенциальные цели предупреждены о бдительности*

Bitdefender призывает организации, подверженные риску стать мишенью FIN8 (в первую очередь, финансовые, розничные и гостиничные организации),

быть начеку и проверять свои сети на предмет известных индикаторов компрометации FIN8.

«FIN8 продолжает укреплять свои возможности и инфраструктуру доставки вредоносного ПО. Известно, что высококвалифицированный субъект финансовых угроз делает длительные перерывы, чтобы усовершенствовать инструменты и тактику, чтобы избежать обнаружения, прежде чем он поразит жизнеспособные цели», - заключили исследователи Cyber Threat Intelligence Lab.

«Bitdefender рекомендует компаниям в целевых вертикалях (розничная торговля, гостиничный бизнес, финансы) проверять наличие потенциального компромисса, применяя [IoC] к своим EDR, XDR и другим средствам защиты».

Дополнительные сведения о внутренней работе Sardonic и индикаторах взлома (IOC), включая информацию об инфраструктуре и хэши вредоносных программ, можно найти в конце официального документа Bitdefender». ***(Sergiu Gatlan. FIN8 cybercrime gang backdoors US orgs with new Sardonic malware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fin8-cybercrime-gang-backdoors-us-orgs-with-new-sardonic-malware/). 25.08.2021).***

***

**«Киберпреступники, стоящие за вредоносным ПО BazaLoader, придумали новую приманку, чтобы обманом заставить владельцев веб-сайтов открывать вредоносные файлы: поддельные уведомления о том, что сайт участвует в распределенных атаках типа «отказ в обслуживании» (DDoS).**

Сообщения содержат юридическую угрозу и файл, хранящийся в папке Google Диска, который якобы предоставляет доказательства источника атаки.

*Поддельные юридические угрозы*

Тема DDoS - это разновидность другой приманки, жалобы о нарушении Закона о защите авторских прав в цифровую эпоху (DMCA) со ссылкой на файл, который предположительно содержит доказательства кражи изображений.

В сообщениях, которые видел BleepingComputer, злоумышленник использовал URL-адреса Firebase для загрузки BazaLoader. Однако цель та же: используйте контактные формы для доставки вредоносного ПО BazaLoader, которое часто сбрасывает Cobalt Strike, что может привести к краже данных или атаке программы-вымогателя.

Microsoft предупредила об этом способе доставки в апреле, когда киберпреступники использовали его для доставки вредоносного ПО IcedID. Недавние кампании похожи, только изменились грузоподъемность и приманка.

Разработчик и дизайнер веб-сайтов Брайан Джонсон на прошлой неделе сообщил, что два его клиента получают официальные уведомления о взломе их веб-сайтов с целью проведения DDoS-атак против крупной компании (Intuit, Hubspot).

Отправитель пригрозил судебным иском, если получатели не «немедленно очистят» свой веб-сайт от вредоносных файлов, которые помогли развернуть DDoS-атаку.

«Я поделился файлом журнала с записанными доказательствами того, что атака исходит от [example.com], а также подробными инструкциями по

безопасному обращению, поиску и очистке всех вредоносных файлов вручную, чтобы устранить угрозу для нашей сети,» - говорится в фальшивом уведомлении.

Злонамеренный отправитель также включил ссылку на файл, размещенный на Google Диске, якобы предоставляющий доказательства DDoS-атаки и ее происхождения…

Исследователь безопасности Proofpoint Мэтью Меса отмечает в своем твите, что эти сообщения отправляются через контактную форму веб-сайта и доставляют вредоносное ПО BazaLoader, размещенное на сайте Google.

Исследователь также говорит, что приманка является разновидностью темы нарушения авторских прав, также представленной через контактную форму веб-сайта…

В сообщении содержится ссылка на файл, в котором якобы перечислены изображения, использованные без разрешения. Данные хранятся в облачном хранилище Google Firebase.

Чтобы дело выглядело срочным, отправитель также заявляет, что владелец веб-сайта «возможно, несет ответственность за установленный законом ущерб в размере до 120 000 долларов». Однако это все уловка для распространения вредоносного ПО…

Аналитик вредоносного ПО Брэд Дункан изучил файл и обнаружил, что это был ZIP-архив с JavaScript, который извлекает библиотеку BazaLoader DLL, бэкдор, приписываемый банде TrickBot, который обычно приводит к заражению вымогателями.

Затем вредоносная программа достигает своего сервера управления и контроля (C2) и получает Cobalt Strike, инструмент тестирования на проникновение, которым киберпреступники часто злоупотребляют для поддержания устойчивости и доставки других полезных данных.

Как видно из приведенных выше примеров, уведомления довольно убедительны и используют легитимность электронных писем с контактной формой, что увеличивает шансы на получение отметки «безопасно» от решений безопасности электронной почты.

Поиск признаков злого умысла (неполная контактная информация, неправильная грамматика, подозрительные ссылки) - хороший способ не попасть в эту ловушку социальной инженерии». ***(Ionut Ilascu. Fake DMCA complaints, DDoS threats lead to BazaLoader malware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fake-dmca-complaints-ddos-threats-lead-to-bazaloader-malware/). 27.08.2021).***

***

**«Разработчик вредоносного ПО запустил свое творение в своей системе, чтобы опробовать новые функции, и данные попали на платформу разведки киберпреступлений, что позволило получить представление о деятельности киберпреступников.**

Злоумышленник является разработчиком Raccoon, программы для кражи информации, которая может собирать данные из десятков приложений, популярность которой растет в течение последних двух лет.

*Электронная почта и имя, но недостаточно*

Во время тестирования варианта стилера разработчик Raccoon заразил свою собственную систему, и этот шаг немедленно инициировал передачу данных на сервер управления и контроля (C2), а затем на форумы, посвященные киберпреступности.

Зараженная тестовая система разработчика Raccoon была обнаружена с помощью платформы Hudson Rock Cavalier, базы данных разведки киберпреступлений, которая отслеживает взломанные машины.

Алон Гал, соучредитель и технический директор Hudson Rock, говорит, что у Raccoon infostealer есть более миллиона скомпрометированных систем, которые отслеживаются через Cavalier.

Исследователь сообщил BleepingComputer, что разработчик инфостиллера Raccoon заразил их машину в феврале, но остался незамеченным, поскольку не представлял интереса, поскольку не принадлежал клиентам компании.

Он привлек внимание своим IP-адресом 1.1.1.1, специально измененным на сервере управления, чтобы реальный не был захвачен, говорит Гэл. Как ни странно, IP-адрес используется преобразователем общедоступной системы доменных имен (DNS) Cloudflare.

Данные, собранные из самозараженной системы, показывают, что разработчик проверил способность вредоносного ПО извлекать пароли из Google Chrome, что является важным атрибутом любого злоумышленника.

Дополнительная информация, полученная с тестового компьютера Raccoon, выявила имя и несколько адресов электронной почты, связанных с вредоносной программой.

К сожалению, подробностей недостаточно, чтобы определить личность разработчика Raccoon. Гэл говорит, что создатель вредоносного ПО «вероятно, специально заразил [машину]» и был достаточно осторожен, чтобы удалить детали, которые могли бы раскрыть, кто они, прежде чем запускать вредоносное ПО.

Например, адреса электронной почты, используемые для различных служб, содержат либо «raccoon», либо «raccoonstealer», что указывает на то, что они используются для общения с клиентами.

Исследователь также нашел имя Бенджамина Энгеля, хакера из Берлина и главного героя немецкого хакерского фильма 2014 года «Кто я».

Другие детали, выбранные из тестовой системы, показали, что в тестовой коробке разработчика были файлы cookie, указывающие на вход на русскоязычный форум, популярный среди известных киберпреступных групп.

Гэл смогла сравнить идентификатор в файле cookie, созданном при входе на форум, с идентификатором, привязанным к учетной записи Raccoon stealer в сообществе.

Хотя информация, собранная таким образом, не содержит подсказок, необходимых для того, чтобы назвать разработчика Raccoon настоящим именем, она показывает, что киберпреступники также могут ошибаться, и все еще есть надежда застать их врасплох». ***(Ionut Ilascu. Malware dev infects own PC and data ends up on intel platform // Bleeping Computer®***

***(https://www.bleepingcomputer.com/news/security/malware-dev-infects-own-pc-and-data-ends-up-on-intel-platform/). 16.08.2021).***

***

**«Анализ данных статистики Dr.Web в июле показал увеличение общего числа обнаруженных угроз на 3.44% по сравнению с июнем. При этом количество уникальных угроз уменьшилось на 9.5%.** Большинство детектирований по-прежнему приходится на долю рекламных программ и нежелательных приложений. В почтовом трафике по частоте распространения лидирует разнообразное вредоносное ПО, в том числе бэкдоры, направленные на хищение паролей.

Число обращений пользователей за расшифровкой файлов увеличилось на 35.2% по сравнению с первым летним месяцем. Самым распространенным шифровальщиком июля стал Trojan.Encoder.26996, на долю которого приходится почти половина всех инцидентов.

Основные угрозы июля, согласно данным сервиса статистики «Доктор Веб»:

Adware.SweetLabs.5 – альтернативный каталог приложений и надстройка к графическому интерфейсу Windows от создателей Adware.Opencandy;

Adware.Elemental.17 – семейство рекламных программ, попадающих на устройства путем подмены ссылок на файлообменных сервисах. Вместо ожидаемых файлов жертвы получают приложения с рекламой, а также устанавливают ненужное ПО;

Adware.Downware.19856 – рекламное ПО, выступающее в роли промежуточного установщика пиратских программ;

Trojan.MulDrop16.4830 – вредоносная программа, загружающая нежелательные приложения на компьютер жертвы;

Trojan.Autoit.289 – утилита, написанная на скриптовом языке AutoIt и распространяемая в составе майнера или RAT-трояна. Выполняет различные вредоносные действия, затрудняющие обнаружение основной полезной нагрузки.

Статистика вредоносных программ в почтовом трафике:

W97M.DownLoader.2938 – семейство троянов-загрузчиков, использующих уязвимости файлов Microsoft Office. Предназначены для загрузки на атакуемый компьютер других вредоносных программ;

BackDoor.SpyBotNET.25 – бэкдор, написанный на.NET. Способен манипулировать файловой системой (копирование, удаление, создание директорий и т.д.), завершать процессы и делать снимки экрана;

HTML.FishForm.123 – веб-страница, распространяющаяся посредством фишинговых рассылок. Представляет собой фиктивную форму ввода учетных данных, которая имитирует авторизацию на известных сайтах. Введенные пользователем данные отправляются злоумышленникам;

BackDoor.RatNet.2 – бэкдор, считывающий пароли, хранящиеся в браузере;

Trojan.MulDrop17.58659 – вредоносная программа, загружающая нежелательные приложения на компьютер жертвы.

По сравнению с июнем, в июле число запросов на расшифровку файлов, затронутых шифровальщиками, увеличилось на 35,2%. Наиболее активные

вымогатели: Trojan.Encoder.26996 – 47.8%; Trojan.Encoder.567 – 10.44%; Trojan.Encoder.11539 – 1.10%; Trojan.Encoder.858 – 0.82%; Trojan.Encoder.11464 – 0.82%.

Наиболее заметные события, связанные с «мобильной» безопасностью в июле: обнаружение нового семейства банковских троянов под Android; выявление очередных угроз в каталоге Google Play; активность рекламных троянов, а также вредоносных приложений, выполняющих произвольный код». ***(Рекламные приложения остаются главной угрозой, по итогам июля // Компьютерное Обозрение (https://ko.com.ua/reklamnye_prilozheniya_ostayutsya_glavnoj_ugrozoj_po_itogam_iyulya_138380). 13.08.2021).***

***

**«В июле вирусные аналитики «Доктор Веб» выявили очередные вредоносные приложения в каталоге Google Play.** Среди них – трояны семейства Android.Joker, подписывавшие жертв на платные мобильные услуги. Среди угроз, выявленных на Android-устройствах, наибольшую активность вновь проявили рекламные вредоносные приложения, а также трояны, способные выполнять произвольный код и загружать другие программы.

Специалисты обнаружили новое семейство банковских троянов Android.BankBot.Coper. Вначале эти вредоносные приложения атаковали колумбийских пользователей, однако позднее специалисты выявили модификации, нацеленные на владельцев Android-устройств ряда европейских стран.

Эти банковские трояны обладают модульной архитектурой, а также различными механизмами защиты, что позволяет им успешнее выполнять возложенные на них задачи. Например, по команде злоумышленников вредоносные программы перехватывают и отправляют SMS, контролируют push-уведомления, демонстрируют фишинговые окна и даже способны отслеживать вводимую на клавиатуре информацию.

Android.HiddenAds.1994, Android.HiddenAds.615.origin – трояны, предназначенные для показа навязчивой рекламы. Они распространяются под видом безобидных приложений и в некоторых случаях устанавливаются в системный каталог другими вредоносными программами;

Android.RemoteCode.284.origin, Android.RemoteCode.6122 – вредоносные программы, которые загружают и выполняют произвольный код. В зависимости от модификации они также могут загружать различные веб-сайты, переходить по ссылкам, нажимать на рекламные баннеры, подписывать пользователей на платные услуги и выполнять другие действия;

Android.Triada.510.origin – многофункциональный троян, выполняющий разнообразные вредоносные действия. Относится к семейству троянских приложений, проникающих в процессы всех работающих программ. Различные представители этого семейства могут встречаться в прошивках Android-устройств, куда злоумышленники внедряют их на этапе производства. Кроме того, некоторые их модификации могут эксплуатировать уязвимости, чтобы получить доступ к защищенным системным файлам и директориям.

Program.FakeAntiVirus.1 – детектирование рекламных программ, которые имитируют работу антивирусного ПО. Такие программы могут сообщать о несуществующих угрозах и вводить пользователей в заблуждение, требуя оплатить покупку полной версии;

Program.WapSniff.1.origin – программа для перехвата сообщений в мессенджере WhatsApp;

Program.KeyStroke.1.origin – Android-программа, способная перехватывать вводимую на клавиатуре информацию. Некоторые ее модификации также позволяют отслеживать входящие SMS-сообщения, контролировать историю телефонных звонков и выполнять запись телефонных разговоров;

Program.FreeAndroidSpy.1.origin – приложение, которое следит за владельцами Android-устройств и может использоваться для кибершпионажа. Оно контролирует местоположение устройств, получает доступ к телефонной книге и списку контактов пользователей, а также копирует хранящиеся на устройствах фотографии и видео;

Program.CreditSpy.2 – детектирование программ, предназначенных для присвоения кредитного рейтинга на основании персональных данных пользователей. Такие приложения загружают на удаленный сервер SMS-сообщения, информацию о контактах из телефонной книги, историю вызовов, а также другие сведения.

Tool.SilentInstaller.6.origin, Tool.SilentInstaller.7.origin, Tool.SilentInstaller.13.origin, Tool.SilentInstaller.14.origin – потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему;

Tool.Packer.1.origin – специализированная утилита-упаковщик, предназначенная для защиты Android-приложений от модификации и обратного инжиниринга. Она не является вредоносной, но может быть использована для защиты как безобидных, так и троянских программ.

Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах. В зависимости от семейства и модификации они могут демонстрировать рекламу в полноэкранном режиме, блокируя окна других приложений, выводить различные уведомления, создавать ярлыки и загружать веб-сайты. Adware.SspSdk.1.origin, Adware.AdPush.36.origin, Adware.Adpush.6547, Adware.Myteam.2.origin, Adware.Dowgin.5.origin.

Кроме того, в июле вирусные аналитики выявили очередные угрозы в каталоге Google Play. Среди них были новые трояны семейства Android.Joker, добавленные в вирусную базу Dr.Web как Android.Joker.803, Android.Joker.837 и Android.Joker.846. Они скрывались в безобидных, на первый взгляд, приложениях – редакторе изображений Background Changer, мессенджере Sweet Emoji SMS и программе с функциями фонарика Flashlight LED Pro. Приложения действительно работали так, как того ожидали пользователи, однако незаметно для жертв они также подписывали их на платные мобильные сервисы и могли выполнять произвольный код». ***(Модульный банковский троян Coper расширяет географию***

***нанесения ущерба // Компьютерное Обозрение (https://ko.com.ua/modulnyj_bankovskij_troyan_coper_rasshiryaet_geografiyu_deyatelnosti_138395). 16.08.2021).***

***

**«Компанія Eset повідомляє про виявлення 10 раніше незафіксованих сімейств шкідливих програм, розроблених у вигляді розширення для серверного ПО Internet Information Services (IIS).** Ці загрози здатні перехоплювати дані та втручатися в комунікації сервера, націлюючись на поштові скриньки урядових установ та фінансові онлайн-транзакції.

Відповідно до даних телеметрії Eset та результатів додаткових інтернет-сканувань, у 2021 році щонайменше п’ять бекдорів поширювалися за допомогою несанкціонованого використання поштових серверів Microsoft Exchange.

Серед жертв зокрема опинилися урядові установи Південно-Східної Азії та десятки компаній з різних галузей, розташовані переважно в Канаді, В'єтнамі та Індії, а також в США, Новій Зеландії, Південній Кореї та інших країнах. Крім цього, цілями одного з бекдорів стала невелика кількість серверів IIS в Україні.

Загрози цього виду використовуються для кібершпигунства, шахрайства з пошуковою оптимізацією (SEO) та інших злочинних цілей. У всіх випадках основна мета кіберзлочинців – перехопити HTTP-запити, які надходять на скомпрометований сервер IIS, та вплинути на відповіді сервера.

Спеціалісти Eset визначили п’ять основних сценаріїв роботи шкідливих програм, націлених на IIS:

Бекдори дозволяють дистанційно управляти скомпрометованим комп'ютером зі встановленим програмним забезпеченням IIS;

Програми для викрадення дозволяють перехоплювати регулярний трафік між скомпрометованим сервером та легітимними відвідувачами, а також викрадати облікові дані для входу та платіжну інформацію;

Інжектори змінюють HTTP-відповіді, які відправляються легітимним відвідувачам, для поширення шкідливого вмісту;

Проксі-модулі перетворюють скомпрометований сервер у частину командного сервера для іншого сімейства шкідливих програм;

SEO-шахрайство, під час якого шкідливі програми змінюють контент пошукових систем для маніпулювання алгоритмами пошукової видачі та підвищення рейтингу інших сайтів, у яких зацікавлені зловмисники.

«На серверах IIS рішення з безпеки використовуються не часто, що дозволяє зловмисникам залишатися непоміченими протягом тривалого часу. Це має викликати занепокоєння у авторитетних вебпорталів, які хочуть захистити дані своїх відвідувачів, включно з інформацією про аутентифікацію та платіжні дані. Організації, які використовують Outlook, також повинні бути обережними, оскільки вони залежать від IIS та можуть стати новою ціллю для шпигунства», – пояснює Зузана Хромцова, дослідниця компанії Eset». (***Небезпечні бекдори атакують сервери IIS в різних країнах, з Україною включно // Компьютерное Обозрение (https://ko.com.ua/nebezpechni_bekdori_atakuyut_serveri_iis_v_riznih_krayinah_z_ukrayinoyu_vklyuchno_138317). 09.08.2021).***

***

**«Операторы вредоносного ПО Phorpiex отключили ботнет и выставили его исходный код на продажу на одном из киберпреступных форумов. Код предлагается по цене в $9 тыс.**

Согласно сообщению на сайте, причина продажи заключается в том, что ни один из изначальных авторов вредоносного кода более не принимает участие в проекте.

Специалист компании Check Point Алексей Бухтеев подтвердил достоверность рекламного объявления. По его словам, управляющие серверы Phorpiex уже более двух месяцев не проявляют активность. Последний раз серверы получили команду на самоудаление 6 июля текущего года. С тех пор ботнет исчез из поля зрения специалистов.

«Мы знаем, что исходный код является приватным и ранее не выставлялся на продажу, поэтому это объявление на форуме выглядит действительно правдоподобно», - отметил Бухтеев в беседе с журналистом издания The Record.

Хотя сейчас C&C-серверы Phorpiex неактивны, тот, кто купит исходный код, сможет настроить свои серверы и получить доступ к инфицированным устройствам, предупредил специалист.

«Существует немало зараженных машин = активных ботов. Мы не можем точно сказать сколько, но мы постоянно наблюдаем атаки на наши шлюзы», - говорит эксперт.

Кроме того, архитектура бота позволяет оператору пассивно зарабатывать деньги на подмене адресов в криповалютных кошельках даже без активных C&C-серверов.

На данный момент неясно, приобрел ли уже кто-нибудь исходный код Phorpiex». ***(Исходный код вредоносного ПО Phorpiex выставлен на продажу в даркнете // SecurityLab.ru (https://www.securitylab.ru/news/523843.php). 30.08.2021).***

***

**«Исследователи в области кибербезопасности из AT&T Alien Labs обнаружили кластер исполняемых файлов Linux ELF, идентифицированных как модификации бэкдора PRISM с открытым исходным кодом. Злоумышленники использовали бэкдор в ходе нескольких кампаниях на протяжении более трех лет.**

«PRISM — простой и понятный бэкдор с открытым исходным кодом. Его трафик отчетливо идентифицируется, а его двоичные файлы легко обнаружить. Несмотря на это, двоичные файлы PRISM до сих пор не обнаруживались, а его C&C-сервер оставался в сети более 3,5 лет», — отметили эксперты.

Одним из обнаруженных вариантов PRISM является WaterDrop с функцией xencrypt, которая выполняет шифрование XOR со встроенным однобайтовым ключом 0x1F.

«Начиная с версии 7 варианта WaterDrop, образцы включают текстовую строку «WaterDropx vX start», где X — это целочисленный номер версии. До сих

пор мы наблюдали версии 1, 2.2 и 3, все еще использующие имя PRISM. Версии 7, 9 и 12 называются WaterDropx. Он также использует легко идентифицируемую строку пользовательского агента «agent-waterdropx» для передачи команд и управления на основе HTTP и достигает поддоменов waterdropx[.]com», — пояснили исследователи.

Домен waterdropx[.]com был зарегистрирован на нынешнего владельца 18 августа 2017 года, а по состоянию на 10 августа 2021 года он все еще был в Сети.

По словам исследователей, помимо базовых функций PRISM, WaterDrop предоставляет XOR-шифрование для конфигурации и дополнительный процесс, который регулярно запрашивает у C&C-сервера команды для выполнения. Эта связь с сервером обычно представляет собой обычный текстовый HTTP-протокол HTTP и выполняется с помощью команды curl.

Исследователи обнаружили образцы вредоносного ПО, помеченные как PRISM v1, которые они с высокой степенью уверенности связывают с группировкой, использующей другие обнаруженные исполняемые варианты PRISM Linux ELF.

Новая версия PRISM создает дочерний процесс, который постоянно будет запрашивать у C&C-сервера команды для выполнения. PRISM v1 не поддерживает никакого вида обфускации, упаковки или шифрования двоичных файлов.

Версии PRISM v2.2 и PRISM v3 практически идентичны — обе используют командные строки BASH для сокрытия конфиденциальных данных». ***(Обнаружена новая версия бэкдора PRISM // SecurityLab.ru (https://www.securitylab.ru/news/523768.php). 26.08.2021).***

***

**«Специалисты в области кибербезопасности антивирусной компании ESET обнаружили модульный бэкдор SideWalk, использующийся APT-группировкой под названием SparklingGoblin. Данный бэкдор имеет много общего с бэкдором CROSSWALK, используемым группой.**

SideWalk — модульный бэкдор, который может динамически загружать дополнительные модули, отправленные с C&C сервера, использовать Google Docs для активации следующего этапа атаки (dead drop resolver) и платформу Cloudflare Workers в качестве C&C-сервера. Он также может корректно обрабатывать связь через прокси.

Хакерская группировка в основном нацелена на академический сектор в Восточной и Юго-Восточной Азии, но также проявила усиленный интерес к сфере образования в Канаде, медиакомпаниям в США и по крайней мере к одной неназванной компании по продаже компьютеров в США.

Неизвестно, на какие компании были совершены атаки и когда произошли взломы. Также неизвестно откуда родом группировка, однако ESET отметила, что некоторые из процедур APT были описаны в блоге на китайском языке, предполагая, что она может базироваться в Восточной Азии.

ESET классифицирует эту группу как APT, которая используют «непрерывные, тайные и изощренные хакерские методы для получения доступа к

системе и пребывания внутри нее в течение длительного периода времени с потенциально разрушительными последствиями».

По данным ESET, аналогичный набор инструментов, используемый SparklingGoblin, применялся в ходе серии атак на университеты Гонконга участниками группировки Winnti Group». ***(APT SparklingGoblin атаковала высшие образовательные учреждения по всему миру // SecurityLab.ru (https://www.securitylab.ru/news/523716.php). 25.08.2021).***

***

**«Windows-бэкдор под названием ShadowPad, позволяющий злоумышленникам загружать дополнительные вредоносные модули или красть данные, с 2017 года активно используется пятью различными китайскими кибершпионскими группировками.**

По словам исследователей в области кибербезопасности из SentinelOne, использование ShadowPad значительно снижает затраты на разработку и обслуживание вредоносов для злоумышленников. Как отметили эксперты, «некоторые группировки прекратили разработку собственных бэкдоров после того, как получили доступ к ShadowPad».

ИБ-эксперты назвали ShadowPad «шедевром китайского шпионажа в частном секторе вредоносных программ». Будучи преемником PlugX, ShadowPad привлек к себе всеобщее внимание после атак на цепочку поставок NetSarang, CCleaner и ASUS.

Атаки с применением ShadowPad затронули организации в Гонконге, а также критически важную инфраструктуру в Индии, Пакистане и других странах Центральной Азии. Хотя эксперты в первую очередь связывают вредонос с APT41, он также используется китайскими шпионскими группировками Tick, RedEcho, RedFoxtrot, Operation Redbonus, Redkanku и Fishmonger.

Вредоносная программа расшифровывает и загружает в память устройства подключаемый модуль Root, обеспечивающий загрузку других встроенных модулей, в дополнение к динамическому развертыванию дополнительных подключаемых модулей с удаленного C&C-сервера. Это позволяет злоумышленникам использовать дополнительные функции, по умолчанию не встроенные во вредоносное ПО. На сегодня идентифицировано как минимум 22 уникальных плагина.

Зараженные компьютерные системы управляются контроллером на базе Delphi, который используется для обмена данными через бэкдор, обновления инфраструктуры C&C-сервера и управления плагинами.

Как отметили ИБ-эксперты, набор функций, доступный для пользователей ShadowPad, жестко контролируется продавцом. Каждый плагин продается отдельно, и большинство образцов содержит менее чем девять плагинов». ***(Вредоносное ПО ShadowPad стало любимым инструментом китайских шпионов // SecurityLab.ru (https://www.securitylab.ru/news/523626.php). 23.08.2021).***

***

**«Атакующий IoT-устройства P2P-ботнет Mozi получил новые функции, позволяющие ему сохранять персистентность в сетевых шлюзах производства Netgear, Huawei и ZTE.**

Как сообщили специалисты Microsoft Security Threat Intelligence Center и Azure Defender Section 52, сетевые шлюзы представляют собой «лакомый кусочек» для злоумышленников, поскольку они «идеальны для первоначального доступа к корпоративным сетям».

«Заражая маршрутизаторы, они (хакеры – ред.) могут осуществлять атаки "человек посередине" (MITM) с помощью перехвата HTTP и спуфинга DNS с целью компрометации конечных точек и развертывания вымогательского ПО или для вызова нарушения безопасности на объектах OT», - сообщается в уведомлении специалистов.

Впервые задокументированный в декабре 2019 года компанией Netlab 360 ботнет Mozi традиционно заражает маршрутизаторы и цифровые видеорегистраторы и включает их в IoT-ботнет, который может использоваться для осуществления DDoS-атак, похищения данных и выполнения полезной нагрузки. Ботнет эволюционировал из исходного кода нескольких семейств вредоносного ПО, в частности Gafgyt, Mirai и IoT Reaper. Mozi распространяется путем подбора ненадежных или заводских паролей, а также путем эксплуатации неисправленных уязвимостей.

Как недавно обнаружили специалисты команды безопасности IoT-устройств компании Microsoft, вредоносное ПО «принимает особые меры для повышения своих шансов на то, чтобы «пережить» перезагрузку и попытки другого вредоносного ПО или ИБ-специалистов вмешаться в его операции». В частности, вредонос пытается получить персистентность на атакуемых устройствах и заблокировать TCP-порты (23, 2323, 7547, 35000, 50023 и 58000), использующиеся для получения удаленного доступа к шлюзам.

Более того, Mozi получил поддержку новых команд, позволяющих ему взламывать HTTP-сеансы и осуществлять спуфинг DNS для переадресации трафика на подконтрольный хакерам домен.

Домашним и бизнес-пользователям маршрутизаторов Netgear, Huawei и ZTE рекомендуется обезопасить свои устройства с помощью надежных паролей и обновлений прошивки до последних версий». ***(IoT-ботнет Mozi теперь атакует сетевые шлюзы Netgear, Huawei и ZTE // SecurityLab.ru (https://www.securitylab.ru/news/523606.php). 20.08.2021).***

***

**«Специалисты Positive Technologies проанализировали актуальные киберугрозы II квартала 2021 года.** Анализ показал рекордное количество атак с использованием программ-шифровальщиков, смену методов атак на отрасль торговли, а также тенденцию к созданию вредоносов, нацеленных на Unix-системы.

По данным анализа, количество атак во II квартале 2021 года увеличилось лишь на 0,3% в сравнении с I кварталом. Эксперты считают, что подобного замедления следовало ожидать, так как компании успели адаптироваться к работе в

условиях пандемии, в том числе приняли меры по защите сетевого периметра и систем удаленного доступа.

Однако во II квартале были побиты все рекорды по количеству атак с использованием шифровальщиков: их доля составила 69% среди всех атак с использованием ВПО. Наибольшее количество инцидентов было выявлено специалистами в апреле (45%). Тем не менее нашумевшие атаки на крупнейшую трубопроводную систему США Colonial Pipeline и полицию округа Колумбия, которые привлекли внимание правоохранительных органов, сказались на активности операторов и распространителей шифровальщиков, и уже в июне число атак с использованием вымогательского ПО снизилось вдвое.

В исследовании Positive Technologies отмечается, что на форумах в дарквебе относительно недавно появился запрет на публикацию постов на тему партнерских программ операторов шифровальщиков. Эксперты считают, что в скором времени можно ожидать исчезновения так называемых партнеров как отдельной роли, а их задачи возьмут на себя сами операторы программ-вымогателей, которые будут собирать команды распространителей и курировать их напрямую.

Среди других тенденций, которые отмечают эксперты компании, — укрепившийся тренд на создание вредоносов, нацеленных на Unix-системы.

«Мы привыкли к мысли, что злоумышленники, распространяющие ВПО, — проблема систем на базе Windows, — говорит аналитик информационной безопасности Positive Technologies Яна Юракова. — Сейчас мы видим укрепление тренда на создание вредоносов для атак на Unix-системы, средства виртуализации и оркестраторы. Все больше компаний, в том числе крупных, используют ПО на базе Unix, и логично, что злоумышленники стали обращать внимание также на эти системы».

Одной из самых заметных тенденций стало изменение ландшафта киберугроз в сфере торговли. Эксперты обратили внимание на значительное снижение числа атак с использованием так называемых веб-скиммеров. При этом интерес к этой отрасли у злоумышленников, распространяющих шифровальщики, только растет. Доля атак с использованием программ-вымогателей среди атак с использованием ВПО во II квартале составила в торговле 95%. Эксперты связывают эти изменения с тем, что раньше основной целью злоумышленников, атакующих торговые компании, была кража данных — платежных реквизитов, персональных и учетных данных клиентов. Сейчас же преступники все чаще преследуют прямую финансовую выгоду, рассчитывая получить крупный выкуп». ***(Positive Technologies: число атак с использованием шифровальщиков бьет все рекорды // Positive Technologies (https://www.ptsecurity.com/ru-ru/about/news/positive-technologies-chislo-atak-s-ispolzovaniem-shifrovalshchikov-bet-vse-rekordy/). 30.08.2021).***

***

**«Британские университеты призываются проявлять бдительность в отношении возникающей угрозы кибербезопасности со стороны фабрик по выпуску эссе.**

Предупреждение поступило, поскольку сектор продолжает бороться с беспрецедентным всплеском атак программ-вымогателей.

Essay Mills, также известные как сайты с мошенничеством по контрактам, стремятся обмануть студентов и заработать на них, взламывая веб-сайты университетов и размещая в своих целях контент, который кажется законным и соответствует университетским услугам.

Как правило, злоумышленники пишут на страницах, предназначенных для студентов, с гиперссылками на их собственные веб-сайты или перехватывают ссылки на законные службы с перенаправлением на сайты мошенничества.

Этот тип коварной деятельности уже применялся в университетах США и Австралии, и аналогичная тактика вполне может быть использована в Великобритании.

Чтобы помочь университетам справиться с этой новой угрозой, британский цифровой орган высшего образования, Jisc, и Агентство обеспечения качества высшего образования, QAAобъединили усилия для повышения осведомленности и предоставления рекомендаций непосредственно вузам.

В отличие от программ-вымогателей, которые нацелены на массовое разрушение в качестве рычага для вымогательства, злоумышленники стараются оставаться незамеченными и действуют без ведома соответствующих университетов, но многие советы по предотвращению остаются теми же.

Директор по безопасности Jisc, Генри Хьюз, сказал:

«Кибератаки становятся растущей проблемой для колледжей и университетов и, как это, вероятно, имеет место в случае с незаконной деятельностью фабрики сочинений, часто вызваны организованной преступностью.

«Есть шаги, которые могут быть предприняты для минимизации риска, включая использование сервисов кибербезопасности, которые могут блокировать известный вредоносный контент, помогать уменьшать попытки фишинга и другие формы атак на британское образование и исследования.

«Jisc работает с университетами, колледжами, отраслевыми органами и регулирующими органами, чтобы помочь скоординировать основанный на политике подход к блокированию широкого спектра угроз кибербезопасности».

Глава отдела политики и коммуникаций QAA Гарет Кроссман сказал:

«Essay Mills представляют угрозу для мировой репутации британского высшего образования. Эти компании недобросовестны, и их эксплуатация студентов ставит под угрозу их академическую и будущую карьеру, открывая их для шантажа и киберпреступлений.

«Их единственная мотивация - деньги, поэтому нам нужны действия со стороны правительств и онлайн-платформ, чтобы максимально усложнить работу. Вот почемуQAA также проводит кампанию за принятие закона о криминализации фабрики сочинений.

«Мы настоятельно призываем университеты следовать техническим советам Jisc и повышать осведомленность сотрудников и студентов о новой тактике, применяемой фабриками по выпуску эссе. Пользователи должны знать, на что обращать внимание и как сообщать о любых подозрениях». ***(Universities urged to be vigilant over essay mill hacking risk // Jisc (https://www.jisc.ac.uk/news/universities-urged-to-be-vigilant-over-essay-mill-hacking-risk-05-aug-2021). 05.08.2021).***

***

**«ФБР опубликовало предупреждение о программе-вымогателе Hive после того, как на прошлой неделе группа взломала Memorial Health System.**

В предупреждении объясняется, что Hive - это партнерская программа-вымогатель, впервые появившаяся в июне и использующая «несколько механизмов для взлома бизнес-сетей, включая фишинговые электронные письма с вредоносными вложениями для получения доступа и протокол удаленного рабочего стола для горизонтального перемещения в сети».

«После компрометации сети жертвы злоумышленники Hive извлекают данные и шифруют файлы в сети. Актеры оставляют записку о выкупе в каждом затронутом каталоге в системе жертвы, в которой содержатся инструкции о том, как приобрести программное обеспечение для дешифрования. Записка о выкупе также угрожает утечка эксфильтрованных данных о жертвах на сайте Tor, HiveLeaks, - пояснили в ФБР.

«Программа-вымогатель Hive ищет процессы, связанные с резервным копированием, антивирусным / антишпионским ПО и копированием файлов, и завершает их, чтобы облегчить шифрование файлов. Зашифрованные файлы обычно заканчиваются расширением.hive».

В предупреждении объясняется, как программа-вымогатель повреждает системы и резервные копии, прежде чем направить жертвам ссылку на «отдел продаж» группы, доступ к которой можно получить через браузер TOR. Ссылка приводит жертв к живому чату с людьми, стоящими за атакой, но ФБР отметило, что некоторым жертвам даже звонили злоумышленники с требованием выкупа.

У большинства жертв крайний срок выплаты составляет от двух до шести дней, но другие смогли продлить свои сроки путем переговоров.

Группа управляет сайтом утечки, который они используют, чтобы запугать жертв, чтобы они заплатили. ФБР включило признаки компрометации, ссылку на сайт утечки и образец записки о выкупе, переданной жертве.

Джон Ригги, старший советник по кибербезопасности Американской ассоциации больниц, сказал, что новая программа-вымогатель Hive вызывает особую озабоченность у организаций здравоохранения. На данный момент Hive атаковал не менее 28 организаций, в том числе Memorial Health System, на которую 15 августа была совершена атака с использованием программ-вымогателей. У этой некоммерческой организации есть несколько больниц, клиник и медицинских учреждений в Огайо и Западной Вирджинии.

Генеральный директор Скотт Кэнтли заявил в своем заявлении, что сотрудники трех больниц - Marietta Memorial, Selby и Sistersville General Hospital -

были вынуждены использовать бумажные диаграммы, пока их ИТ-команды работали над восстановлением своих систем.

Все неотложные хирургические операции и рентгенологические обследования на понедельник, 16 августа, были отменены из-за нападения. Отделения неотложной помощи системы здравоохранения Мемориал были вынуждены перейти в другое место из-за нападения, а больница Мемориал Мариетта согласилась только продолжать принимать пациентов, пострадавших от инсультов и травм.

Всех, кто нуждался в помощи, просто нужно было переправлять в другие больницы. Специалисты ФБР, CISA и кибербезопасности помогли больнице отреагировать на атаку.

В заявлении, сделанном тремя днями позже, Кэнтли сказал, что больничная система «достигла согласованного решения и начинает процесс, который восстановит работу как можно быстрее и безопаснее».

Позже он признался The Marietta Times, что больница заплатила выкуп за получение ключей дешифрования.

«Мы заключили соглашение и получили ключи для разблокировки наших серверов и начала процесса восстановления. У ФБР есть подозрения относительно новой и сложной организации в Восточной Европе», - пояснил Кэнтли.

«Это хорошая новость для наших сотрудников - получить обратно наши инструменты. У нас есть 800 серверов и более 3000 персональных устройств, которые наши врачи используют для обслуживания пациентов. Мы сохраним необходимые услуги, и на следующей неделе мы должны вернуться к обычным услугам. Мы продолжаем служить нашим пациентам с большой осторожностью перед лицом невзгод».

Системы больницы были снова подключены к выходным, и Кэнтли сказал, что нет «признаков того, что какие-либо данные о пациентах или сотрудниках были публично опубликованы или разглашены».

«Очень жаль, что многие медицинские организации сталкиваются с воздействием меняющегося ландшафта киберугроз», - сказал Кэнтли». ***(Jonathan Greig. FBI releases alert about Hive ransomware after attack on hospital system in Ohio and West Virginia // ZDNet (https://www.zdnet.com/article/fbi-releases-alert-about-hive-ransomware-after-attack-on-hospital-system/). 26.08.2021).***

***

**«Эксперт по кибербезопасности предупредил, что атаки программ-вымогателей будут усугубляться - и в конечном итоге можно будет уничтожить инфраструктуру целого умного города с поддержкой 5G.**

Киберпреступники, использующие программы-вымогатели, регулярно атакуют государственные службы. Бюджеты ИТ государственного сектора не только означают, что сети менее защищены от атак, но и указанные сети также используются для предоставления жизненно важных услуг сообществу.

В некоторых случаях местные органы власти платят выкуп за расшифровку сети и восстановление услуг, что делает их идеальными объектами для вымогательства.

Городская инфраструктура, включая службы экстренной помощи, транспорт, управление светофорами, видеонаблюдение и многое другое, все чаще подключается к службам и датчикам 5G Интернета вещей (IoT) для сбора данных и предоставления более качественных и эффективных услуг.

Но хотя у подключенных городов есть потенциал для улучшения городских услуг, любое отсутствие безопасности в устройствах Интернета вещей может сделать их очень привлекательной целью для атак программ-вымогателей - и, учитывая нынешнюю обстановку в отношении программ-вымогателей, вопрос не в том, если, а в том, когда.

«Я смотрю через два года, и мой прогноз - умный город 5G будет удержан за выкуп. Я не вижу, чтобы сейчас происходило что-либо, что говорило бы мне, что это предсказание не сбудется», - Тереза Пэйтон, генеральный директор Fortalice Solutions и бывший ИТ-директор Белого дома сказал в интервью ZDNet Security Update.

Было много случаев, когда города и общественная инфраструктура были скомпрометированы программами-вымогателями - и это может иметь чрезвычайно разрушительные последствия. Например, когда киберпреступники атакуют больницы с помощью программ-вымогателей, характер отрасли означает, что во многих случаях - но не во всех - поставщики медицинских услуг чувствуют, что у них нет другого выбора, кроме как платить.

А постоянный успех атак программ-вымогателей означает, что преследование подключенной инфраструктуры является следующим логическим шагом для киберпреступников. «Я просто не вижу достаточного прогресса, чтобы мы могли искоренить программы-вымогатели - к сожалению, я вижу, что ситуация становится намного хуже, прежде чем мы действительно выясним, как с ними бороться, и ситуация станет лучше», - сказала Пэйтон., добавив, что киберпреступников «действительно не волнует, каковы последующие последствия, они просто пытаются заработать».

Однако в умных городах можно применять меры для защиты от кибератак.

Руководство по безопасности умного города от Национального центра кибербезопасности Великобритании (NCSC) рекомендует, чтобы города развертывали устройства только от проверенных поставщиков и чтобы ни одно устройство IoT в сети не использовало имя пользователя и пароль по умолчанию, поскольку это делает их легкой мишенью.

Организации также должны регулярно проверять, были ли учетные данные, принадлежащие сотрудникам с привилегиями учетной записи высокого уровня, раскрыты в результате утечки данных. Если да, то пароли - и, возможно, даже имена учетных записей - следует изменить, чтобы снизить риск злоупотребления ими со стороны групп программ-вымогателей или других киберпреступников.

«Ищите эти учетные записи электронной почты, ищите эти пароли и подумайте о том, чтобы фактически отказаться от учетных записей электронной почты, которые находятся в свалках данных паролей и имеют доступ к основным системам», - сказал Пэйтон». ***(Danny Palmer. Ransomware: It's only a matter of time before a smart city falls victim, and we need to take action now // ZDNet***

***(https://www.zdnet.com/article/ransomware-its-only-a-matter-of-time-before-an-iot-smart-city-falls-victim-to-an-attack-if-action-isnt-taken-now/). 27.08.2021).***

***

**«Исследователи кибербезопасности предупредили о четырех новых семействах программ-вымогателей, которые могут представлять серьезную угрозу кибербезопасности для бизнеса.**

Программы-вымогатели остаются одной из ключевых угроз кибербезопасности, с которыми сталкиваются предприятия по всему миру, поскольку киберпреступники пытаются взломать сети и зашифровать их, чтобы потребовать выкуп, который может достигать миллионов.

Эта приманка потенциально легких денег привлекает киберпреступников всех уровней к программам-вымогателям, от специализированных банд программ-вымогателей, которые хранят вредоносное ПО для себя, до групп программ-вымогателей как услуги, которые сдают свой незаконный продукт в аренду злоумышленникам низкого уровня, которые хотят принять участие в действии.

В последние месяцы, похоже, исчезли некоторые крупные операторы программ-вымогателей. Но это не значит, что программы-вымогатели представляют собой меньшую проблему - появляются новые группы, чтобы заполнить пробелы.

Исследователи кибербезопасности из Palo Alto Networks подробно описали четыре новых семейства программ-вымогателей, обнаруженных в ходе расследований, и при определенных обстоятельствах любое из них может стать следующей большой угрозой программ-вымогателей.

Одним из них является LockBit 2.0, программа-вымогатель как услуга, которая существует с сентября 2019 года, но получила большую популярность в течение этого лета. Те, кто стоит за этим, обновили свои операции в даркнете в июне - когда они запустили версию LockBit 2.0 - и агрессивная реклама привлекла внимание киберпреступников.

По данным исследователей, с июня LockBit взломал 52 организации по всему миру. В первую очередь, злоумышленники, использующие LockBit, скомпрометировали Accenture, хотя компания смогла восстановить данные из резервных копий без необходимости платить выкуп.

Рост популярности LockBit не остался незамеченным, поскольку Австралийский Центр кибербезопасности опубликовал предупреждение, предупреждающее организации об угрозе.

Но LockBit - не единственная разновидность программного обеспечения-вымогателя, которое набирает обороты - программа-вымогатель AvosLocker впервые появилась в июле и предлагает схему «вымогатель как услуга», в которую входят операторы, ведущие переговоры о выкупе.

Группа взломала несколько организаций по всему миру, в том числе юридические фирмы в США и Великобритании. Как и другие группы программ-вымогателей, AvosLocker утекает украденные данные, если выкуп не уплачен.

Требования выкупа после атак AvosLocker относительно невысоки для программ-вымогателей в 2021 году и будут составлять от 50 000 до 75 000

долларов. Но в отличие от многих других групп программ-вымогателей, которые требуют платеж в биткойнах, AvosLocker запрашивает его в Monero - криптовалюте, которая должна быть анонимной. Monero не так ценен, как биткойн, но дополнительная анонимность означает, что сложнее отследить киберпреступников, которые его используют.

Еще одним новым игроком на рынке программ-вымогателей является программа-вымогатель Hive, которая впервые была замечена в заражении организаций в июне 2021 года. Злоумышленники, стоящие за ней, также используют украденные данные и двойное вымогательство, чтобы заставить жертв заплатить выкуп.

Всего на сегодняшний день Hive унесло 28 жертв, включая медицинских работников, в результате атак, которые могут помешать лечению пациентов. Такое бесцеремонное отношение к благополучию широкой публики может сделать Hive опасной угрозой вымогателей.

Четвертая новая угроза, подробно описанная исследователями, - это разновидность установленной формы программы-вымогателя. Программа-вымогатель Hello Kitty впервые появилась в декабре 2020 года и была предназначена в первую очередь для систем Windows. Теперь исследователи определили новую версию Hello Kitty, которая нацелена на системы Linux, открывая совершенно новую платформу для атак киберпреступников.

«Программы-вымогатели преследуют не только системы Windows - теперь, когда вариант Hello Kitty нацелен на ESxi, они пытаются получить совершенно другой рынок, который ранее не исследовался», - сказал ZDNet Доэль Сантос, аналитик по анализу угроз в Unit 42, Palo Alto Networks.

Организации по всему миру стали мишенью этого варианта Hello Kitty, который изменяет требования выкупа в зависимости от цели. Преступники потребовали от одной жертвы до 10 миллионов долларов в Monero, хотя операторы также открыты для приема платежей в биткойнах.

Рост числа этих групп программ-вымогателей свидетельствует о том, что, несмотря на то, что существующие группы, казалось бы, исчезают, на их место приходят новые игроки. Многие из них будут применять тактику и методы успешных программ-вымогателей, которые существовали до них, чтобы сделать атаки максимально эффективными.

«Многие более распространенные группы проложили путь для появления этих более мелких групп, предоставив им бизнес-модель, которой можно было бы следовать для выполнения операций. Это еще одна причина, по которой мы видим, что эти появляющиеся группы программ-вымогателей используют методы двойного вымогательства, которые стали стандартом с тех пор, как вымогатели Maze, - сказал Сантос.

Независимо от того, какой тип программ-вымогателей используют киберпреступники, они представляют собой серьезную угрозу для бизнеса. Чтобы защитить сети от атак программ-вымогателей, рекомендуется своевременно применять исправления безопасности для предотвращения использования злоумышленниками известных уязвимостей. М аутентификация ульт-фактор также должна применяться ко всем пользователям, чтобы обеспечить дополнительный

барьер для атак, эксплуатирующих украденные или просочились имена пользователей и пароли в качестве точки входа.

Компаниям также рекомендуется регулярно обновлять и тестировать свои резервные копии - и хранить их в автономном режиме - поэтому, если сеть действительно подвергнется атаке программы-вымогателя, есть возможность восстановить ее без необходимости платить выкуп». ***(Danny Palmer. Ransomware: These four rising gangs could be your next major cybersecurity threat // ZDNet (https://www.zdnet.com/article/ransomware-these-four-rising-threats-could-be-the-next-major-cybersecurity-risk-facing-your-business/). 25.08.2021).***

***

**«Увеличилось количество кибератак с использованием вымогателей, которые впервые появились почти два года назад.** Но, несмотря на то, что он относительно старый, он по-прежнему пользуется успехом для киберпреступников.

Исследователи кибербезопасности из компании Trend Micro подробно рассказали об увеличении числа кампаний вымогателей LockBit с начала июля. Эта программа-вымогатель как услуга впервые появилась в сентябре 2019 года и была относительно успешной, но этим летом ее активность резко возросла.

В рекламе на подпольных форумах авторы LockBit заявляют, что LockBit 2.0 - один из самых быстрых вариантов программ-вымогателей для шифрования файлов на рынке сегодня. И эти утверждения оказались интересными для киберпреступников, стремящихся заработать на программах-вымогателях.

В последние недели исследователи Trend Micro наблюдали ряд кампаний вымогателей LockBit, нацеленных преимущественно на организации в Чили, а также в Великобритании, Италии и Тайване.

Хотя LockBit оставался незамеченным на протяжении большей части этого года, он попал в заголовки новостей благодаря атаке на фирму профессиональных услуг Accenture. LockBit также, похоже, извлек выгоду из очевидного исчезновения банд программ-вымогателей, включая REvil и Darkside, при этом значительное количество филиалов этих операторов обратилось к LockBit как к новому средству выполнения атак программ-вымогателей.

Злоумышленники часто проникают в сети, используя взломанный протокол удаленного рабочего стола (RDP) или учетные записи VPN, которые были пропущены или украдены; в качестве альтернативы атаки LockBit иногда пытаются привлечь инсайдеров, чтобы получить доступ с помощью законных учетных данных.

LockBit также добился успеха, следуя по стопам известных групп вымогателей, используя определенные тактики, техники и процедуры (ДТС) во время атак. Например, LockBit теперь использует функцию Ryuk Wake-on-LAN, отправляя пакеты для пробуждения автономных устройств, чтобы помочь перемещаться по сети и компрометировать как можно больше машин.

LockBit также использует инструмент, ранее развернутый программой-вымогателем Egregor, который использует сетевые принтеры для распечатки записок о выкупе.

«На них сильно повлияла банда вымогателей Maze, и когда они закрылись, они, похоже, переключили свое внимание на TTP групп вымогателей Ryuk и Egregor», - сказал ZDNet Джон Клей, вице-президент Trend Micro по аналитике угроз.

«Что мы можем извлечь из этого, так это то, что многие банды злоумышленников, вероятно, следят за новостями о том, насколько успешны другие банды, и стремятся сами смоделировать свои ТТП. Программы-вымогатели эволюционировали с течением времени, чтобы продолжать быть успешными для своих создателей», - добавил он.

Как и многие самые разрушительные варианты программ-вымогателей, LockBit также добавляет к атакам элемент двойного вымогательства, крадя данные жертвы и угрожая их утечкой, если выкуп не будет выплачен в течение установленного периода.

«Банда LockBit существует уже некоторое время и продолжает обновлять свои TTP, чтобы проводить успешные кампании атак», - сказал Клэй.

Ожидается, что атаки программ-вымогателей LockBit будут продолжать оставаться угрозой кибербезопасности в течение некоторого времени, особенно с учетом того, что группа активно рекламирует дополнительные филиалы. Но хотя группы программ-вымогателей агрессивно настойчивы, есть действия, которые группы информационной безопасности могут предпринять, чтобы защитить сети от атак.

Это включает в себя применение последних исправлений безопасности и обновлений для операционных систем и программного обеспечения, поэтому киберпреступники не могут использовать известные уязвимости для запуска атак. Организациям также следует применять многофакторную аутентификацию в сети, чтобы киберпреступникам было сложнее использовать украденные учетные данные для облегчения атак». ***(Danny Palmer. This ransomware has returned with new techniques to make attacks more effective // ZDNet (https://www.zdnet.com/article/this-ransomware-has-returned-with-new-techniques-to-make-attacks-more-effective/). 18.08.2021).***

***

**«Программы-вымогатели сегодня представляют собой одну из самых серьезных угроз кибербезопасности для бизнеса, и киберпреступники потенциально могут заработать миллионы долларов в биткойнах за одну успешную атаку.**

Эта соблазн быстро заработать большие суммы денег привлекает интерес со всего спектра киберпреступников, от изощренных группировок, специализирующихся на атаках программ-вымогателей, до партнерских схем, в которых подражатели вымогателей могут сдавать их в аренду в качестве услуги в обмен на долю прибыли.

Это также привлекает киберпреступников низкого уровня, которые видят возможность захватить кусок пирога с программами-вымогателями, даже если они плохо понимают, что делают.

Исследователи кибербезопасности из Abnormal Security подробно описали любительскую кампанию по вымогательству с использованием социальной инженерии, пытаясь обманом заставить сотрудников установить вымогатель DemonWare в сети своей организации в обмен на часть выплаты.

Программа-вымогатель DemonWare, также известная как Black Kingdom и DEMON, является одной из наименее сложных форм программ-вымогателей, но это не остановило киберпреступников, пытающихся ее использовать.

В этом случае злоумышленник использует LinkedIn и другую общедоступную информацию для определения целей и обращается к ним по электронной почте, спрашивая, хотят ли они установить вымогатель DemonWare в сети в обмен на миллион долларов - это 40% сокращение от 2,5 миллиона долларов. выкуп.

Злоумышленник оставляет адрес электронной почты и имя пользователя Telegram для связи с заинтересованными сторонами - что и сделали исследователи, используя вымышленную личность, чтобы узнать больше о кампании и тех, кто за ней стоит.

Вскоре стало очевидно, что злоумышленник-вымогатель не был самым изощренным киберпреступником в мире, и они быстро снизили предлагаемую стоимость выкупа до 120 000 долларов. Однако для злоумышленника это все равно будет большими деньгами.

«Как и большинство финансово мотивированных киберпреступников, этот актер просто пытается заработать любую сумму денег на этой афере. Хотя он быстро перешел на гораздо меньшую сумму выкупа в ходе нашего разговора, 100000 долларов или 1 миллион долларов и то, и другое были бы целой жизнью. изменение суммы для него», - сказал ZDNet Крейн Хассолд, директор по анализу угроз компании Abnormal Security.

Злоумышленник утверждал, что человек, ответственный за установку вымогателя в сети, не будет пойман, утверждая, что DemonWare зашифрует все, включая файлы видеонаблюдения. Исследователи отмечают, что такой подход предполагает, что злоумышленник «не очень хорошо знаком с цифровой криминалистикой или расследованиями реагирования на инциденты».

Но анализ файлов, отправленных злоумышленником, подтвердил, что они действительно пытаются распространить рабочую версию программы-вымогателя DemonWare. Злоумышленник утверждает, что он сам закодировал программу-вымогатель, но это ложь - DemonWare можно бесплатно загрузить с GitHub, и его фактический автор разместил ее там, "чтобы продемонстрировать, насколько легко [sic] создать программу-вымогатель и как это сделать. работа [так в оригинале]».

Заявления злоумышленника о самокодировании, вероятно, всего лишь еще одна часть попытки убедить людей использовать схему. По словам злоумышленника, они успешно поощряли людей помогать им в развертывании программ-вымогателей, хотя их заявления вряд ли заслуживают доверия.

Но кто этот подражатель злоумышленника-вымогателя? Используя электронную почту и контактные данные Telegram, которые они предоставили в своем первоначальном сообщении, исследователи смогли отследить их до веб-сайта, на котором можно было торговать валютой Нигерии Найра, а также

российской платформы социальных сетей. Когда эта информация была представлена в сообщениях, злоумышленник подтвердил, что они нигерийцы, что может объяснить первоначальные попытки социальной инженерии.

Киберпреступники из Нигерии, как правило, сосредоточивают свои усилия на атаках фишинга и компрометации деловой электронной почты (BEC), но в данном случае они взяли то, что знали, и попытались применить это к программам-вымогателям.

«Знание того, что за этой кампанией стоит нигерийец, действительно добавляет много контекста к тактике, которую он использует. В течение многих лет киберпреступники в Нигерии использовали базовые методы социальной инженерии для совершения самых разнообразных мошенничеств, поэтому логично предположить, что этот актер является пытается использовать ту же тактику для развертывания программ-вымогателей», - сказал Хассолд.

«Похоже, что этот актер пытается запрыгнуть на подножку вымогателей из-за внимания, которое к недавним атакам привлекли средства массовой информации; однако он адаптировал исторические методы доставки вымогателей, чтобы вписаться в структуру атаки, к которой он, вероятно, привык», - добавил он.

Хотя этот злоумышленник может быть не очень успешным, другие более опытные операторы вымогателей извлекают выгоду из поиска инсайдеров, которые помогают им получить доступ к сетям. Например, программа-вымогатель LockBit, популярность которой резко возросла в последние месяцы, регулярно привлекает инсайдеров для помощи в проведении кампаний…». ***(Danny Palmer. Ransomware: This amateur attack shows how clueless criminals are trying to get in on the action // ZDNet (https://www.zdnet.com/article/ransomware-this-amateur-attack-shows-how-clueless-criminals-are-trying-to-get-in-on-the-action/). 19.08.2021).***

***

**«Colonial Pipeline рассылает письма с уведомлением о нарушениях 5810 нынешним и бывшим сотрудникам, чья личная информация была доступна группе вымогателей DarkSide во время атаки в мае.**

Компания признала в письме от 13 августа, что 6 мая группа вымогателей «приобрела определенные записи», хранящиеся в их системах.

«Затронутые записи содержат определенную личную информацию, такую как имя, контактную информацию, дату рождения, удостоверение личности государственного образца (например, номер социального страхования, военный билет, идентификационный номер налогоплательщика и номера водительских прав) и информацию, связанную со здоровьем (включая информацию о медицинском страховании). Не вся эта информация была затронута для каждого пострадавшего человека», - говорится в письме.

В мае агентство Bloomberg сообщило, что, прежде чем заблокировать бизнес-системы конвейера, группа похитила почти 100 ГБ данных.

Colonial Pipeline заявила, что предлагает жертвам взлома два бесплатных года «восстановления личности» и услуги кредитного мониторинга от Experian. Они призвали пострадавших проверять свои кредитные отчеты на предмет любых несанкционированных действий.

О письме впервые сообщил Bleeping Computer, и официальный представитель компании подтвердил CNN Business, что личная информация была потеряна во время атаки программы-вымогателя.

Атака на Colonial Pipeline, в результате которой значительная часть Восточного побережья оставалась без газа в течение нескольких дней, положила начало быстрому изменению реакции правительства на инциденты с программами-вымогателями. После атаки было выпущено несколько новых правил для важнейших отраслей в целом, а также для нефтегазовой отрасли в частности.

В итоге Colonial выплатила группе DarkSide выкуп в размере 4,4 миллиона долларов из-за срочности газового кризиса, но правоохранительным органам США удалось вернуть часть выкупа.

Из-за возросшего интереса правоохранительных органов во всем мире люди, стоящие за DarkSide, закрыли свою деятельность, а некоторые участники реформировались под новым названием: BlackMatter.

The Record поговорил с операторами BlackMatter, которые особо назвали атаку Colonial Pipeline "ключевым фактором закрытия REvil и DarkSide", добавив, что группа теперь "запретила такой тип таргетинга, и мы не видим смысла атаковать их.» ***(Jonathan Greig. Colonial Pipeline sends breach letters to more than 5,000 after ransomware group accessed SSNs, more // ZDNet (https://www.zdnet.com/article/colonial-pipeline-sends-breach-letters-to-more-than-5000-after-ransomware-group-accessed-ssns-more/). 16.08.2021).***

***

**«Правительство Бразилии опубликовало заметку, в которой говорится, что в пятницу Национальное казначейство подверглось атаке с использованием программ-вымогателей (13).**

Согласно заявлению Министерства экономики, первоначальные меры по сдерживанию воздействия кибератаки были приняты немедленно. Первые оценки пока что показали, что системам структурирования Национального казначейства, таким как платформы, относящиеся к управлению государственным долгом, не было нанесено никакого ущерба.

Последствия атаки программ-вымогателей анализируются специалистами по безопасности из Национального казначейства и Секретариата цифрового правительства (DGS). Федеральная полиция также была уведомлена. В министерстве отметили, что новая информация об инциденте «будет раскрыта своевременно и с должной прозрачностью».

В еще одном заявлении, опубликованном сегодня совместно с Бразильской фондовой биржей (16), отмечалось, что атака «никоим образом» не повлияла на работу Tesouro Direto - программы, позволяющей покупать бразильские государственные облигации физическими лицами.

Инцидент в Национальном казначействе последовал за крупной кибератакой, которая произошла в ноябре 2020 года против Высшего избирательного суда Бразилии. В результате атаки системы Суда остановились более чем на две недели.

В то время это событие считалось наиболее масштабной атакой, когда-либо организованной против бразильского государственного сектора, с точки зрения его сложности и масштабов нанесенного ущерба.

В июле правительство Бразилии объявило о создании сети реагирования на кибератаки, направленной на содействие более быстрому реагированию на киберугрозы и уязвимости посредством координации между органами федерального правительства.

СГД, действующая в рамках Специального секретариата по управлению и цифровому правительству Министерства экономики, будет играть стратегическую роль в формировании сети. DGS - центральный орган SISP, системы, используемой для планирования, координации, организации, эксплуатации, контроля и надзора за ресурсами информационных технологий федерального правительства в более чем 200 органах.

В частном секторе в основных атаках программ-вымогателей, которые произошли в 2021 году в Бразилии, были задействованы такие крупные компании, как медицинская фирма Fleury и аэрокосмический конгломерат Embraer». ***(Angelica Mari. Brazilian National Treasury hit with ransomware attack // ZDNet (https://www.zdnet.com/article/brazilian-national-treasury-hit-with-ransomware-attack/). 17.08.2021).***

***

**«Внезапное исчезновение одной из самых распространенных программ-вымогателей заставило мошенников переключиться на другие формы программ-вымогателей, и одна из них, в частности, стала очень популярной.**

Revil - также известный как Sodinokibi - вымогатели банда потемнела в июле, вскоре после того, как найти себе привлечь внимание Белого дома следующих массовых вымогателей атаки, что сказалось 1500 организаций по всему миру.

Пока неясно, ушли ли REvil навсегда или они вернутся под другим брендом, но партнеры схемы вымогателей не ждут, чтобы узнать; они переходят на использование программ-вымогателей других производителей, и, согласно анализу исследователей кибербезопасности Symantec, вымогатели LockBit стали их предпочтительным оружием.

LockBit впервые появился в сентябре 2019 года, а в январе 2020 года разработчики добавили схему вымогателя как услуги, позволяющую киберпреступникам сдавать в аренду LockBit для запуска атак программ-вымогателей в обмен на сокращение прибыли.

LockBit не так популярен, как некоторые другие формы программ-вымогателей, но те, кто его использует, зарабатывают деньги на выкупных платежах, выплачиваемых в биткойнах.

Теперь очевидное исчезновение REvil привело к увеличению числа киберпреступников, которые обращаются к LockBit для проведения атак с использованием программ-вымогателей - при этом авторы LockBit приложили усилия, чтобы предложить обновленную версию.

«LockBit в последние недели агрессивно рекламирует новых партнеров. Во-вторых, они заявляют, что имеют новую версию своей полезной нагрузки с гораздо

более высокими скоростями шифрования. Для злоумышленника, чем быстрее вы сможете зашифровать компьютеры до того, как ваша атака будет раскрыта, тем больше будет ущерб вы вызовете», - сказал ZDNet Дик О'Брайен, старший редактор Symantec.

Исследователи отмечают, что многие из тех, кто сейчас использует LockBit, используют те же тактики, инструменты и процедуры, которые они использовали ранее при попытках доставить REvil жертвам - они просто переключили полезную нагрузку.

Эти методы включают в себя использование незащищенных брандмауэров и уязвимостей VPN или атаки методом грубой силы на службы протокола удаленного рабочего стола (RPD), оставленные доступными в Интернет, а также использование инструментов, включая Mimikatz и Netscan, для помощи в установлении доступа к сети, необходимого для установки вымогателей.

И, как и другие группы программ-вымогателей, злоумышленники LockBit также используют атаки с двойным вымогательством, крадут данные у жертвы и угрожают опубликовать их, если выкуп не будет уплачен.

Несмотря на то, что до сих пор он несколько пролетал незамеченным, злоумышленники, использующие LockBit, использовали его в попытке атаки вымогателя против Accenture - хотя компания заявила, что это не имело никакого эффекта, поскольку они смогли восстановить файлы из резервной копии.

LockBit также привлек внимание служб национальной безопасности; Австралийский центр кибербезопасности (ACSC) выпустил на этой неделе предупреждение о LockBit 2.0, предупреждая о росте атак. Программы-вымогатели представляют угрозу для организаций независимо от того, какой бренд используется. Тот факт, что одна известная группа, казалось бы, исчезла - на данный момент - это не означает, что программы-вымогатели представляют меньшую угрозу.

«Мы считаем LockBit сравнимой угрозой. Это не просто программа-вымогатель, это умение злоумышленников, развертывающих ее. В обоих случаях злоумышленники, стоящие за угрозами, весьма искусны», - сказал О'Брайен.

«В краткосрочной перспективе мы ожидаем, что Lockbit по-прежнему будет одним из семейств программ-вымогателей, наиболее часто используемых в целевых атаках. Долгосрочные перспективы зависят от того, вернутся ли некоторые из недавно ушедших разработчиков программ-вымогателей, такие как REvil и Darkside», - добавил он…». ***(Danny Palmer. One big ransomware threat just disappeared. Now another one has jumped up to fill the gap // ZDNet (https://www.zdnet.com/article/one-big-ransomware-threat-just-disappeared-now-another-one-has-jumped-up-to-fill-the-gap/). 13.08.2021).***

***

**«Австралийский центр кибербезопасности назвал программы-вымогатели «высшей киберугрозой», с которой сталкиваются австралийские предприятия.** Согласно отчету Crowdstrike Report за 2020 год, более двух третей (67%) австралийских организаций пострадали от атак программ-вымогателей за последние 12 месяцев. Мировая ставка составляет всего 57%. В 33% этих случаев

пострадавшая компания платила выкуп, стоимость которого составляла в среднем 1,25 миллиона австралийских долларов за каждое нарушение. Выплата выкупа предоставляет ресурсы преступным организациям, проводящим эти атаки, и создает у них стимул для проведения новых атак.

Чтобы бороться с этим и позволить австралийским службам связи и правоохранительным органам собирать полезную информацию о том, куда идут деньги от программ-вымогателей, чтобы они могли отслеживать и нацеливаться на ответственные преступные группы, федеральное правительство внесло закон о платежах от программ-вымогателей 2021 (Cth) (Законопроект). Законопроект прошел Палату представителей и должен быть рассмотрен Сенатом.

Законопроект налагает обязательное обязательство на организацию, осуществляющую платеж с использованием программ-вымогателей, по уведомлению Австралийского центра кибербезопасности как можно скорее. Хотя это и не отражено в законопроекте, депутат Тим Уоттс в своем выступлении во втором чтении указал, что уведомление должно быть сделано до того, как организации произведут платеж. За неуведомление будет применяться гражданский штраф в размере 1000 штрафных единиц (в настоящее время 222 000 долларов США). Уведомление должно включать имя и контактные данные организации, то, что ей известно о личности злоумышленника, и описание атаки, включая кошелек криптовалюты, на который был выплачен выкуп, сумму и любые признаки компрометации (технические доказательства личности или методов злоумышленника). Уведомление не допускается ни в одном уголовном процессе, за исключением случаев предоставления ложной или вводящей в заблуждение информации.

Информация, содержащаяся в уведомлении (включая идентификационные данные соответствующей организации), не может быть опубликована в дальнейшем, за исключением процессов правоприменения или если она не будет деидентифицирована и раскрыта с целью информирования лица / общественности о текущих событиях. среда киберугроз.

Обязательство по уведомлению будет, если законопроект будет принят, будет применяться ко всем австралийским организациям, включая все субъекты Содружества (корпоративные и некорпоративные), государственные и территориальные агентства и указанные субъекты частного сектора, но исключая малые предприятия (которые являются субъектами с совокупным оборотом менее более 10 миллионов долларов США), индивидуальные предприниматели, юридические лица без образования юридического лица и благотворительные организации. Это применимо, если данные, компьютер, компьютерный стол или другое устройство находятся в Австралии или используются лицом в Австралии.

Для целей законопроекта атаки программ-вымогателей определяются как включающие широкий спектр ситуаций кибербезопасности, в которых злоумышленник требует оплаты. Определение охватывает ситуации, в которых человек, который знает, что у него нет полномочий для этого, получает доступ к данным, изменяет данные, ухудшает обмен данными с компьютером или с него или ухудшает надежность, безопасность или работу любых данных, хранящихся на диске или другом устройстве. используется для хранения данных с помощью

электронных средств и требует оплаты для прекращения или исправления соответствующей ситуации или последствий несанкционированного доступа, модификации или нарушения.

Несмотря на это, Австралийский центр кибербезопасности рекомендует организациям не платить выкуп во время атаки вымогателя, поскольку нет гарантии, что киберпреступники расшифруют файлы после уплаты выкупа, есть вероятность, что файлы не удастся восстановить (например, если файлы безвозвратно изменяются или удаляются), а ссылка, предоставленная жертве для оплаты и информации, может непреднамеренно установить дополнительное вредоносное ПО в систему или сеть жертвы.

Организации также должны знать о других обязательствах по уведомлению, применяемых в случае утечки данных, включая (но не ограничиваясь):

обязательные обязательства по уведомлению об утечке данных, предусмотренные Законом о конфиденциальности 1988 г. (Cth);

Обязательства по уведомлению в соответствии с уголовным законодательством штата и территории, касающимся серьезных преступлений, подлежащих обвинению, например, в соответствии с Законом о преступлениях 1900 года (NSW).

обязательства по уведомлению в отношении инцидентов информационной безопасности и существенных уязвимостей безопасности в соответствии с APRA Prudential Standard CPS 234; а также

Обязательства по уведомлению, налагаемые предлагаемыми реформами Закона о безопасности критической инфраструктуры 2018 (Cth).

В случае, если вы пострадали от какого-либо нарушения данных, будь то программа-вымогатель или иное, Bird & Bird может помочь проконсультировать по любому уведомлению или другим применимым правовым обязательствам». ***(Sophie Dawson, Emma Croft, Emmanuel Akinyemi. Ransom-where is your money going? Introduction of the Ransomware Payments Bill 2021 (Cth) // MediaWrites (https://mediawrites.law/ransom-where-is-your-money-going-introduction-of-the-ransomware-payments-bill-2021-cth/#page=1). 18.08.2021).***

***

**«Исследователи Heimdal Security обнаружили новую программу-вымогатель, получившую название DeepBlueMagic.** По словам Хеймдаля, это особенно беспокоит, потому что он может отключать инструменты безопасности, которые используют компании, чтобы избежать обнаружения. После отключения средств безопасности программа-вымогатель развертывается и шифрует все жесткие диски, кроме системного. DeepBlueMagic использует другие инструменты, чтобы сделать восстановление дисков невозможным.

Штаммы программ-вымогателей продолжают появляться быстрыми темпами, показывая, что в ближайшее время проблема не будет устранена. Злоумышленники лихорадочно создают опасную нагрузку и развертывают ее быстрее, чем компании могут за ней угнаться.

Профилактика продолжает оставаться главной стратегией, включая использование элементарной кибергигиены. Мы продолжаем видеть успешные

атаки с использованием старых приемов против известных уязвимостей, включая отсутствие многофакторной аутентификации, уязвимости VPN, неспособность исправить известные уязвимости и уязвимости протокола удаленного рабочего стола. Крайне важно оставаться на вершине этих уязвимостей, чтобы предотвратить развертывание известных и новых штаммов вредоносных программ и программ-вымогателей, таких как DeepBlueMagic, в вашей системе и последующий хаос и убытки, которые они могут нанести вашему бизнесу». ***(Linn Foster Freedman. DeepBlueMagic Ransomware Appears on the Scene // Robinson & Cole LLP (https://www.dataprivacyandsecurityinsider.com/2021/08/deepbluemagic-ransomware-appears-on-the-scene/). 19.08.2021).***

***

**«Компания Blackbaud, которая пострадала от утечки данных своих клиентов в результате атаки программы-вымогателя в 2020 году, в которой она признала уплату выкупа в результате атаки с двойным вымогательством [см. Связанные сообщения], столкнулась с множеством коллективных исков после атаки. Дела были объединены в судебные тяжбы между несколькими округами и в настоящее время составляют 29 дел.**

Федеральный судья, наблюдающий за этими делами, отказался отклонить все претензии, которые истцы предъявляли к Блэкбоуду, и постановил, что Блэкбауд должен столкнуться с исками о нарушении Закона о защите прав потребителей Калифорнии (CCPA), ложными и недобросовестными обвинениями в торговой практике, выдвинутыми Флоридой и Истцы из Нью-Йорка и отдельный иск истца из Калифорнии о компрометации медицинской информации.

Судья заявил, что истцы достаточно обоснованно утверждали, что Blackbaud был «бизнесом», как этот термин определен в CCPA, отчасти потому, что Blackbaud был зарегистрированным брокером данных в штате Калифорния.

Судья отклонил несколько требований, предъявленных истцами в соответствии с законом. Мы продолжим следить за этим делом и за защитой Blackbaud от требований CCPA». ***(Linn Foster Freedman. Blackbaud Must Face CCPA Claims in Multi-district Class Action from Data Breach // Robinson & Cole LLP (https://www.dataprivacyandsecurityinsider.com/2021/08/blackbaud-must-face-ccpa-claims-in-multidistrict-class-action-from-data-breach/). 19.08.2021).***

***

**«Eskenazi Health в Индианаполисе перенаправляет пациентов отделения неотложной помощи, прибывающих на машине скорой помощи, в другие больницы, так как она отключила свою сеть после атаки вымогателя 4 августа 2021 года.** Утешение осуществляется «из-за излишней осторожности и для поддержания безопасности и целостности. заботы о наших пациентах »согласно выписке из больницы.

Больница заявила, что в настоящее время не было обнаружено, что нападение затронуло какие-либо данные о сотрудниках или пациентах, хотя больница все еще оценивает инцидент.

Тем не менее, инцидент подтверждает, что отрасль здравоохранения продолжает подвергаться атакам программ-вымогателей и их серьезным последствиям для безопасности пациентов и медицинской помощи». ***(Linn Foster Freedman. Hospital Continues to Divert Patients Over a Week After Ransomware Attack // Robinson & Cole LLP (https://www.dataprivacyandsecurityinsider.com/2021/08/hospital-continues-to-divert-patients-over-a-week-after-ransomware-attack/). 12.08.2021).***

***

**«Количество программ-вымогателей стремительно растет. Согласно отчету Verizon о расследовании утечки данных за 2021 год, он появился в 10% случаев, что более чем вдвое превышает частоту в предыдущем году.** А последний отчет Fortinet о глобальном ландшафте угроз показал, что к концу 2020 года о программах-вымогателях ежедневно сообщалось 17 200 устройств.

Рост числа программ-вымогателей подчеркивает одну из самых серьезных проблем, стоящих перед областью кибербезопасности: нехватку навыков. Хотя дефицит несколько снизился, по- прежнему оценивается отсутствие 3,12 млн специалистов, в соответствии с (ISC) 2 «2020 Кибербезопасность Workforce Study. В то же время в США и во всем мире огромное количество соискателей, многие из которых ищут что-то новое. Итак, как нам соединить эти точки?

Рост числа программ-вымогателей подчеркивает необходимость повышения осведомленности

Чтобы помочь создать прочную основу для осведомленности о цифровых технологиях в обществе, по-прежнему важно повышать осведомленность общественности посредством целевого просвещения по вопросам кибербезопасности. Киберграмотность - необходимый ингредиент для создания киберустойчивости и своевременная возможность для более активного взаимодействия и партнерства между государственным и частным секторами. Ни один из них не может решить проблему в одиночку, и если злонамеренная киберактивность будет продолжаться, то это напрямую затронет как частные, так и государственные организации. Это означает, что они взаимно выигрывают от сотрудничества.

Американский закон о грамотности в области кибербезопасности - это большой шаг со стороны федерального правительства и других организаций в совместной работе над повышением безопасности на всех уровнях. Двухпартийная группа законодателей представила этот законопроект, цель которого - организовать кампанию по повышению грамотности в области кибербезопасности, сосредоточенную на рисках кибербезопасности и опережая киберпреступников, которые продолжают преследовать и разрушать жизнь людей, предприятий, правительства и других организаций. Такое сотрудничество может иметь большое значение для создания культуры осознания безопасности во всей стране.

*Устранение разрыва между работодателями и сотрудниками*

Киберграмотность и осведомленность, безусловно, имеют большое значение в продолжающейся борьбе с злоумышленниками и программами-вымогателями, но как насчет следующего уровня? Очень важно найти профессионалов в области

безопасности для выполнения этих задач, но с учетом процветания программ-вымогателей становится ясно, что это необходимо сделать более приоритетным.

Уровень безработицы в США недавно достиг нового минимума в 5,4 процента, но цифры говорят лишь отчасти - гораздо больше людей, все еще ищущих работу, не учтены в этом числе. Многие из этих соискателей работы - и другие - не обязательно имеют образование в области компьютерных наук или иным образом соответствуют «традиционному» образу профессионала в области кибербезопасности. А в прошлом они могли сразу игнорироваться рекрутерами и менеджерами по найму.

Учитывая, как быстро меняется поле, это уже не так. Расширяя область поиска, организации могут расширять свои кадровые резервы и играть активную роль в сокращении разрыва в навыках. Чтобы помочь людям реализовать свой потенциал, организациям необходимо предоставить соответствующие ресурсы, а кандидаты должны быть готовы воспользоваться этими ресурсами.

Выходя за рамки грамотности, чтобы предоставить возможности для обучения

Государственные и частные организации могут и должны работать вместе, чтобы помочь в борьбе с программами-вымогателями. Часть этой работы должна включать совместную работу по созданию конвейера талантов. Частные организации могут сотрудничать с образовательными учреждениями, например, для создания и развития своих учебных программ по кибербезопасности. Кроме того, есть несколько общественных организаций, которые признают ценность разнообразия в отрасли и предоставляют доступ к контенту и программам, предназначенным для решения проблемы нехватки талантов.

Например, такие организации, как ICMCP и WiCyS, вступают в партнерские отношения с частными организациями для создания доступа к программам обучения и наставничества для женщин и меньшинств, которые хотят перейти или развиваться в области кибербезопасности. Общая цель этих общественных организаций - не только помочь людям начать свою карьеру, но и продвинуться на руководящие должности. Посредством этого приоритезации государственного и частного партнерства общественные организации могут способствовать представительству женщин и меньшинств в рамках кибербезопасности.

*Совместная работа по устранению препятствий*

Пробел в навыках кибербезопасности может сокращаться, но не ожидается, что он исчезнет в ближайшее время, а программы-вымогатели продолжают оставаться серьезной проблемой, которая также не показывает признаков замедления. Чтобы полностью решить эту задачу, отрасль должна работать, чтобы охватить сообщества, которые существуют за пределами типичного стереотипа профессионала в области кибербезопасности, включая женщин и меньшинства. Организации и партнерские группы также должны найти и привлечь множество соискателей по всей стране, ищущих новые возможности.

Группы начинают процесс с партнерства с общественными организациями, которые создают доступ к ресурсам, которые поддерживают различных кандидатов, вступающих в сферу кибербезопасности. С этого момента организации должны продолжать продвигать возможности для роста с помощью программ

обучения и сертификации, которые помогают их сотрудникам не только быстро освоиться, но и развиваться в своих ролях. Безудержное распространение программ-вымогателей является напоминанием о нехватке навыков в области кибербезопасности, но всегда будет другая угроза, с которой можно довольствоваться. Организации должны предпринять новые действия, чтобы получить другой результат, который заполнит цепочку талантов и укрепит позиции корпоративной безопасности». ***(Sandra Wheatley. Scourge of Ransomware Underscores the Cybersecurity Skills Gap // Dice (https://insights.dice.com/2021/08/26/scourge-of-ransomware-underscores-the-cybersecurity-skills-gap/). 26.08.2021).***

***

**«Похоже, что банда вымогателей Ragnarok объявила о закрытии и выпустила главный ключ, который может расшифровать файлы, заблокированные их вредоносным ПО.**

Злоумышленник не оставил записки с объяснением этого шага; внезапно они заменили всех жертв на своем сайте утечки короткой инструкцией по расшифровке файлов.

*Бросился выезд*

Место утечки было лишено визуальных элементов. Все, что осталось, это краткая текстовая ссылка на архив, содержащий мастер-ключ и сопутствующие двоичные файлы для его использования.

Глядя на место утечки, похоже, что банда не планировала закрывать сегодня, а просто стерла все и прекратила свою деятельность.

Ранее сегодня сайт утечки вымогателей Ragnarok показал 12 жертв, добавленных в период с 7 июля по 16 августа, сообщил BleepingComputer провайдер аналитики угроз HackNotice.

Публикуя список жертв на своем веб-сайте, Рагнарок пытался заставить их заплатить выкуп под угрозой утечки незашифрованных файлов, украденных во время вторжения.

Перечисленные компании из Франции, Эстонии, Шри-Ланки, Турции, Таиланда, США, Малайзии, Гонконга, Испании и Италии работают в различных секторах, от производства до юридических услуг.

Эксперт по программам-вымогателям Майкл Гиллеспи сообщил BleepingComputer, что выпущенный сегодня дешифратор Ragnarok содержит главный ключ дешифрования…

Позже исследователь подтвердил, что он может расшифровать случайный файл, что делает утилиту главным дешифратором, который можно использовать для разблокировки файлов с различными расширениями вымогателей Ragnarok.

Универсальный дешифратор для вымогателя Ragnarok в настоящее время находится в разработке. Вскоре он станет доступен в Emsisoft, компании, известной тем, что помогает жертвам программ-вымогателей расшифровывать данные.

Группа вымогателей Ragnarok существует по крайней мере с января 2020 года и заявила о десятках жертв после того, как в прошлом году заговорили об использовании уязвимости Citrix ADC.

Ragnarok - не единственная банда вымогателей, выпустившая ключ дешифрования в этом году

Операция вымогателя Ziggy прекратилась в феврале, а ее оператор поделился файлом с 922 ключами

В мае программа- вымогатель Conti предоставила ВШЭ Ирландии бесплатный дешифратор.

Программа-вымогатель Avaddon закрылась в июне и выпустила ключи дешифрования

Банда вымогателей SynAck, переименованная в El_Cometa, выпустила главные ключи дешифрования как часть этого перехода

Исследователи также предоставили дешифраторы [1, 2, 3], и иногда происхождение этих инструментов оставалось неопределенным, как это произошло с атакой Kaseya». ***(Ionut Ilascu. Ragnarok ransomware releases master decryptor after shutdown // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ragnarok-ransomware-releases-master-decryptor-after-shutdown/). 26.08.2021).***

***

**«SAC Wireless, дочерняя компания Nokia в США, раскрыла утечку данных в результате атаки с использованием программ-вымогателей, когда операторы Conti смогли успешно взломать ее сеть, украсть данные и зашифровать системы.**

Полностью принадлежащая и независимая компания Nokia со штаб-квартирой в Чикаго, штат Иллинойс, работает с операторами связи, крупными владельцами вышек и производителями оригинального оборудования (OEM) по всей территории США.

SAC Wireless помогает клиентам проектировать, строить и модернизировать сотовые сети, включая 5G, 4G LTE, малую соту и FirstNet.

Обнаружена атака после систем, зашифрованных программой-вымогателем Conti

Компания обнаружила, что ее сеть была взломана операторами программ-вымогателей Conti 16 июня, только после развертывания их полезной нагрузки и шифрования систем SAC Wireless.

Дочерняя компания Nokia обнаружила, что личная информация, принадлежащая нынешним и бывшим сотрудникам (а также иждивенцам или бенефициарам их планов медицинского страхования), также была украдена во время атаки с использованием программ-вымогателей 13 августа после судебно-медицинской экспертизы, проведенной с помощью внешних экспертов по кибербезопасности.

«Злоумышленник, Conti, получил доступ к системам SAC, загрузил файлы в свое облачное хранилище, а затем, 16 июня, развернул программу-вымогатель для шифрования файлов в системах SAC», - говорится в письмах с уведомлением об утечке данных, отправленных неизвестному лицу. количество пострадавших.

После завершения судебно-медицинской экспертизы компания считает, что украденные файлы содержат следующие категории личной информации: «имя, дата

рождения, контактная информация (например, домашний адрес, адрес электронной почты и телефон), государственные идентификационные номера (например, водительские права., паспорт или военный билет), номер социального страхования, статус гражданства, рабочая информация (например, титул, зарплата и оценки), история болезни, информация о полисе медицинского страхования, номерные знаки, цифровые подписи, свидетельства о браке или рождении, налог информацию о возврате и имена иждивенцев / бенефициаров».

В ответ на атаку программы-вымогателя SAC принял ряд мер для предотвращения будущих нарушений, в том числе:

изменены правила брандмауэра,

отключенные VPN-соединения,

активированы политики условного доступа к географическому местоположению, чтобы ограничить доступ за пределами США,

проведено дополнительное обучение сотрудников,

развернуты дополнительные инструменты мониторинга сети и конечных точек,

расширенная многофакторная аутентификация,

и развернуты дополнительные инструменты для поиска угроз и обнаружения конечных точек и реагирования на них.

Две недели назад, 12 августа, BleepingComputer обратилась в SAC Wireless за дополнительной информацией об атаке, но представитель компании отказался подтвердить, что она была связана с программой-вымогателем, или предоставить дополнительные сведения.

«SAC известно об инциденте, и в настоящее время мы расследуем этот инцидент», - сказал пресс-секретарь. «По мере того, как мы продолжаем оценивать инцидент, мы связываемся с соответствующими сторонами, чтобы рекомендовать принятие соответствующих мер предосторожности».

*Conti утверждает, что украл 250 ГБ файлов*

Хотя компания отказалась признать атаку программы-вымогателя и не предоставила дополнительной информации о степени ущерба, банда программ-вымогателей Conti на своем сайте утечки сообщила, что они украли более 250 ГБ данных.

Согласно недавнему обновлению, группа программ-вымогателей вскоре утекнет в сеть все украденные файлы, если дочерняя компания Nokia не заплатит требуемый выкуп.

Программа-вымогатель Conti - это частная операция по предоставлению программ- вымогателей как услуги (RaaS), которая, вероятно, контролируется российской киберпреступной группой, известной как Wizard Spider.

Conti делится частью своего кода с печально известной программой-вымогателем Ryuk, чьи каналы распространения TrickBot они начали использовать после того, как Ryuk снизил активность примерно в июле 2020 года.

Банда недавно нарушившая работу ирландской системы здравоохранения Service Executive (HSE) и Департамента здравоохранения (DOH), прося заплатить выкуп $ 20 миллионов после шифрования своих систем.

В мае ФБР также предупредило, что операторы Conti пытались взломать сети более десятка американских организаций здравоохранения и служб быстрого реагирования…». ***(Sergiu Gatlan. Nokia subsidiary discloses data breach after Conti ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/nokia-subsidiary-discloses-data-breach-after-conti-ransomware-attack/). 23.08.2021).***

***

**«Федеральное бюро расследований (ФБР) поделилось информацией об злоумышленнике, известном как OnePercent Group, который активно атакует американские организации с помощью программ-вымогателей как минимум с ноября 2020 года.**

Федеральное правоохранительное агентство США представило индикаторы компрометации, тактики, техники и процедур (TTP), а также меры по смягчению последствий в экстренном предупреждении, опубликованном в понедельник.

«ФБР стало известно о киберпреступной группе, которая идентифицирует себя как «OnePercent Group» и которая использовала Cobalt Strike для увековечения атак программ-вымогателей на американские компании с ноября 2020 года», - заявило ФБР.

«Актеры OnePercent Group шифруют данные и выводят их из систем жертв. Актеры связываются с жертвами по телефону и электронной почте, угрожая раскрыть украденные данные через сеть маршрутизатора (TOR) и чистую сеть, если выкуп не будет выплачен виртуальной валютой».

*Сети жертв взломаны с помощью фишинга*

Злоумышленники используют вредоносные фишинговые вложения электронной почты, которые сбрасывают полезную нагрузку банковского трояна IcedID на системы целей. После заражения трояном злоумышленники загружают и устанавливают Cobalt Strike на скомпрометированных конечных точках для бокового перемещения по сетям жертв.

После сохранения доступа к сетям своих жертв в течение одного месяца и извлечения файлов перед развертыванием полезных нагрузок программы-вымогателя OnePercent зашифрует файлы с использованием случайного восьмисимвольного расширения (например, dZCqciA) и добавит записки о выкупе с уникальным именем, ссылающиеся на сообщения банды. луковый сайт.

Жертвы могут использовать веб-сайт Tor, чтобы получить дополнительную информацию о требуемом выкупе, провести переговоры с злоумышленниками и получить «техническую поддержку».

В большинстве случаев жертв попросят заплатить выкуп в биткойнах, при этом ключ дешифрования будет предоставлен в течение 48 часов после совершения платежа.

По данным ФБР, филиал программы-вымогателя также будет обращаться к своим жертвам, используя поддельные телефонные номера, угрожая утечкой украденных данных, если они не будут связаны с переговорщиком компании.

«После успешного развертывания программы-вымогателя жертва начнет получать телефонные звонки по поддельным телефонным номерам с требованиями

выкупа, и ей будет предоставлен адрес электронной почты ProtonMail для дальнейшего общения», - добавили в ФБР.

«Актеры будут настойчиво требовать разговора с уполномоченным переговорщиком компании-жертвы или иным образом угрожать опубликовать украденные данные.

Приложения и сервисы, используемые операторами OnePercent Group, включают облако AWS S3, IcedID, Cobalt Strike, Powershell, Rclone, Mimikatz, SharpKatz, BetterSafetyKatz, SharpSploit.

*Злоумышленник со связями в REvil, Maze и Egregor*

Флэш-оповещение ФБР не предоставляет подробную информацию о прошлых атаках OnePercent Group или используемом шифровальщике, что затрудняет отнесение их к дочерним компаниям определенной программы-вымогателя как услуги.

Тем не менее, агентство связывало OnePercent Group с известной бандой вымогателей REvil (Sodinokibi), чей сайт утечки данных они использовали для утечки и продажи украденных файлов своих жертв.

«Если выкуп не будет выплачен полностью после «однопроцентной утечки», участники OnePercent Group угрожают продать украденные данные Sodinokibi Group для публикации на аукционе», - заявило ФБР.

BleepingComputer узнал, что злоумышленник, вероятно, является партнером REvil по «картелю», то есть они осуществляют свои собственные атаки и выкуп и работают с REvil только тогда, когда они не могут самостоятельно произвести платеж.

В июне 2020 года банда вымогателей Maze начала перечислять жертв на своих данных, например на сайте, вымогательством которых занималась другая банда вымогателей, известная как LockBit.

Когда мы спросили Maze, почему они это делают, они сказали BleepingComputer, что работают с другими группами, делясь информацией и предоставляя доступ к своей платформе утечки данных.

«Через несколько дней на нашем новостном сайте появится еще одна группа, мы все видим в этом сотрудничестве путь, ведущий к взаимовыгодным результатам как для групп участников, так и для компаний».

«Более того, они используют не только нашу платформу для публикации данных о компаниях, но также наш опыт и репутацию, строя выгодное и прочное будущее. Мы относимся к другим группам как к нашим партнерам, а не как к нашим конкурентам. За каждым успехом стоят организационные вопросы. бизнес», - сказал Мейз BleepingComputer.

Узнав об этом, BleepingComputer придумал термин «картель программ-вымогателей», который вскоре приняли другие операции с программами-вымогателями, чтобы описать, как они начали работать друг с другом.

Управляющие серверы, упомянутые в списке IOC ФБР (golddisco [.] Top и june85 [.] Cyou), также указывают на злоумышленника UNC2198, известного тем, что он использует ICEDID для развертывания программ-вымогателей Maze и Egregor.

Те же IOC также упоминались в отчете Team Cymru от мая 2021 года о картировании активной сетевой инфраструктуры IcedID». ***(Sergiu Gatlan. FBI: OnePercent Group Ransomware targeted US orgs since Nov 2020 // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fbi-onepercent-group-ransomware-targeted-us-orgs-since-nov-2020/). 23.08.2021).***

***

**«Новый анализ образца вымогателя Diavol показывает более четкую связь с бандой, стоящей за ботнетом TrickBot, и эволюцией вредоносного ПО.**

Недавнее исследование - второе, которое находит точки соприкосновения в коде двух угроз, связывая их с одним и тем же субъектом.

*Ранний образец имеет подсказки*

Предыдущий анализ программы-вымогателя Diavol (румынский для дьявола), проведенный лабораторией Fortinet FortiGuard Labs, выявил ряд сходств с вредоносным ПО TrickBot, а также различия, которые не позволили установить достоверную атрибуцию кода.

В оценке Fortinet в начале июля было отмечено, что и Diavol, и Conti - семейство программ-вымогателей, тесно связанных с TrickBot, - использовали одни и те же параметры командной строки для различных задач (протоколирование, шифрование, сканирование).

Отчет аналитиков угроз IBM X-Force Шарлотты Хаммонд и Криса Кариди дает подсказки, указывающие на более сильную связь между программой-вымогателем Diavol и бандой TrickBot.

В отличие от образца, проанализированного Fortinet, который был более новым, «полностью функциональным и оснащенным оружием вымогателем», тот, который исследовала IBM, представляет собой более старый вариант, более близкий к разрабатываемой версии, используемой для целей тестирования.

Неполное состояние вредоносной программы содержало признаки, которые позволили исследователям сделать более надежный вывод.

IBM X-Force изучила образец, отправленный в Virus Total 27 января 2021 года, с заявленной датой компиляции 5 марта 2020 года. Для сравнения, дата компиляции версии в анализе Fortinet - 30 апреля 2021 года.

Исследователи заметили, что программа-вымогатель Diavol собирала основную информацию из зараженной системы и генерировала идентификатор системы или бота, который помогает злоумышленнику отслеживать множественные вторжения со стороны филиалов в операции «программа-вымогатель как услуга» (RaaS).

Формат идентификатора бота программы-вымогателя Diavol включает имя хоста, имя пользователя и версию Windows скомпрометированной системы, а также глобальный уникальный идентификатор (GUID). Аналитики отмечают, что формат «практически идентичен» формату, создаваемому вредоносной программой TrickBot.

Очень похожий шаблон идентификатора бота был замечен с Anchor DNS, еще одним вредоносным ПО, приписываемым банде TrickBot, говорят исследователи в своем отчете.

Идентификаторы жертвы важны для операторов вредоносных программ, поскольку они могут отслеживать успех различных кампаний и сообщать об этом аффилированным лицам.

Исследователи также отмечают, что HTTP-заголовки для взаимодействия с сервером управления и контроля (C2) были «настроены так, чтобы отдавать предпочтение русскоязычному контенту», что также одобряется операторами TrickBot.

Еще одна подсказка, указывающая на российских злоумышленников, - это код для проверки языка скомпрометированной системы для фильтрации жертв в России или в регионе Содружества Независимых Государств (СНГ).

Хотя Fortinet не нашла этот код проверки языка в проанализированном ими образце вымогателя Diavol, IBM заявляет, что в разрабатываемой версии обнаружены признаки того, что такой код «мог присутствовать или предназначался для разработки, даже если он не был активирован в скомпилированной версии». образцы».

Учитывая разные стадии разработки двух вариантов вымогателя Diavol и время их обнаружения, становится ясно, что вредоносное ПО развивается.

IBM X-Force не нашла убедительных доказательств связи программы-вымогателя Diavol с бандой TrickBot, но обнаружила новые признаки, указывающие на связь.

Но между их отчетом и выводом Fortinet о том, что вредоносное ПО функционирует так же, как Conti, баланс атрибуции, похоже, заметно смещается в сторону TrickBot». ***(Ionut Ilascu. Diavol ransomware sample shows stronger connection to TrickBot gang // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/diavol-ransomware-sample-shows-stronger-connection-to-trickbot-gang/). 18.08.2021).***

***

**«Tokio Marine Holdings, транснациональная страховая холдинговая компания в Японии, объявила на этой неделе, что ее сингапурский филиал Tokio Marine Insurance Singapore (TMiS) подвергся атаке с использованием программ-вымогателей.**

Объявление было сделано в начале недели и содержит мало информации об инциденте, помимо действий, предпринятых для борьбы с вторжением.

*Ограниченная атака*

Tokio Marine Holdings, являясь крупнейшей (с точки зрения доходов) группой по страхованию имущества и от несчастных случаев в Японии, является привлекательной целью для киберпреступников, которые могут использовать взлом для поиска и компрометации клиентов организации.

Tokio Marine отмечает, что атака с использованием программ-вымогателей затронула Tokio Marine Insurance Singapore и что другие компании группы в стране не пострадали.

Неясно, как и когда произошла атака и какой ущерб она причинила, но TMiS изолировала сеть сразу после ее обнаружения и проинформировала органы местного самоуправления.

Материнская компания заявляет, что она может «подтвердить отсутствие признаков нарушения какой-либо информации о клиентах или конфиденциальной информации Группы».

Большинство атак программ-вымогателей в наши дни также рассматриваются как инциденты утечки данных, поскольку злоумышленник также крадет файлы из сети жертвы перед их шифрованием.

Однако была привлечена третья сторона для анализа систем и оценки воздействия атаки.

Компания сообщила об инциденте на своем веб-сайте как на японском, так и на английском языках, извиняясь перед своими клиентами за любые «доставленные неудобства и опасения».

*Вспышка атак на страховщиков*

Тим Старков из CyberScoop нот, что Tokio Marine является вторым страховщиком на этой неделю, чтобы объявить о кибер - атаке, Райана Специализация группа также раскрывать в понедельник, что в апреле он обнаружен несанкционированный доступ на некоторых счетах сотрудников.

Однако в начале этого года некоторые из крупных страховых компаний стали жертвами атак программ-вымогателей.

В марте CNA Financial Corporation - седьмая по величине коммерческая страховая компания в США - была взломана программой- вымогателем Phoenix CryptoLocker, которая также похитила файлы, содержащие информацию о клиентах.

В мае банда вымогателей Avaddon ударила по филиалам AXA в Таиланде, Малайзии, Гонконге и на Филиппинах, заявив о краже 3 ТБ данных.

Призыв вымогателя к страховым компаниям объяснил представитель банды вымогателей REvil в интервью ранее в этом году Дмитрию Смилянецу, аналитику разведки Recorded Future.

Под псевдонимом Неизвестный представитель банды заявил, что страховые компании - «один из самых вкусных кусков». Их взлом дает злоумышленнику доступ к клиентской базе компании, а затем он в конце поражает страховщика». (***Ionut Ilascu. Japanese insurer Tokio Marine discloses ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/japanese-insurer-tokio-marine-discloses-ransomware-attack/). 18.08.2021).***

***

**«Вероятно, вдохновленный бандой вымогателей LockBit, нигерийский злоумышленник попытал счастья с помощью платежной приманки на 1 миллион долларов, чтобы нанять инсайдера, который взорвал полезную нагрузку вымогателя на серверах компании.**

План сработал, когда мошенник выбрал не ту цель, раскрывая свою технику, а также отсутствие опыта и навыков разведки.

*Предложение на миллион долларов*

Несколько сообщений, отправленных во входящие, защищенные облачной платформой безопасности электронной почты Abnormal Security, привлекли

внимание исследователей из-за предложения отправителя для получателя: выплаты в размере 1 миллиона долларов за развертывание вымогателя в сети.

Demonware (также известное как Black Kingdom) - это проект вымогателей с открытым исходным кодом, доступный на GitHub и обычно развертываемый отдельными лицами, менее техническими специалистами. Однако актер утверждал, что это их проект на языке Python.

Исследователи отреагировали на приглашение злоумышленника поболтать, представившись сотрудником, который хотел немного заработать, пишет сегодня в блоге Крейн Хассолд, директор по анализу угроз компании Abnormal Security.

Поскольку в представлении больше не было необходимости, злоумышленник доставил полезную нагрузку программы-вымогателя, и разговор продолжался через Telegram, давая представление о мотивации и технических способностях мошенника.

По мере продолжения чата актер продолжал снижать выплату сначала до 250 000 долларов, а затем до 120 000 долларов, что явным признаком того, что они не знакомы с тем, как ведется игра с программами-вымогателями.

Злоумышленник заявил, что пытается попытать счастья с помощью программы-вымогателя для финансирования своего предполагаемого бизнеса, стартапа социальной сети под названием Sociogram, в котором он утверждал, что выступает в качестве генерального директора. Они раскрыли некоторые подробности, заявив, что находятся в Нигерии и поделились профилем LinkedIn, предположительно связанным с их бизнесом.

Эта информация соответствует деталям, которые исследователи обнаружили перед тем, как начать разговор с актером, ища в Интернете данные, связанные с адресом электронной почты в первоначальном сообщении.

Однако более важным для исследователей был метод, использованный для сбора целевых адресов электронной почты. В этом не было ничего сложного: анализировать учетные записи LinkedIn на предмет корпоративных писем, принадлежащих сотрудникам высшего звена.

По словам злоумышленника, они прибегли к программе-вымогателю после безуспешной попытки взломать учетные записи электронной почты с помощью фишинга.

Нигерия наиболее известна в индустрии информационной безопасности как колыбель мошенников, занимающихся компрометацией деловой электронной почты (BEC), поэтому социальная инженерия является распространенной тактикой среди киберпреступников в стране.

Похоже, что нигерийский актер не смог придумать оригинальную приманку и взял страницу из книги LockBit, когда пытался привлечь к работе инсайдера.

В начале месяца BleepingComputer сообщила, что банда вымогателей LockBit объявила, что они ищут корпоративных инсайдеров для помощи в взломе и шифровании сетей.

Группа пообещала миллионы долларов США сотрудникам, которые переключились на их сторону и предоставили учетные данные RDP, VPN или корпоративной электронной почты, которые разрешили доступ к сети». ***(Ionut Ilascu. CEO tried funding his startup by asking insiders to deploy ransomware //***

***Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ceo-tried-funding-his-startup-by-asking-insiders-to-deploy-ransomware/). 19.08.2021).***

***

**«Тайваньский производитель материнских плат Gigabyte подвергся нападению банды вымогателей RansomEXX, которая угрожает опубликовать 112 ГБ украденных данных, если не будет уплачен выкуп.**

Gigabyte наиболее известна своими материнскими платами, но также производит другие компьютерные компоненты и оборудование, такие как видеокарты, серверы центров обработки данных, ноутбуки и мониторы.

Атака произошла поздно вечером вторника в среду и вынудила компанию отключить системы на Тайване. Инцидент также затронул несколько веб-сайтов компании, включая сайт поддержки и отдельные части тайваньского веб-сайта.

Клиенты также сообщали о проблемах с доступом к документам поддержки или получении обновленной информации о RMA, что, вероятно, связано с атакой программы-вымогателя.

Согласно китайскому новостному сайту United Daily News, Gigabyte подтвердила, что подверглась кибератаке, затронувшей небольшое количество серверов.

Обнаружив аномальную активность в своей сети, они отключили свои ИТ-системы и уведомили правоохранительные органы.

Gigabyte подвергается атаке вымогателя RansomEXX

Хотя Gigabyte официально не сообщила, какая операция вымогателя выполнила атаку, BleepingComputer узнал, что ее провела банда RansomEXX.

Когда операторы RansomEXX шифруют сеть, они создают записки о выкупе на каждом зашифрованном устройстве.

Эти записки о выкупе содержат ссылку на непубличную страницу, которая должна быть доступна только жертве для проверки расшифровки одного файла и для оставления адреса электронной почты для начала переговоров о выкупе.

Сегодня источник отправил BleepingComputer ссылку на закрытую страницу утечки RansomEXX для Gigabytes Technologies, где злоумышленники утверждают, что во время атаки украли 112 ГБ данных.

В записке о выкупе, которую также видел BleepingComputer, злоумышленники заявляют: «Привет, Gigabyte (gigabyte.com)!» и включите ту же ссылку на частную страницу утечки, которой поделился с нами наш источник.

На этой частной странице утечки злоумышленники утверждают, что украли 112 ГБ данных из внутренней сети Gigabyte, а также из репозитория Git American Megatrends,

Мы скачали 112 ГБ (120 971 743 713 байт) ваших файлов и готовы ОПУБЛИКОВАТЬ их.
Многие из них находятся под NDA (Intel, AMD, American Megatrends).
Источники утечки: newautobom.gigabyte.intra, git.ami.com.tw и некоторые другие.

Злоумышленники также поделились скриншотами четырех документов по соглашению о неразглашении, украденных во время атаки.

Хотя мы не будем публиковать просочившиеся изображения, конфиденциальные документы включают отладочный документ American Megatrends, документ Intel «Возможные проблемы», «График обновления стека SKU Ice Lake D» и руководство AMD по пересмотру.

BleepingComputer попытался связаться с Gigabyte по поводу атаки, но в настоящее время не получил ответа.

*Что нужно знать о RansomEXX*

Операция вымогателя RansomEXX первоначально началась под названием Defray в 2018 году, но в июне 2020 года была переименована в RansomEXX, когда они стали более активными.

Как и другие операции с программами-вымогателями, RansomEXX может взломать сеть с помощью протокола удаленного рабочего стола, эксплойтов или украденных учетных данных.

Получив доступ к сети, они будут собирать больше учетных данных, постепенно получая контроль над контроллером домена Windows. Во время этого бокового распространения по сети банда вымогателей будет красть данные с незашифрованных устройств, которые используются в качестве рычага для вымогательства выкупа.

RansomEXX не только нацелен на устройства Windows, но также создал шифровальщик Linux для шифрования виртуальных машин, на которых работают серверы VMware ESXi.

За последний месяц банда RansomEXX стала более активной, поскольку они недавно атаковали регион Лацио в Италии и государственную корпорацию Эквадора «Корпорасьон Насьональ де Телекомуникасьон» (CNT)…». ***(Lawrence Abrams. Computer hardware giant GIGABYTE hit by RansomEXX ransomware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/computer-hardware-giant-gigabyte-hit-by-ransomexx-ransomware/). 06.08.2021).***

***

**«Недавно обнаруженный вариант программы-вымогателя eCh0raix добавил поддержку шифрования устройств QNAP и Synology Network-Attached Storage (NAS).**

Этот штамм вымогателя (также известный как QNAPCrypt) впервые появился в июне 2016 года после того, как жертвы начали сообщать об атаках в теме форума BleepingComputer.

Программа-вымогатель поразила устройства NAS от QNAP несколькими волнами, две из которых были зарегистрированы в июне 2019 года и в июне 2020 года.

eCh0raix также зашифровал устройства, созданные Synology в 2019 году, при этом исследователи Anomali обнаружили, что злоумышленники подобрали учетные данные администратора путем перебора, используя учетные данные по умолчанию или словарные атаки.

В то время производитель NAS предупредил своих клиентов, чтобы они защищали свои данные от продолжающейся крупномасштабной кампании вымогателей. Однако он не назвал операцию вымогателя, ответственную за атаки.

*Цели, установленные для клиентов Synology и QNAP*

Хотя в прошлом он нацелился на устройства QNAP и Synology в рамках отдельных кампаний, исследователи безопасности Unit 42 из Palo Alto Networks заявили в опубликованном сегодня отчете, что eCh0raix начал объединять функции для шифрования обоих семейств NAS, начиная с сентября 2020 года.

«До этого у злоумышленников, вероятно, были отдельные кодовые базы для кампаний, нацеленных на устройства от каждого из поставщиков», - сказал Unit 42.

Как они далее выяснили, операторы программ-вымогателей используют CVE-2021-28799 (уязвимость, обеспечивающую злоумышленникам доступ к жестко закодированным учетным данным, также известным как бэкдор-аккаунт) для шифрования устройств QNAP - тот же недостаток был использован в крупномасштабной кампании Qlocker в Апрель.

Злоумышленники используют грубую силу, чтобы доставить полезные данные программы-вымогателя на устройства Synology NAS, пытаясь угадать обычно используемые учетные данные администратора (та же тактика, использованная в кампании Synology 2019, упомянутой выше).

Несмотря на то, что компания Synology не подключила его напрямую к программе-вымогателю eCh0raix, на прошлой неделе компания Synology выпустила рекомендацию по безопасности, в которой клиентам сообщалось, что ботнет StealthWorker активно нацеливает их данные на текущие атаки методом грубой силы, которые могут привести к заражению программами-вымогателями.

QNAP также уведомила клиентов об атаках программ-вымогателей eCh0raix в мае, всего через две недели после того, как предупредила их о продолжающейся эпидемии вымогателей AgeLocker.

Устройства QNAP также пострадали от масштабной кампании вымогателей Qlocker, начавшейся с середины апреля, когда злоумышленники заработали 260 000 долларов всего за пять дней, заблокировав данные жертв с помощью файлового архиватора с открытым исходным кодом 7zip.

Не менее 250 000 устройств NAS подвержены атакам.

Согласно данным, собранным с помощью платформы Cortex Xpanse Palo Alto Networks, существует не менее 250 000 подключенных к Интернету устройств QNAP и Synology NAS.

Исследователи Unit 42 советуют владельцам Synology и QNAP NAS следовать этому короткому списку передовых методов для блокирования атак программ-вымогателей, направленных на их данные:

Обновите прошивку устройства, чтобы предотвратить подобные атаки. Подробную информацию об обновлении устройств QNAP NAS от CVE-2021-28799 можно найти на веб-сайте QNAP.

Создавайте сложные пароли для входа, чтобы злоумышленники усложнили взлом.

Ограничьте подключения к устройствам, подключенным к SOHO, только с помощью жестко запрограммированного списка распознанных IP-адресов, чтобы предотвратить сетевые атаки, используемые для доставки программ-вымогателей на устройства.

«Мы публикуем наши выводы об этом новом варианте eCh0raix, чтобы повысить осведомленность о текущих угрозах для секторов SOHO и малого бизнеса», - добавил Unit 42.

«Пользователи SOHO привлекательны для операторов программ-вымогателей, которые хотят атаковать более крупные цели, потому что злоумышленники потенциально могут использовать устройства SOHO NAS в качестве ступеньки в атаках цепочки поставок на крупные предприятия, которые могут принести огромные выкуп». ***(Sergiu Gatlan. eCh0raix ransomware now targets both QNAP and Synology NAS devices // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ech0raix-ransomware-now-targets-both-qnap-and-synology-nas-devices/). 10.08.2021).***

***

**«Исследователи безопасности, расследующие несколько кампаний по распространению вредоносных программ, обнаружили, что подпольная служба распределения трафика под названием Prometheus отвечает за доставку угроз, которые часто приводят к атакам программ-вымогателей.**

Среди семейств вредоносных программ, которые компания Prometheus TDS представила на данный момент, - BazarLoader, IcedID, QBot, SocGholish, Hancitor и Buer Loader, и все они обычно используются на промежуточных этапах атаки для загрузки более опасной полезной нагрузки.

*Служба доставки троянцев*

Система направления трафика (TDS) позволяет перенаправлять пользователей к контенту на основе конкретных характеристик (например, местоположения, языка, типа устройства), которые определяют дальнейшие действия.

Такие инструменты злоумышленники используют более десяти лет. В отчете Trend Micro за 2011 год подробно рассказывается об обновлении ботнета Koobface компонентом TDS, который увеличил прибыль за счет привлечения трафика на сайты партнерской рекламы.

Исследователи из компании Group-IB, занимающейся кибербезопасностью, обнаружили, что операция Prometheus TDS Malware-as-a-Service (MaaS) рекламируется на подпольных форумах как минимум с августа 2020 года за 250 долларов в месяц.

Пользователь по имени Main продвигает его как «профессиональную систему перенаправления» с защитой от ботов, которая подходит для электронного маркетинга, генерации трафика и социальной инженерии.

Prometheus использует сеть веб-сайтов, зараженных бэкдором, доступным из панели администрирования сервиса, где клиенты могут создать профиль для своих целей.

Исследователи говорят, что пользователи могут быть перенаправлены на веб-сайт, зараженный Prometheus.Backdoor через кампанию электронной почты, доставляющую HTML-файл с перенаправлением, или ссылку на веб-оболочку, ведущую на взломанный сайт, или документ Google, указывающий на вредоносный URL-адрес.

Когда пользователи попадают на взломанный веб-сайт, Prometheus.Backdoor на основе PHP собирает сведения о подключении (IP-адрес, пользовательский агент, заголовок реферера, часовой пояс, язык) и перенаправляет их в панель администратора.

Вредоносный код часто скрывается во вредоносных документах Microsoft Word или Excel, хотя также использовались архивы ZIP и RAR.

В ходе расследования команда Group-IB Threat Intelligence обнаружила более 3000 целевых адресов электронной почты в кампаниях, в которых использовался Prometheus TDS.

Некоторые из целевых почтовых ящиков принадлежали правительственным агентствам, компаниям и корпорациям США в сфере банковского и финансового права, розничной торговли, энергетики и горнодобывающей промышленности, кибербезопасности, здравоохранения, информационных технологий и страхования.

При исследовании кампаний по распространению вредоносного ПО Prometheus TDS исследователи обнаружили десятки вредоносных документов Office, которые доставляли Campo Loader (также известный как BazarLoader), Hancitor, QBot, IcedID, Buer Loader и SocGholish.

Все перечисленные выше троянов являются вредоносными программами загрузчиков, участвующие в течение прошлого года в более ранних стадиях вымогателей атаки (WastedLocker, RYUK, эгрегор, RansomExx, Revil, Куба, Conti).

Однако команда Group-IB Threat Intelligence сообщила BleepingComputer, что они не могут связать Prometheus TDS с атаками программ-вымогателей, поскольку они исследовали вредоносные файлы в виртуальной среде.

После загрузки вредоносного ПО некоторые вредоносные документы перенаправляли пользователей на легитимные веб-сайты (DocuSign, USPS), чтобы замаскировать заражение вредоносным ПО.

*Поддельный VPN, спам и подбор паролей*

Помимо вредоносных программ, Prometheus TDS также использовался для перенаправления пользователей на сайты, предлагающие поддельные решения VPN, продающие фармацевтические продукты (спам Viagra) или фишинговые страницы с банковской информацией.

Тот, кто стоит за Prometheus, также использует другую службу под названием BRChecker - инструмент для подбора паролей, который разделяет инфраструктуру, используемую службой TDS.

Group-IB обнаружила, что реклама BRChecker была выпущена еще в середине июня 2018 года от пользователя по имени Mainin, что очень похоже на то, что продвигает Prometheus.

Исследователи сообщили BleepingComputer, что совпадение функциональности и инфраструктуры указывает на то, что у обеих служб один и тот же разработчик.

Обе системы активны, поскольку исследователи ежедневно видят новые веб-сайты, зараженные Prometheus.Backdoor. Кроме того, административные панели появляются регулярно, что является явным признаком новых клиентов». ***(Ionut Ilascu. Prometheus TDS: The $250 service behind recent malware attacks // Bleeping***

***Computer® (https://www.bleepingcomputer.com/news/security/prometheus-tds-the-250-service-behind-recent-malware-attacks/). 05.08.2021).***

***

**«Компанія Eset повідомляє про зростання активності програм-вимагачів. Найчастіше загрози поширюються через протокол віддаленого робочого столу (RDP), електронну пошту та ланцюг постачання.** За даними телеметрії Eset, тільки за період з січня 2020 р. до червня 2021 р. кількість виявлених спроб атак методом підбору пароля на RDP перевищила 71 млрд.

Іншим способом проникнення програми-вимагача на пристрій може стати протокол SMB, який використовується переважно для спільного використання файлів та принтерів у корпоративних мережах. За період з січня до квітня 2021 р. технології Eset заблокували 335 млн. спроб атак методом підбору пароля до служб SMB.

Крім цього, популярним способом поширення програм-вимагачів залишається розсилка спаму зі шкідливими макросами, посиланнями та виконуваними файлами ботнетів. Зокрема кіберзлочинці використовують небезпечні вкладення електронної пошти для встановлення на пристрій жертви шкідливого програмного забезпечення. Згодом загроза може бути використана для викрадення цінних даних та шифрування всіх файлів користувачів.

Також збільшилась кількість атак програм-вимагачів на ланцюг постачання, що підтверджується численними дослідженнями Eset. Зокрема за період з листопада 2020 р. до лютого 2021 р. тільки спеціалісти Eset виявили чотири випадки атак на ланцюг постачання. Крім цього, нещодавно жертвою програм-вимагачів став постачальник Kaseya. Використавши «0-денну» уразливість в його продукті, кіберзлочинці змогли зашифрувати дані понад 100 компаній.

Для збільшення шансів отримати викуп зловмисники постійно застосовують техніки посилення тиску на жертву. Зокрема останні два роки кіберзлочинці активно використовують прийом «подвійного» вимагання, яке поєднує шифрування даних з шантажем жертви щодо оприлюднення конфіденційної інформації у разі несплати викупу. Деякі зловмисники пішли ще далі, звертаючись до партнерів або клієнтів жертви, яка не сплатила викуп, з пропозицією чинити тиск на неї. У деяких випадках кіберзлочинці навіть вимагали оплати від партнерів чи клієнтів.

Крім цього, за останні роки також змінилися підходи хакерів до вибору цілей – від великої кількості випадкових користувачів до цілеспрямованого вибору з вимогою більших сум викупу. Жертвами все частіше стають ті організації та компанії, які не можуть дозволити собі втратити доступ до своїх даних або контроль над ними. У середньому розмір викупу програм-вимагачів становить близько 170 тис. дол.

Варто зазначити, виплата викупу не гарантує того, що кіберзлочинці відновлять доступ до даних. Однак така плата зловмисникам допомагає фінансувати майбутні злочини, через що наразі обговорюється визнання таких дій незаконними.

Варто зазначити, щороку технології Eset виявляють мільйони атак з використанням програм-вимагачів. Зокрема власна технологія захисту від атак методом підбору пароля в період з січня 2020 р. до квітня 2021 р. ефективно виявила і заблокувала загалом близько 55 млрд. спроб атак на майже 1 млн. користувачів. Тоді як понад 300 тис. користувачів завантажили один із загальнодоступних інструментів Eset для запобігання інфікуванню програмами-вимагачами.

Крім цього, компанія Eset приєдналася до міжнародної ініціативи No More Ransom, заснованої правоохоронними органами та компаніями з IT-безпеки з метою допомоги жертвам програм-вимагачів у відновленні даних. З моменту свого створення інструменти для розшифрування, доступні на платформі No More Ransom, безкоштовно відновили дані понад 6 млн. користувачів. Завдяки цьому зловмисники не змогли заробити на своїх атаках майже мільярд євро». ***(Одним з найпопулярніших способів поширення програм-вимагачів є атаки на RDP // Компьютерное Обозрение (https://ko.com.ua/odnim_z_najpopulyarnishih_sposobiv_poshirennya_program-vimagachiv_ye_ataki_na_rdp_138342). 11.08.2021).***

***

**«Крупнейшая в Бразилии сеть магазинов одежды Lojas Renner подверглась кибератаке с использованием вымогательского ПО, в результате которой некоторые ее IT-системы оказались недоступны.**

Lojas Renner впервые сообщила об инциденте во время биржевых торгов в четверг, 19 августа. Как утверждали местные СМИ и блогеры, атака привела к закрытию всех физических магазинов Lojas Renner в Бразилии. Однако на следующий день компания подала второй документ с целью развеять слухи и уверить акционеров в том, что все магазины продолжают работать, а атака затронула только подразделение электронной коммерции.

Подробностей об атаке Lojas Renner не раскрывает, но, как сообщает один из бразильских блогов, за ней может стоять кибервымогательская группировка RansomExx, получившая доступ к серверам компании через крупнейшего в Бразилии поставщика цифровых и IT-услуг Tivit. Однако в интервью CNN Brazil Business представители Tivit опровергли данное заявление и уверили в том, что ни их корпоративная сеть, ни серверы взломаны не были.

Хотя компания и подтвердила факт кибератаки, она попыталась приуменьшить ее значение, заявив, что ее главная база данных не была взломана или зашифрована. Тем не менее, удалось ли злоумышленникам похитить данные с скомпрометированных серверов, на которых вероятнее всего хранятся данные сайтов электронной коммерции, не сообщается. Если RansomExx действительно причастна к атаке, скорее всего, группировка похитила данные перед шифрованием.

По словам анонимного источника издания The Record, Lojas Renner заплатила вымогателям $20 млн, но сама компания пока никак не комментирует это заявление.

В любом случае, Lojas Renner вполне могла позволить себе заплатить такую сумму. Компания является одной из крупнейших в Южной Америке – управляет более 600 магазинов в трех странах под брендами Renner, Camicado, Youcom и Ashua». ***(Крупнейшая в Бразилии сеть магазинов одежды Lojas Renner подверглась атаке вымогателей // SecurityLab.ru (https://www.securitylab.ru/news/523624.php). 23.08.2021).***

***

**«После серии разрушительных атак на топливного гиганта Colonial Pipeline и крупнейшего в мире поставщика мяса JBS с использованием программ-вымогателей на киберпреступных форумах были запрещены публикации, связанные с вымогательским ПО. Но группировки нашли способы обойти данный запрет, сообщило издание The Daily Beast.**

Киберпреступники проявили изобретательность перед лицом новых запретов и теперь планируют свои атаки так, чтобы избежать подозрений со стороны правоохранительных органов.

Один из пользователей форумов XSS и Exploit размещал сообщения, предлагая «помощь» другим пользователям, которые взломали компьютерные сети компании и имели различные возможности доступа. Пользователь «хотел помочь другим людям с доступом к уязвимым виртуальным частным сетям (VPN), но которые не знали, что с ним делать».

Другой пользователь на форуме XSS рекламировал якобы «команду опытных пентестеров», которые хотят купить доступ к уязвимым корпоративным сетям. Такое поведение типично для намерения сотрудничества с программами-вымогателями.

По словам экспертов, желающие заключить партнерство с операторами вымогателей, начинают ставить «лайки» чужим сообщениям на криминальных форумах с целью привлечь внимание киберпреступников и связаться с ними по частным каналам». ***(Хакеры используют специальные шифры для обсуждения вымогателей на подпольных форумах // SecurityLab.ru (https://www.securitylab.ru/news/523605.php). 20.08.2021).***

***

## *Програми-трояни*

---

**«Эксперты из области кибербезопасности американской компании AT&T провели исследования и опубликовал отчет относительного нового трояна, который получил распространение в Telegram, — FatalRat.** По результатам исследования стало понятно, что он обладает определенными уникальными способностями и сложно устроен. Активно распространяться троян стал в последние несколько месяцев. В основном это касается групповых чатов, а также интернет-форумов. Киберпреступники используют средства маскировки, чтобы вирус имел возможность проникнуть в систему компьютера пользователя. Так его внедряют в пиратские копии Windows и в публикации СМИ. Что такое

FatalRat Это троян, относящийся к категории RAT, обладает широкими функциональными возможностями. Прежде чем произойдет заражение компьютера, вирус проверяет систему на нескольких важных параметров. В первую очередь он анализирует объем свободного дискового пространства, наличие виртуальных машин, число процессоров и прочее. Отдельно он получает сведения о степени защищенности персонального компьютера жертвы – есть антивирус или нет, если установлен, то какой. В системе остается надолго за счет того, что автоматически добавляется в список автозагрузок и в дальнейшем маскируется под системные процессы. После заражения системы он способен отслеживать действия пользователя, удалять важную информацию, перехватывать текст, который вводится при помощи клавиатуры. Известно, что если пользователь начнет стирать логин и пароль с формы Google, вирус заставит повторно вводить их, перехватит текст и отправит его в центр управления. Также FatalRat умеет производить анализ локальных сетей. Он запускает процессы с подбором наиболее распространенных паролей. Эксперты убеждены, что в дальнейшем FatalRat будет распространяться еще активней. Ситуацию может усугубить появление других версий троянов, основанных на этом виде. Как защититься от вируса? Правила предосторожности прежние – не переходить по подозрительным ссылкам, установить антивирус и поддерживать его базы сигнатур в актуальном состоянии». ***(В Telegram распространяют опасный вирус RAT // информационный портал "ua.today" (http://ua.today/news/technology_and_science/v_telegram_rasprostranyayut_opasnyj_virus_rat). 17.08.2021).***

***

**«Фирма Zimperium, занимающаяся кибербезопасностью, обнаружила новый троян для Android, который в понедельник опубликовал отчет, в котором объясняется, как вредоносной программе удалось поразить более 10 000 жертв в 144 странах.**

Троян, названный исследователями Zimperium FlyTrap, с марта может распространяться через «захват социальных сетей, сторонние магазины приложений и загружаемые неопубликованные приложения».

Группы исследования мобильных угроз Zimperium zLabs сначала определили вредоносное ПО и выяснили, что оно использует приемы социальной инженерии для взлома учетных записей Facebook. Вредоносная программа захватывает учетные записи социальных сетей, заражая устройства Android, позволяя злоумышленникам собирать информацию от жертв, такую как идентификатор Facebook, местоположение, адрес электронной почты и IP-адрес, а также файлы cookie и токены, привязанные к вашей учетной записи Facebook.

«Эти захваченные сеансы Facebook могут быть использованы для распространения вредоносного ПО путем злоупотребления авторитетом жертвы в обществе посредством личных сообщений со ссылками на троян, а также для пропаганды или дезинформации с использованием данных о геолокации жертвы», - пишут исследователи Zimperium.

«Эти методы социальной инженерии очень эффективны в мире цифровых технологий и часто используются киберпреступниками для распространения вредоносных программ от одной жертвы к другой. Злоумышленники использовали несколько тем, которые могут показаться пользователям привлекательными, например, бесплатные коды купонов Netflix, Google AdWords. коды купонов и голосование за лучшую футбольную команду или игрока».

Исследователи отнесли вредоносное ПО к группам, базирующимся во Вьетнаме, и заявили, что они могут распространять его через Google Play и другие магазины приложений. В Google отправили отчет о вредоносном ПО, проверили его и удалили все приложения магазина.

Но в отчете отмечается, что три приложения все еще доступны в «сторонних, незащищенных репозиториях приложений».

Как только жертвы убеждают загрузить приложение с помощью обманного дизайна, приложение побуждает пользователей к взаимодействию и в конечном итоге просит людей ввести данные своей учетной записи Facebook, чтобы проголосовать за что-то или получить коды купонов. Как только все введено, приложение выводит жертв на экран, на котором указано, что срок действия купона уже истек.

Исследователи объяснили, что вредоносная программа использует метод под названием «JavaScript-инъекция», который позволяет приложению открывать допустимые URL-адреса внутри «WebView, настроенного с возможностью внедрения кода JavaScript». Затем приложение извлекает такую информацию, как файлы cookie, данные учетной записи пользователя, местоположение и IP-адрес, путем внедрения вредоносного JS-кода.

Zimperium предлагает пользователям Android найти способы проверить, есть ли у каких-либо приложений на их устройстве FlyTrap, и отметил, что эти взломанные учетные записи могут использоваться в качестве ботнета для других целей, таких как повышение популярности определенных страниц или сайтов.

«FlyTrap - лишь один из примеров продолжающихся активных угроз для мобильных устройств, направленных на кражу учетных данных. Мобильные конечные точки часто являются сокровищницей незащищенной информации для входа в учетные записи социальных сетей, банковских приложений, корпоративных инструментов и многого другого», - говорят исследователи Zimperium.

«Инструменты и методы, используемые FlyTrap, не новы, но эффективны из-за отсутствия продвинутой защиты мобильных конечных точек на этих устройствах. Злоумышленнику не потребуется много времени, чтобы захватить FlyTrap или любой другой троян и изменить его, чтобы нацелить еще больше. критическая информация».

Сету Кулкарни, вице-президент NTT Application Security, сказал, что FlyTrap представляет собой «отличную комбинацию» нескольких уязвимостей и использует в своих интересах обилие открытых для доступа метаданных, таких как местоположение, а также неявное доверие, которое можно получить. умными, но сомнительными ассоциациями с такими компаниями, как Google, Netflix и другими.

«Это даже не самый тревожный момент - он связан с сетевым эффектом, который этот тип трояна может вызвать, распространяясь от одного пользователя ко многим. Более того, как говорится в сводке результатов Zimperium, этот троян мог быть эволюционирован для эксфильтрации значительно более важная информация, такая как банковские реквизиты», - сказал Кулкарни.

«Сценарии «что, если», к сожалению, на этом не заканчиваются. Что, если этот тип трояна теперь предлагается как услуга, или что, если он быстро превратится в программу-вымогатель, нацеленную на сотни тысяч пользователей. Итог не изменится. Он не изменится. все начинается с пользователя, которого соблазняют щелкнуть ссылку. Возникает вопрос - не должны ли Google и Apple делать больше для решения этой проблемы для всей своей клиентской базы?» ***(Jonathan Greig. Android Trojan hijacks social media in 140 countries hits 10,000 victims // ZDNet (https://www.zdnet.com/article/android-trojan-hits-140-countries-10000-victims-through-social-media-hijacking/). 09.08.2021).***

***

**«Вредоносная версия мода FMWhatsappWhatsApp предоставляет полезную нагрузку Triadatrojan, неприятный сюрприз, который заражает их устройства дополнительными вредоносными программами, включая очень трудно удаляемый троян xHelper.**

FMWhatsApp обещает улучшить пользовательский интерфейс WhatsApp с помощью дополнительных функций, таких как улучшенная конфиденциальность, настраиваемые темы чата, доступ к пакетам смайликов других социальных сетей и блокировка приложений с помощью PIN-кода, пароля или сенсорного идентификатора.

Однако, как выяснили исследователи «Лаборатории Касперского», версия FMWhatsapp 16.80.0 также будет сбрасывать троян Triada на устройства пользователей с помощью рекламного SDK.

«Это приложение было доступно на некоторых популярных сайтах распространения модов WhatsApp. Однако мы не можем делиться ссылками на них», - сказал BleepingComputer эксперт по безопасности Kaspersky Игорь Головин.

«Что касается [клонов FMWhatsApp] в Google Play - эти приложения обычно содержат только различную рекламу и инструктируют пользователей о том, как загружать и устанавливать моды, но на самом деле не содержат самих вредоносных модов».

Троянец собирает информацию об устройстве и устанавливает больше вредоносных программ

После установки Triada начинает сбор информации об устройстве и отправляет ее на свой командно-управляющий сервер, который отвечает ссылкой на дополнительную полезную нагрузку, которую троян загрузит и запустит на скомпрометированном устройстве Android.

По словам Касперского, Triada будет загружать и запускать на целевые устройства несколько типов дополнительных вредоносных программ, в том числе:

Trojan-Downloader.AndroidOS.Agent.ic, скачивающий и запускающий другие вредоносные модули.

Trojan-Downloader.AndroidOS.Gapac.e, устанавливающий другие вредоносные модули и показывающий полноэкранную рекламу.

Trojan-Downloader.AndroidOS.Helper.a устанавливает модуль установки троянца xHelper и запускает невидимую рекламу в фоновом режиме.

Trojan.AndroidOS.MobOk.i подписывает владельца Android-устройства на платную подписку.

Trojan.AndroidOS.Subscriber.l также подписывает жертв на премиальные подписки.

Trojan.AndroidOS.Whatreg.b собирает информацию и запрашивает код подтверждения для входа в учетные записи WhatsApp жертв.

Вредоносное ПО, сброшенное Triada на устройства Android пользователей FMWhatsApp, может легко подписать их на премиум-подписку, учитывая, что приложение запрашивает доступ к текстовым сообщениям жертв при установке.

«С этим приложением пользователям трудно распознать потенциальную угрозу, потому что мод-приложение действительно делает то, что предлагается - оно добавляет дополнительные функции», - сказал Головин.

«Однако мы наблюдали, как киберпреступники начали распространять вредоносные файлы через рекламные блоки в таких приложениях. Поэтому мы рекомендуем использовать только программное обеспечение для обмена сообщениями, загруженное из официальных магазинов приложений.

«У них могут отсутствовать некоторые дополнительные функции, но они не установят на ваш смартфон кучу вредоносных программ».

*Неубиваемый и практически невозможно удалить xHelper*

Среди вредоносных программ, поставляемых Triada, xHelper выделяется своей необычайной способностью повторно заражать устройства Android через несколько часов после удаления или после сброса зараженных устройств до заводских настроек.

Впервые обнаруженный Malwarebytes в марте 2019 года, когда он начал медленно распространяться на более чем 32000 устройств Android, xHelper в конечном итоге заразил в общей сложности 45000 устройств до октября 2019 года.

xHelper использует «веб-перенаправления», чтобы обмануть цели, заставляя их загружать вредоносные APK-файлы из сторонних магазинов приложений Android, при этом установленные приложения загружают и запускают троян xHelper.

Троян переживает попытки удаления, копируя себя в системный раздел, который монтируется заново в режиме записи. Он также заменяет системную библиотеку libc.so, чтобы заблокировать полный доступ к монтированию и запретить пользователям использовать тот же метод для его удаления.

Хотя полная перепрошивка системы Android на зараженных устройствах является наиболее надежным способом избавиться от xHelper, Malwarebytes придумал второй метод, который включает установку бесплатного приложения Malwarebytes для Android». ***(Sergiu Gatlan. Malicious WhatsApp mod infects Android devices with malware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/malicious-whatsapp-mod-infects-android-devices-with-malware/). 24.08.2021).***

***

## Технічні аспекти кібербезпеки

**«Ученые из инженерной школой Тандон Нью-Йоркского университета проверили систему на базе искусственного интеллекта GitHub Copilot с точки зрения безопасности и обнаружили, что примерно в 40% случаев сгенерированный помощником по программированию код в лучшем случае содержит ошибки, а в худшем — потенциально уязвим к атакам.**

Согласно статье An Empirical Cybersecurity Evaluation of GitHub Copilot's Code Contributions («Эмпирическая оценка кибербезопасности вклада кода GitHub Copilot»), исследователи создали для Copilot 89 сценариев по разработке кода, в результате чего было создано 1692 программы. Как оказалось, около 40% решений содержали уязвимости или конструктивные недостатки, которые могут быть использованы злоумышленником.

Copilot доступен для частного бета-тестирования в качестве расширения Microsoft Visual Studio Code. Система позволяет разработчикам описывать функциональные возможности в строке комментариев, а затем пытается сгенерировать код, соответствующий описанию. Copilot также может предсказать по именам переменных и функций и другим подсказкам, что разработчик собирается написать дальше.

Исследователи рассмотрели три отдельных аспекта результатов Copilot: степень, в которой он генерирует код, отображающий список 25 наиболее часто встречающихся уязвимостей; вероятность того, что различные подсказки генерируют уязвимости внедрения SQL-кода; и как он обрабатывает предложения кода для менее популярных языков (например, Verilog).

По словам специалистов, в ряде случаев Copilot создавал на языке C, использующий указатели из malloc (), не проверяя, что они не равны NULL, код со встроенными учетными данными, код, который передавал ненадежные пользовательские вводимые данные прямо в командную строку, а также код, отображающий более четырех последних цифр номера социального страхования США». ***(Система на базе ИИ GitHub Copilot примерно в 40% случаев создает уязвимый код // SecurityLab.ru (https://www.securitylab.ru/news/523751.php). 26.08.2021).***

***

## *Виявлені вразливості технічних засобів та програмного забезпечення*

**«Команда исследователей Check Point Research (CPR) обнаружила уязвимости в самой популярной в мире «читалке» для электронных книг Amazon Kindle, воспользовавшись которыми, хакеры могли бы получить**

**полный контроль над Kindle пользователя, похитить токен устройства и другие сохраненные на нем конфиденциальные данные. Для успешной атаки на Kindle достаточно одной книги с вредоносным кодом.**

Потенциальная атака начинается с отправки вредоносной электронной книги на почту пользователя. После получения такого вложения жертве достаточно открыть его – и это запустит цепочку действий по эксплуатации устройства. Каких-либо дополнительных разрешений и действий со стороны пользователя не требуется. Специалисты CPR доказали, что электронные книги могут использоваться в качестве вредоносного ПО для Kindle с различными последствиями. Например, хакер может удалить все электронные книги пользователя, или превратить Kindle во вредоносного бота и использовать его для атак на другие устройства в локальной сети пользователя.

Кроме того, обнаруженные уязвимости позволяли злоумышленникам атаковать конкретную категорию пользователей. Например, чтобы выбрать определенную группу людей или демографическую группу, киберпреступнику достаточно было использовать популярную электронную книгу на соответствующем языке или диалекте. В результате кибератака становилась узконаправленной.

CPR сообщила о своих выводах Amazon в феврале. Апрельское обновление прошивки Kindle до версии 5.13.5 содержало патч для обнаруженных уязвимостей. С ним прошивка автоматически устанавливается на подключенные к сети устройства.

«Как и другие умные устройства, Kindle часто воспринимается как безобидный гаджет, не подверженный рискам безопасности. Однако наши исследования показывают, что любое устройство с возможностью подключения к сети, по сути, мало отличается от компьютера. Любые подключенные к ПК устройства, особенно такие распространенные как Kindle, представляют риск с точки зрения кибербезопасности, и пользователи должны это осознавать», – говорит Янив Балмас, руководитель исследований в сфере кибербезопасности компании Check Point Software Technologies». ***(Электронная книга с вредоносным кодом может дать хакерам полный контроль над Amazon Kindle // Компьютерное Обозрение (https://ko.com.ua/jelektronnaya_kniga_s_vredonosnym_kodom_mozhet_dat_hakeram_polnyj_kontrol_nad_amazon_kindle_138312). 09.08.2021).***

***

**«Аналитики по кибербезопасности обнаружили критические уязвимости в чипах Realtek, которые затрагивают более 65 производителей оборудования и различные беспроводные устройства.** Уязвимости были обнаружены компанией IoT Inspector, создателем одноименной платформы для анализа безопасности встроенного ПО, в ходе анализа двоичных файлов, являющихся частью SDK Realtek. Уязвимости могут быть использованы злоумышленниками удаленно для полной компрометации уязвимых устройств и выполнения произвольного кода с максимальным уровнем привилегий. Список производителей оборудования, пострадавших от уязвимостей Realtek, включает Asus, Belkin, D-

Link, Edimax, Logitech, Netgear, ZTE и других, и охватывает столь же широкий спектр устройств, от шлюзов для жилых помещений до туристических маршрутизаторов, повторителей Wi-Fi, IP-камер, интеллектуальных молниеотводов и даже игрушек. Исследователи уведомили Realtek об уязвимости, и патч был выпущен незамедлительно. IoT Inspector призывает производителей, использующих уязвимые модули Wi-Fi, проверить свои устройства и незамедлительно предоставить исправления безопасности своим пользователям». ***(Уязвимости в ПО Realtek ставят под угрозу сотни тысяч маршрутизаторов и IoT-устройств // информационный портал "ua.today" (http://ua.today/news/technology_and_science/uyazvimosti_v_po_realtek_stavyat_pod_ugrozu_sotni_tysyach_marshrutizatorov_i_iot_ustrojstv). 18.08.2021).***

***

**«Компания Cisco недавно объявила, что не будет выпускать обновления программного обеспечения для устранения уязвимости с помощью службы Universal Plug-and-Play (UPnP) в маршрутизаторах Cisco Small Business RV110W, RV130, RV130W и RV215W.**

Уязвимость позволяет удаленному злоумышленнику, не прошедшему проверку подлинности, выполнить произвольный код или вызвать неожиданный перезапуск уязвимого устройства, что приведет к отказу в обслуживании (DoS).

«Эта уязвимость возникает из-за неправильной проверки входящего UPnP-трафика. Злоумышленник может воспользоваться этой уязвимостью, отправив созданный UPnP-запрос на уязвимое устройство. Успешный эксплойт может позволить злоумышленнику выполнить произвольный код от имени пользователя root в базовой операционной системе или вызвать перезагрузку устройства, что приведет к состоянию DoS», - говорится в заявлении Cisco.

«Cisco не выпускала обновлений программного обеспечения, устраняющих эту уязвимость. Не существует способов обхода этой уязвимости».

Уязвимость затрагивает маршрутизаторы серии RV только в том случае, если на них настроен UPnP, но служба UPnP включена по умолчанию на интерфейсах LAN и отключена по умолчанию на интерфейсах WAN.

Компания объяснила, что, чтобы выяснить, включена ли функция UPnP на LAN-интерфейсе устройства, пользователи должны открыть веб-интерфейс управления и перейти в «Основные настройки»> «UPnP». Если флажок «Отключить» не установлен, на устройстве включен UPnP.

Cisco заявила, что, хотя отключение уязвимой функции оказалось успешным в некоторых тестовых средах, заказчики должны «определить применимость и эффективность в своей собственной среде и в своих собственных условиях использования».

Они также предупредили, что любое обходное решение или смягчение последствий может повредить работе или работе их сети. Cisco призвала клиентов перейти на маршрутизаторы Cisco Small Business RV132W, RV160 или RV160W.

Уязвимость и уведомление Cisco вызвали незначительный переполох среди ИТ-руководителей, некоторые из которых заявили, что для ее эксплуатации требуется, чтобы злоумышленник имел доступ к внутренней сети, который можно

легко получить с помощью фишингового сообщения электронной почты или другими способами.

Джейк Уильямс, технический директор BreachQuest, добавил, что, оказавшись внутри, злоумышленник может использовать эту уязвимость, чтобы легко получить контроль над устройством с помощью эксплойта.

«Уязвимые устройства широко используются в небольших бизнес-средах. Некоторые крупные организации также используют устройства для удаленных офисов. Уязвимость заключается в uPnP, который предназначен для динамической перенастройки брандмауэров для внешних служб, которым необходимо пропускать трафик, входящий из Интернета», - сказал Уильямс ZDNet.

«Хотя uPnP - чрезвычайно полезная функция для домашних пользователей, ей нет места в бизнес-средах. Cisco, вероятно, оставит функцию uPnP включенной в своей линейке продуктов для малого бизнеса, потому что в этих средах с меньшей вероятностью будет выделенный персонал службы поддержки, который может перенастроить брандмауэр как в таких условиях персоналу нужно все, чтобы «просто работало». В области безопасности мы должны помнить, что каждая функция также является дополнительной поверхностью атаки, ожидающей использования».

Уильямс добавил, что даже без уязвимости, если включен uPnP, злоумышленники внутри среды могут использовать его для открытия портов на брандмауэре, пропуская опасный трафик из Интернета.

«Поскольку уязвимые устройства почти всегда используются в среде малого бизнеса, с небольшим количеством сотрудников службы технической поддержки, они почти никогда не обновляются», - отметил он.

Генеральный директор Vulcan Cyber Янив Бар-Даян сказал, что UPnP - это очень злонамеренная служба, используемая в большинстве подключенных к Интернету устройств, по оценкам, более 75% маршрутизаторов имеют UPnP.

Хотя группа реагирования на инциденты, связанные с безопасностью продуктов Cisco, заявила, что до сих пор не знала о злонамеренном использовании этой уязвимости, Бар-Даян сказал, что UPnP использовался хакерами для получения контроля над всем, от IP-камер до сетевой инфраструктуры предприятия.

Другие эксперты, такие как старший консультант по безопасности приложений nVisium Зак Варнелл, добавили, что устройства очень часто редко - или никогда - получают обновления.

«Пользователи, как правило, хотят оставить все в покое и не прикасаться к хорошо работающему устройству, в том числе, когда ему требуются важные обновления. Часто пользователи также пользуются преимуществами функции plug-and-play, поэтому они делают очень мало или совсем ничего изменения конфигурации, оставляя устройство в состоянии по умолчанию и, в конечном счете, уязвимым», - сказал Варнелл.

Глобальный вице-президент New Net Technologies по исследованиям в области безопасности Дирк Шрейдер добавил, что, хотя UPnP является одной из наименее известных утилит для среднего потребителя, он широко используется в

сетевых устройствах SOHO, таких как DSL или кабельный маршрутизатор, устройства WLAN, даже в принтерах.

«UPnP присутствует почти во всех домашних сетевых устройствах и используется устройством для поиска других сетевых устройств. Ранее он был целью, и одна из крупных ботнетов, Mirai, в значительной степени полагалась на UPnP. Учитывая, что названные устройства Cisco размещены в сегменте SOHO и SMB владельцы, скорее всего, не знают о UPnP и о том, что он делает», - сказал Шрейдер.

«Это, а также тот факт, что обходной путь или исправление пока недоступны, представляют собой довольно опасную комбинацию, поскольку установленная база определенно немала. Можно надеяться на то, что - по умолчанию - UPnP не включен на интерфейсах WAN. уязвимого устройства Cisco, только на стороне локальной сети. Поскольку потребители вряд ли изменят это, для использования этой уязвимости злоумышленникам, похоже, потребуется другое, уже установленное место в локальной сети. Но злоумышленники проверит уязвимость и увидят что еще можно с этим сделать». ***(Jonathan Greig. Cisco says it will not release software update for critical 0-day in EOL VPN routers // ZDNet (https://www.zdnet.com/article/cisco-not-planning-to-fix-critical-0-day-rce-vulnerability-in-eol-vpn-routers/). 27.08.2021).***

***

**«Недавно обнаруженная уязвимость в чипсетах тайваньской полупроводниковой компании Realtek стала мишенью ботнета, основанного на старом вредоносном ПО для Интернета вещей Mirai.**

Немецкая компания по безопасности IoT Inspector сообщает, что ошибка Realtek, отслеживаемая как CVE-2021-35395, затрагивает более 200 продуктов Wi-Fi и маршрутизаторов от 65 поставщиков, включая Asus, Belkin, China Mobile, Compal, D-Link, LG, Logitec, Netgear, ZTE и Zyxel.

Уязвимость находится в комплекте разработчика программного обеспечения (SDK) Realtek и в настоящее время подвергается атаке со стороны группы, использующей вариант вредоносного ПО для Интернета вещей, Mirai, которое предназначено для работы на устройствах с бюджетными процессорами и небольшим объемом памяти.

Если атака будет успешной, она предоставит злоумышленнику полный контроль над модулем Wi-Fi и root-доступ к операционной системе устройства.

Атаки выявляют уязвимости в цепочке поставок программного обеспечения, которые президент США Джо Байден надеется исправить с помощью миллиардов долларов, обещанных на этой неделе Microsoft и Google. Это последовало за недавними кибератаками на критически важную инфраструктуру США, которые поставили под угрозу ведущие компании США по кибербезопасности и классических поставщиков критически важной инфраструктуры, таких как дистрибьютор топлива на восточном побережье Colonial Pipeline.

Хотя Mirai представляет некоторую угрозу для информации, хранящейся на таких устройствах, как маршрутизаторы, больший ущерб наносят мощные распределенные атаки типа «отказ в обслуживании» (DDoS) на веб-сайты с

использованием взломанных устройств. В 2016 году Mirai был использован для запуска крупнейшей в мире DDoS-атаки на Dyn - поставщика службы доменных имен (DNS), который сопоставляет имена веб-сайтов с числовыми интернет-адресами. Oracle приобрела фирму вскоре после атаки Mirai.

Исследователи IoT Inspector обнаружили ошибку в модуле Realtek RTL819xD, которая позволяет хакерам получить «полный доступ к устройству, установленным операционным системам и другим сетевым устройствам». Фирма выявила несколько уязвимостей в SDK.

Realtek выпустила патч, но производители устройств (OEM-производители) должны распространять их среди конечных пользователей на устройствах, которые по большей части не имеют пользовательского интерфейса и, следовательно, не могут использоваться для сообщения о наличии патча. Производителям необходимо проанализировать свою прошивку, чтобы проверить наличие уязвимости.

«Производителям, использующим уязвимые модули Wi-Fi, настоятельно рекомендуется проверять свои устройства и предоставлять своим пользователям исправления безопасности», - предупредил Флориан Лукавски, управляющий директор IoT Inspector.

Злоумышленник, как правило, должен находиться в той же сети Wi-Fi, что и уязвимое устройство, но IoT Inspector отметил, что неправильные конфигурации интернет-провайдера могут открыть доступ к уязвимым устройствам напрямую в Интернет.

Согласно данным охранной фирмы Recorded Future, компания SAM, занимающаяся безопасностью Интернета вещей, сообщила, что 18 августа злоумышленники удаленно использовали CVE-2021-35395 через Интернет.

IoT Inspector отмечает, что плохая практика разработки программного обеспечения Realtek и отсутствие тестирования позволили «десяткам критических проблем безопасности остаться нетронутыми в кодовой базе Realtek более десяти лет». ***(Liam Tung. Cybersecurity warning: Realtek flaw exposes dozens of brands to supply chain attacks // ZDNet (https://www.zdnet.com/article/realtek-hardware-bugs-expose-dozens-of-brands-to-supply-chain-cyber-attack/). 26.08.2021).***

***

**«Группа перспективных исследований McAfee Enterprise представила новое исследование уязвимостей, обнаруженных в насосах, созданных немецким гигантом здравоохранения Б. Брауном.**

В отчете описываются проблемы с насосом большого объема Infusomat Space и SpaceStation Б. Брауна, которые предназначены для использования в медицинских учреждениях для взрослых и детей. Инфузионные насосы предназначены для того, чтобы помочь медсестрам и врачам избежать трудоемких ручных инфузий и приобрели известность в последние годы, поскольку многие больницы переводят свои системы в цифровую форму.

Согласно исследованию, злоумышленники могут воспользоваться уязвимостями, чтобы изменить настройку помпы в режиме ожидания, позволяя доставлять пациентам измененные дозы лекарств без каких-либо проверок.

Операционная система помпы не проверяет, откуда поступают команды и кто отправляет ей данные, что дает кибератакам пространство для удаленной атаки. Использование неаутентифицированных и незашифрованных протоколов также дает злоумышленникам множество возможностей получить доступ к внутренним системам помпы, которые регулируют, сколько каждого лекарства должно быть доставлено пациенту.

«Злоумышленники могут использовать несколько уязвимостей нулевого дня, чтобы создать угрозу множеству критических сценариев атаки, что может резко увеличить скорость выдачи лекарств пациентам. Медицинские учреждения должны активно отслеживать эти угрозы с особым вниманием, пока не будет выпущен полный набор исправлений и эффективно адаптировано клиентами B. Braun, говорится в исследовании группы McAfee Advanced Threat Research.

«Благодаря постоянному диалогу с Б. Брауном, McAfee Enterprise ATR раскрыла уязвимость и узнала, что последняя версия помпы удаляет исходный сетевой вектор цепочки атак».

Дуглас Макки, Стив Повольни и Филипп Лаулхере, члены группы McAfee по исследованию передовых угроз, объясняют в своем отчете, что изменение количества лекарств, вводимых пациенту, будет выглядеть как простая неисправность устройства и «будет замечено только после пациенту было выдано значительное количество лекарственного средства, поскольку инфузионный насос показывает именно то, что было прописано, и все это при выдаче потенциально смертельных доз лекарства».

McAfee отметил, что ежегодно во всем мире проводится более 200 миллионов внутривенных инфузий с использованием насосов, подобных тем, которые поставляет B. Braun. Компания является одним из лидеров на рынке насосов для внутривенных вливаний, который в 2020 году принес в США 13,5 млрд долларов.

Шон Нордек, врач, работающий в травматологическом центре 1-го уровня, внес свой вклад в исследование и сказал, что возможность удаленного манипулирования медицинским оборудованием незамеченным, что может нанести вред пациенту, эффективно превращает эти устройства для оказания медицинской помощи в оружие.

«Этот сценарий ранее был возможен только в Голливуде, но теперь подтвержден как реальный вектор атаки на критически важное оборудование, которое мы используем ежедневно», - сказал Нордек об исследовании. «Атаки программ-вымогателей, нацеленные на нашу отрасль, основаны на подобных уязвимостях; именно поэтому данное исследование так важно для понимания и упреждающего предотвращения атак».

McAfee проинформировал Б. Брауна об уязвимостях в январе, и с тех пор компания обновила насосы для решения проблемы. Но возникновение проблемы открывает совершенно новый набор атак, которые можно использовать, если будут обнаружены другие сетевые уязвимости. В отчете отмечается, что, хотя Б. Браун устранил проблемы, во многих больницах все еще используются уязвимые инструменты и программное обеспечение.

«Медицинская отрасль на протяжении многих лет сильно отставала от других в сфере безопасности - пора отказаться от цифровых «пластырей» медленного и реактивного исправления и принять целостное «лекарство», ориентируясь на безопасность прежде всего. «на ранних стадиях разработки в сочетании с быстрым и эффективным решением для исправления», - сказали Макки, Повольни и Лаулхерет.

В итоге McAfee обнаружила пять отдельных новых уязвимостей, связанных с насосами - CVE-2021-33886, CVE-2021-33885, CVE-2021-33882, CVE-2021-33883 и CVE-2021-33884, которые охватывают B. Насос большого объема Infusomat модели 871305U от Braun, док-станция SpaceStation модели 8713142U, вмещающая до 4 насосов, и программный компонент под названием SpaceCom версии 012U000050, все из которых были выпущены в 2017 году.

«При рассмотрении того, как помпа и ее коммуникационный модуль обрабатывают связь и обработку файлов, мы заметили, что важные файлы не подписаны (CVE-2021-33885), большая часть обмена данными осуществляется в виде обычного текста (CVE-2021-33883), а также полное отсутствие аутентификации (CVE-2021-33882) для используемых проприетарных протоколов», - говорится в отчете.

Исследователи безопасности ранее обнаружили уязвимости кибербезопасности в инфузионных насосах от нескольких компаний, помимо B. Braun, таких как Medtronic, Hospira Symbiq и других. Но недавно правительство Германии опубликовало исследование инфузионных насосов, в том числе от Б. Брауна, в рамках более масштабного исследования кибербезопасности медицинских устройств.

«SpaceCom - это встроенная система Linux, которая может работать либо на насосе из своего интеллектуального аккумулятора, либо изнутри SpaceStation. Однако, когда насос подключается к SpaceStation, SpaceCom насоса отключается», - говорится в исследовании.

«SpaceCom действует как внешний коммуникационный модуль для системы и отделен от внутренних операций насоса, независимо от того, откуда он запущен. Важной функцией SpaceCom является возможность обновлять библиотеку лекарств и конфигурацию насоса, хранящуюся в помпе. Библиотека лекарств содержит такую информацию, как отделение и отделение, список предварительно настроенных лекарств с их концентрациями по умолчанию, информационные сообщения, которые будут выводиться на экран при выборе, и, что более важно, мягкие и жесткие ограничения для предотвращения ошибки приема лекарств».

Отчасти потому, что инфузионные насосы так широко используются сейчас, заключается в том, что они помогают медсестрам автоматически регулировать дозы лекарств, а некоторые системы развертывают базы данных с более чем 1500 парами ключ / значение.

Одна из трудностей, с которой могут столкнуться кибератаки, заключается в том, что ОСРВ насоса не подключена к сети, но для внесения каких-либо изменений требуется доступ к ней.

«Хотя эта цепочка атак представляет собой законченный метод изменения критических данных насоса, важно понимать условия, необходимые для успеха

этой атаки. Эти насосы предназначены для сетевого подключения к локальной внутренней сети», - пояснили исследователи.

«Таким образом, при нормальных условиях эксплуатации злоумышленнику необходимо найти способ получить доступ к локальной сети. Может ли эта атака происходить через Интернет? Технически говоря, да; однако вряд ли можно увидеть установку, в которой насос напрямую подключен к Интернету».

Б. Браун предпринял и другие меры для защиты устройства, в том числе функцию, которая позволяет помпе игнорировать запросы во время доставки лекарства, а это означает, что атака может быть усилена только тогда, когда помпа находится в режиме ожидания или в режиме ожидания между инфузиями. Медсестрам также дано указание проверять дозировку и уровни лекарств, прежде чем что-либо устанавливать, а в правилах многих стран подробно объясняется, как медсестры должны управлять устройством.

Но получить доступ к локальным сетям не так сложно, как раньше, и McAfee отметила, что «предпосылки для этой атаки минимальны и недостаточны для смягчения общей угрозы». После доступа к локальной сети киберпреступники могут предпринять ряд шагов, чтобы упростить свою работу, в том числе очистить текущую конфигурацию доверенного сервера и переписать ее на сервер, контролируемый злоумышленником.

Злоумышленники могут даже перезагрузить всю операцию, чтобы персонал больницы не заметил ни одного из внесенных изменений.

Нордек, который более 20 лет проработал врачом в частных учреждениях и в армии США, сказал, что отделения интенсивной терапии представляют собой среду с высоким давлением, в которой существует повышенный риск ошибок инфузии, поскольку этим критическим и часто сложным с медицинской точки зрения пациентам проводят несколько инфузий, которые часто корректируется.

«Ошибки, однако, не ограничиваются отделением интенсивной терапии и могут также легко возникнуть в стационаре или амбулаторных условиях», - сказал Нордек. «По сути, с каждым увеличением переменной (сложность или острота зрения пациента, количество лекарств, изменение скорости, соотношение медсестер и пациентов и т. Д.) Увеличивается риск ошибки».

Нордек добавил, что «такая рутина, как слишком быстрое исправление высокого уровня сахара в крови или натрия, может вызвать опухание мозга или повреждение нервов, что может привести к необратимой инвалидности или даже смерти».

Хотя исследователи отметили, что атаки программ-вымогателей сейчас гораздо более вероятны, для медицинских учреждений было важно защитить себя от новых атак, которые время от времени возникают.

«Производители устройств явно стремятся производить безопасные и надежные продукты, о чем свидетельствуют встроенные меры безопасности. Однако могут существовать недостатки, которые позволяют устройству поддаться атаке с целью выкупа или потенциально причинить вред», - добавил Нордек.

«Поэтому производители должны сотрудничать со специалистами по безопасности, чтобы независимо тестировать свои продукты для обнаружения и устранения потенциальных угроз и, таким образом, для обеспечения безопасности

пациентов и устройств». ***(Jonathan Greig. B. Braun updates faulty IV pump after McAfee discovers vulnerability allowing attackers to change doses // ZDNet (https://www.zdnet.com/article/b-braun-updates-faulty-iv-pump-after-mcafee-discovers-vulnerability-allowing-attackers-to-change-doses/). 24.08.2021).***

***

**«CISA выпустила предупреждение о некоторых продуктах BlackBerry, подверженных уязвимости BadAlloc, на что в начале этого года обратили внимание исследователи Microsoft.**

Во вторник BlackBerry выпустила уведомление, в котором объясняется, что ее операционная система QNX Real Time, которая используется в медицинских устройствах, автомобилях, заводах и даже на Международной космической станции, может быть подвержена воздействию BadAlloc, который представляет собой набор уязвимостей, влияющих на несколько ОСРВ и вспомогательные библиотеки. BlackBerry недавно похвасталась тем, что операционная система QNX Real Time используется в 200 миллионах автомобилей.

CISA добавила, что устройства IoT, операционные технологии и некоторые промышленные системы управления включают операционную систему реального времени QNX, поэтому необходимо срочно принять меры для защиты систем. BlackBerry опубликовала полный список уязвимых продуктов.

«Удаленный злоумышленник может использовать CVE-2021-22156, чтобы вызвать состояние отказа в обслуживании или выполнить произвольный код на затронутых устройствах. BlackBerry QNX RTOS используется в широком спектре продуктов, компрометация которых может привести к получению злоумышленником контроля над высокочувствительные системы, увеличивающие риск для критически важных функций нации», - говорится в сообщении CISA.

«В настоящее время CISA не осведомлено об активном использовании этой уязвимости. CISA настоятельно рекомендует организациям, занимающимся критической инфраструктурой, и другим организациям, разрабатывающим, обслуживающим, поддерживающим или использующим уязвимые системы на основе QNX, как можно быстрее исправлять уязвимые продукты».

Далее в предупреждении объясняется, что уязвимость связана с «уязвимостью целочисленного переполнения, затрагивающей функцию calloc () в библиотеке времени выполнения C нескольких продуктов BlackBerry QNX».

Чтобы злоумышленники могли воспользоваться уязвимостью, они должны уже иметь «контроль над параметрами вызова функции calloc () и возможность контролировать, к какой памяти осуществляется доступ после выделения».

Доступ к сети позволит злоумышленнику удаленно использовать эту уязвимость, если уязвимый продукт работает и уязвимое устройство доступно в Интернете, добавил CISA.

Уязвимость затрагивает каждую программу BlackBerry, зависящую от библиотеки времени выполнения C.

CISA предупредила, что, поскольку многие из устройств, затронутых уязвимостью, являются «критически важными для безопасности», возможность их

использования может дать кибератакам возможность контролировать системы, управляющие инфраструктурой или другими критически важными платформами.

«CISA настоятельно рекомендует организациям критически важной инфраструктуры и другим организациям, разрабатывающим, обслуживающим, поддерживающим или использующим уязвимые системы на базе QNX, как можно быстрее исправлять уязвимые продукты», - говорится в предупреждении.

«Производители продуктов, которые включают уязвимые версии, должны связаться с BlackBerry для получения исправления. Производители продуктов, которые разрабатывают уникальные версии программного обеспечения RTOS, должны связаться с BlackBerry для получения кода исправления», - пояснил CISA, добавив, что некоторым организациям, возможно, придется создавать собственное программное обеспечение. патчи.

Согласно CISA, некоторые обновления программного обеспечения для OCPB требуют удаления устройств или их переноса за пределы предприятия для физической замены встроенной памяти.

BlackBerry сообщила в своем собственном выпуске, что они еще не видели использованную уязвимость. Компания предложила пользователям продукта убедиться, что «доступны только порты и протоколы, используемые приложением, использующим OCPB, блокируя все остальные».

«Следуйте рекомендациям по сегментации сети, сканированию уязвимостей и обнаружению вторжений, подходящим для использования продукта QNX в вашей среде кибербезопасности, чтобы предотвратить злонамеренный или несанкционированный доступ к уязвимым устройствам», - говорится в уведомлении BlackBerry.

По словам BlackBerry, обходных путей для устранения этой уязвимости не существует, но они отметили, что пользователи могут снизить вероятность атаки «путем включения возможности ASLR рандомизировать адреса сегментов процесса».

Уведомление включает ряд обновлений, выпущенных BlackBerry для устранения уязвимости. В апреле Microsoft заявила, что BadAlloc охватывает более 25 CVE и потенциально влияет на широкий спектр доменов, от потребительского и медицинского Интернета вещей до промышленного Интернета вещей.

Во вторник Politico сообщило о закулисном споре между BlackBerry и правительственными чиновниками США после того, как в апреле была обнаружена уязвимость BadAlloc.

BlackBerry якобы отрицала, что уязвимость затрагивает их продукты, и сопротивлялась попыткам правительства опубликовать публичные уведомления о проблеме. BlackBerry даже не знала, сколько организаций используют операционную систему QNX Real Time, когда их спросили правительственные чиновники, вынудив их согласиться с усилиями правительства по раскрытию уязвимости.

Официальные лица CISA координировали свои действия с затронутыми отраслями промышленности и даже Министерством обороны в отношении уведомления о безопасности системы QNX, согласно Politico, в котором

отмечалось, что CISA также проинформирует иностранных должностных лиц об уязвимости.

В июне BlackBerry заявила, что накопленный за QNX доход от лицензионных отчислений увеличился до 490 миллионов долларов в конце первого квартала 2022 финансового года. Компания хвасталась, что они используются в миллионах автомобилей, произведенных Aptiv, BMW, Bosch, Ford, GM, Хонда, Мерседес-Бенц, Тойота и Фольксваген». ***(Jonathan Greig. CISA releases alert on BadAlloc vulnerability in BlackBerry products // ZDNet (https://www.zdnet.com/article/cisa-releases-alert-on-badalloc-vulnerability-in-blackberry-products/). 17.08.2021).***

***

**«Спор разгорелся во вторник после того, как компания Rapid7, занимающаяся кибербезопасностью, опубликовала отчет об уязвимости в продукте Fortinet до того, как компания успела выпустить исправление, устраняющее проблему.**

Rapid7 сообщил, что один из его исследователей, Уильям Ву, обнаружил уязвимость внедрения команд в ОС в версии 6.3.11 и ранее в интерфейсе управления FortiWeb. Уязвимость позволяет удаленным злоумышленникам, прошедшим проверку подлинности, выполнять произвольные команды в системе через страницу конфигурации сервера SAML.

Rapid7 сообщил, что уязвимость связана с CVE-2021-22123, которая была устранена в FG-IR-20-120. Компания добавила, что в отсутствие патча пользователи должны «отключить интерфейс управления устройством FortiWeb от ненадежных сетей, в том числе из Интернета».

Отчет включал временную шкалу, в которой говорилось, что Rapid7 связался с Fortinet по поводу уязвимости в июне, и это было подтверждено Fortinet к 11 июня. Rapid7 утверждает, что они никогда больше не слышали от Fortinet, пока они не опубликовали отчет во вторник.

Представитель Fortinet связался с ZDNet после публикации статьи об этой уязвимости, чтобы раскритиковать Rapid7 за нарушение условий их соглашения о раскрытии информации. Fortinet заявила, что на странице политики PSIRT у нее есть четкая политика раскрытия информации, которая включает в себя «просьбу к отправителям инцидентов сохранять строгую конфиденциальность до тех пор, пока для клиентов не будут доступны полные решения».

«Мы ожидали, что Rapid7 сохранит какие-либо результаты до окончания 90-дневного периода ответственного раскрытия информации. Мы сожалеем, что в этом случае индивидуальные исследования были полностью раскрыты без надлежащего уведомления до 90-дневного окна», - сообщил представитель Fortinet. сказал, добавив, что они часто тесно сотрудничают с исследователями и поставщиками в области кибербезопасности.

«Мы работаем над тем, чтобы доставить клиентам немедленное уведомление об обходном пути и исправлении, выпущенном к концу недели».

Fortinet не ответила на последующие вопросы об исправлении уязвимости.

Rapid7 обновила свой отчет, сообщив, что Fortiweb 6.4.1 будет выпущен в конце августа и будет содержать исправление уязвимости.

Rapid7 оспаривает идею о том, что они нарушили какую-либо часть правил Fortinet, отметив, что 90-дневное окно, которое продолжает упоминать Fortinet, является лишь их собственным раскрытием как поставщика, выявляющего другие уязвимости. Согласно Rapid7, собственные политики Fortinet для организаций, которые могут подозревать уязвимости в сети Fortinet, не упоминают 90-дневное окно.

Rapid7 заявила, что они неоднократно обращались в Fortinet для работы над проблемой, но не получили ответа, поэтому при публикации отчета они следовали своей собственной политике раскрытия информации.

Тод Бердсли, директор по исследованиям Rapid7, сказал ZDNet, что их политика раскрытия уязвимостей предусматривает минимум 60 дней для раскрытия уязвимостей после первоначальных попыток контакта.

«В этом случае первоначальное раскрытие информации было представлено Fortinet 10 июня, а запрос поставщика был получен 11 июня в соответствии с нашим отчетом о раскрытии информации. Мы предприняли несколько последующих попыток с Fortinet после этого первоначального сообщения, и, к сожалению, мы не получили ответа. через 66 дней ", - пояснил Бердсли.

«Нарушений политик раскрытия информации не было. Вскоре после публикации раскрытия мы связались с Fortinet, и они сообщили, что будут выпускать исправление. Как только это исправление будет выпущено, мы обновим наше раскрытие, указав эту ссылку и идентификатор CVE.»

Бердсли добавил, что нет никаких указаний на использование уязвимости, поэтому раскрытие Rapid7 «следует рассматривать как предостережение для пользователей FortiWeb от Fortinet».

Он повторил, что пользователи FortiWeb не должны открывать свой интерфейс управления для Интернета в целом и должны убедиться, что люди с учетными данными для аутентификации выбирают надежные и надежные пароли». ***(Jonathan GreigFortinet slams Rapid7 for disclosing vulnerability before end of their 90-day window // ZDNet (https://www.zdnet.com/article/fortinet-slams-rapid7-for-disclosing-vulnerability-before-end-of-90-day-window/). 17.08.2021).***

***

**«Киберпреступники используют уязвимости Windows PrintNightmare в своих попытках заразить жертв программами-вымогателями, и число групп программ-вымогателей, пытающихся воспользоваться незащищенными сетями, вероятно, будет расти.**

Уязвимости удаленного выполнения кода (CVE-2021-34527 и CVE-2021-1675) в диспетчере очереди печати Windows - службе, включенной по умолчанию во всех клиентах Windows и используемой для копирования данных между устройствами для управления заданиями печати, - позволяют злоумышленникам запускать произвольный код., позволяя им устанавливать программы, изменять, изменять и удалять данные, создавать новые учетные записи с полными правами пользователя и перемещаться по сети.

Теперь банды программ-вымогателей используют PrintNightmare для взлома сетей, шифрования файлов и серверов и требования оплаты от жертв за ключ дешифрования.

Одним из них является Vice Society, относительно новый игрок в сфере программ-вымогателей, который впервые появился в июне и проводит практические кампании против целей, управляемые людьми. Известно, что Vice Society быстро использует новые уязвимости в системе безопасности, чтобы помочь в атаках программ-вымогателей, и, по мнению исследователей кибербезопасности из Cisco Talos, они добавили PrintNightmare в свой арсенал инструментов для компрометации сетей.

Как и многие киберпреступные группы программ-вымогателей, Vice Society использует атаки с двойным вымогательством, крадет данные у жертв и угрожает опубликовать их, если выкуп не будет уплачен. Согласно Cisco Talos, группа в основном сосредоточена на жертвах небольшого и среднего размера, особенно в школах и других образовательных учреждениях.

Повсеместное распространение систем Windows в этих средах означает, что Vice Society может использовать уязвимости PrintNightmare, если не были применены исправления, для выполнения кода, сохранения устойчивости в сетях и доставки программ-вымогателей.

«Использование уязвимости, известной как PrintNightmare, показывает, что злоумышленники уделяют пристальное внимание и будут быстро внедрять новые инструменты, которые они сочтут полезными для различных целей во время своих атак», - написали исследователи Cisco Talos в своем блоге.

«Множество различных злоумышленников сейчас используют преимущества PrintNightmare, и это внедрение, вероятно, будет продолжать расти, пока оно будет эффективным».

Еще одна группа программ-вымогателей, активно использующая уязвимости PrintNightmare, - Magniber. Эта операция с программами-вымогателями активна и вводит новые функции и методы атак с 2017 года. Сначала Magniber использовал вредоносную рекламу для распространения атак, а затем перешел к использованию незащищенных уязвимостей в программном обеспечении, включая Internet Explorer и Flash. Большинство кампаний Magniber нацелено на Южную Корею.

Теперь, по мнению исследователей кибербезопасности из Crowdstrike, программа-вымогатель Magniber использует PrintNightmare в своих кампаниях, снова демонстрируя, как банды вымогателей и другие киберпреступные группы пытаются воспользоваться недавно обнаруженными уязвимостями для помощи в атаках до того, как сетевые операторы применили исправление.

Вполне вероятно, что другие группы программ-вымогателей и злонамеренные хакерские кампании будут стремиться использовать PrintNightmare, поэтому лучшая форма защиты от уязвимости - обеспечить скорейшее исправление систем.

«По оценкам CrowdStrike, уязвимость PrintNightmare в сочетании с развертыванием программы-вымогателя, вероятно, будет и дальше использоваться другими участниками угроз», - сказала Ливиу Арсен, директор по исследованию угроз и отчетности Crowdstrike.

«Мы призываем организации всегда применять последние исправления и обновления безопасности для уменьшения известных уязвимостей и придерживаться передовых методов безопасности, чтобы укрепить свою безопасность против угроз и изощренных злоумышленников», - добавил он». ***(Danny Palmer. Ransomware: Now attackers are exploiting Windows PrintNightmare vulnerabilities // ZDNet (https://www.zdnet.com/article/ransomware-now-attackers-are-exploiting-windows-printnightmare-vulnerabilities/). 13.08.2021).***

***

**«Кибербезопасность исследователь обнаружил несколько новых уязвимостей в вебе - приложениях для управления тренажерного зала Wodify, что дает злоумышленнику возможность для извлечения данных тренировки, личной информации и даже финансовой информации.**

Веб-приложение Wodify для управления спортзалом широко используется боксерами CrossFit в США и других странах, чтобы помочь им расти. Программное обеспечение используется в более чем 5000 спортзалах для таких вещей, как планирование занятий и выставление счетов.

Но Дардан Пребреза, старший консультант по безопасности Bishop Fox, объяснил в отчете, что ряд уязвимостей «позволяет читать и изменять тренировки всех пользователей платформы Wodify».

Благодаря атаке доступ «не был ограничен одним тренажерным залом / боксом / арендатором, поэтому можно было перечислить все записи глобально и изменить их», - добавил Пребреза, отметив, что злоумышленник может захватить сеанс пользователя, украсть хешированный пароль, или JWT пользователя через уязвимость раскрытия конфиденциальной информации.

«Таким образом, комбинация этих трех уязвимостей может иметь серьезный бизнес и репутационный риск для Wodify, поскольку это позволит аутентифицированному пользователю изменять все свои производственные данные, а также извлекать конфиденциальную PII», - сказал Пребреза.

«Кроме того, компрометация административных учетных записей пользователей тренажерного зала может позволить злоумышленнику изменить настройки оплаты и, таким образом, иметь прямые финансовые последствия, поскольку злоумышленник в конечном итоге может получить оплату от членов тренажерного зала, а не от законных владельцев тренажерного зала. злоумышленник может считывать и изменять данные тренировок всех других пользователей, извлекать PII и в конечном итоге получать доступ к административным учетным записям с целью получения финансовой выгоды ».

Prebreza оценила уровень риска уязвимости как высокий, поскольку она может нанести серьезный репутационный ущерб и финансовые разветвления спортивным залам и боксам Wodify, в которых могут быть изменены настройки оплаты.

Wodify не ответила на запрос ZDNet о комментариях по поводу уязвимостей.

Отчет Prebreza включает временную шкалу, показывающую уязвимости, обнаруженные 7 января до того, как с Wodify связались 12 февраля. Wodify

признал уязвимости 23 февраля, но не ответил на дальнейшие запросы о предоставлении информации.

С генеральным директором Wodify Амитом Шахом связались, и он связал команду Bishop Fox с главой отдела технологий Wodify, который в течение апреля проводил встречи с компанией для решения проблем.

19 апреля Wodify подтвердил, что уязвимости будут устранены в течение 90 дней, но после этого неоднократно переносил дату исправления проблем. Во-первых, компания пообещала выпустить патч в мае, но они отложили его до 11 июня, прежде чем снова продлить до 26 июня.

Wodify не отвечал епископу Фоксу еще месяц, признав, что они переносят патч на 5 августа.

Епископ Фокс заявил, что с момента обнаружения уязвимостей прошло более полугода, они сообщили Wodify, что публично раскроют уязвимости 6 августа, а затем опубликовали отчет 13 августа.

Wodify не подтвердил, есть ли на самом деле патч, и епископ Фокс призвал клиентов связаться с компанией.

«На приложение Wodify повлиял недостаточный контроль авторизации, позволяющий аутентифицированному злоумышленнику раскрыть и изменить данные тренировок любого другого пользователя на платформе Wodify», - пояснил Пребреза.

«Пример изменения данных в отчете был выполнен с согласия в учетной записи соавтора, а полезная нагрузка для подтверждения концепции была удалена после снимка экрана. Однако возможность изменять данные означает, что злоумышленник может изменить все результаты тренировки и вставить вредоносные код для атаки на других пользователей Wodify, включая администраторов инстансов и тренажерных залов ".

Согласно исследованию, уязвимости варьировались от недостаточного контроля авторизации до раскрытия конфиденциальной информации и хранимых межсайтовых сценариев, которые могут быть использованы в других атаках.

В то время как злоумышленники смогут изменять все данные о тренировках, изображения и имена пользователей Wodify, атака также позволяет вставлять вредоносный код, который может атаковать других пользователей Wodify, включая администраторов спортзала.

Пребреза сказал, что приложение Wodify было уязвимо для четырех экземпляров хранимых межсайтовых сценариев, один из которых «позволял злоумышленнику вставлять вредоносные полезные данные JavaScript в результаты тренировки».

«Любой пользователь, просмотревший страницу с сохраненной полезной нагрузкой, выполнит JavaScript и выполнит действия от имени злоумышленника. Если злоумышленник таким образом получит административный доступ к определенному тренажерному залу, он сможет вносить изменения в настройки оплаты, как а также доступ и обновление личной информации других пользователей», - отметил Пребреза.

«В качестве альтернативы злоумышленник может создать полезную нагрузку для загрузки внешнего файла JavaScript для выполнения действий от имени

пользователя. Например, полезная нагрузка может изменить адрес электронной почты жертвы и захватить учетную запись, выполнив сброс пароля (примечание: изменение электронной почты адрес не требовал предоставления текущего пароля). Злоумышленник мог аналогичным образом использовать уязвимость раскрытия конфиденциальной информации для получения хешированного пароля жертвы или JWT (т. е. токена сеанса)».

Эрих Крон, защитник осведомленности о безопасности в KnowBe4, сказал, что это был неудачный случай, когда организация не восприняла всерьез раскрытие уязвимостей.

«Хотя первоначальная мысль о том, чтобы просто стереть чью-то историю тренировок, может показаться несущественной для многих, тот факт, что злоумышленник может получить доступ к учетной записи и связанной с ней информации, возможно, включая способы оплаты и личную информацию, является реальной проблемой», - сказал Крон.

«Даже просто информация о тренировке может быть конфиденциальной, если не тот человек использует ее для поиска закономерностей. Например, дни и время, когда генеральный директор организации обычно работает и использует ее в злонамеренных целях. Организации, которые создают программное обеспечение, всегда должны иметь процесс для работы с такими уязвимостями, о которых сообщают, и должен относиться к ним серьезно». ***(Jonathan Greig. Researchers find vulnerabilities in Wodify gym management web application used with CrossFit // ZDNet (https://www.zdnet.com/article/researchers-find-vulnerabilities-in-wodify-gym-management-web-application/). 13.08.2021).***

***

**«Risk Based Security выпустила два новых отчета, охватывающих утечки данных и уязвимости в первой половине 2021 года, обнаружив, что общее количество заявленных нарушений снизилось, но увеличилось количество раскрытых уязвимостей.**

Другой отчет, полученный от команды Risk Based Security VulnDB (R), собрал 12723 уязвимости, которые были обнаружены в первой половине 2021 года.

Они обнаружили, что за первую половину 2021 года количество обнаруженных уязвимостей выросло на 2,8% по сравнению с 2020 годом.

«Из уязвимостей, раскрытых в течение первой половины 2021 года, 32,1% не имеют идентификатора CVE, а еще 7%, имея назначенный идентификатор CVE, находятся в состоянии ЗАБРОНИРОВАНО, что означает, что информация об уязвимости, которую можно предпринять, еще не доступна. в CVE / NVD», - говорится в сообщении.

«В первой половине 2021 года группа VulnDB по Risk Based Security собирала в среднем 80 новых уязвимостей в день. Risk Based Security также обновляла в среднем 200 существующих записей об уязвимостях в день по мере появления информации о новых решениях, справочных материалов и дополнительных метаданных.»

Из уязвимостей, обнаруженных на данный момент в 2021 году, 1425 уязвимостей могут использоваться удаленно и имеют общедоступный эксплойт, а

также решение для смягчения последствий. Почти 900 уязвимостей, которые можно использовать удаленно, вообще не имеют решения по их устранению.

Одна из проблем, затронутых в отчете, - это тенденция организаций не сообщать о нарушениях.

Пандемия COVID-19 сместила акцент с кибербезопасности, и теперь количество публично раскрытых нарушений снизилось на 24% при сравнении данных за первую половину 2020 года и первую половину 2021 года.

Несмотря на сокращение раскрываемых нарушений, количество раскрытых конфиденциальных файлов продолжает расти. В период с января 2021 года по июнь 2021 года было раскрыто более 18 миллиардов конфиденциальных или конфиденциальных записей, что является вторым по величине показателем за всю историю безопасности на основе рисков.

Из данных, потерянных в результате взломов, 61% связан с раскрытием имен, 38% раскрывают номера социального страхования, 25% содержат адреса и 22% содержат финансовую информацию.

В отчетах также была указана первая десятка продуктов по раскрытию уязвимостей во втором квартале 2021 года. Debian Linux лидировал с 628, за ним следует Fedora с 584, openSuSE Leap с 526 и 443 для Ubuntu.

В первую десятку поставщиков по раскрытию уязвимостей во втором квартале 2021 года вошли Microsoft (627), SUSE (590), Fedora (584), IBM (547), а также Oracle и Google (более 500). Cisco, Canonical и Red Hat завершили список более чем 400 раскрытиями уязвимостей. во втором квартале 2021 года». ***(Jonathan Greig. More than 12,500 vulnerabilities disclosed in first half of 2021: Risk Based Security // ZDNet (https://www.zdnet.com/article/more-than-12500-vulnerabilities-disclosed-in-first-half-of-2021-risk-based-security/). 05.08.2021).***

***

**«Microsoft обнаружила, что тысячам пользователей баз данных Azure Cosmos DB может потребоваться обновить свои средства защиты после обнаружения серьезной ошибки.**

Cosmos DB - это служба баз данных Microsoft, которая работает на платформе облачных вычислений Azure и используется различными компаниями из списка Fortune 500 по всему миру.

Исследователи кибербезопасности из компании Wiz, занимающейся безопасностью облачной инфраструктуры, обнаружили ряд недостатков в одной из функций службы базы данных, которые могут быть использованы злоумышленниками для получения полного контроля над базой данных, что означает, что они могут читать или даже удалять данные.

«Кошмар каждого директора по информационной безопасности - это когда кто-то получает ключи доступа и убирает гигабайты данных одним махом. Так что вы можете себе представить наше удивление, когда мы смогли получить полный неограниченный доступ к учетным записям и базам данных нескольких тысяч клиентов Microsoft Azure, включая многие компании из списка Fortune 500», - пишут Нир Офельд и Саги Цадик из Wiz в совместном блоге.

*Бесключевой доступ*

Исследователи безопасности отмечают, что использование уязвимости, которую они назвали ChaosDB, было «тривиальным».

Уязвимость существует в функции Jupyter Notebook, которая помогает пользователям визуализировать свои данные. Он был представлен в 2019 году и был автоматически включен для всех баз данных Cosmos DB в феврале 2021 года.

Не вдаваясь в подробности, исследователи отмечают, что реализация Jupyter предоставила злоумышленникам доступ к первичным ключам базы данных и другим высокочувствительным секретам, таким как токен доступа к хранилищу BLOB-объектов.

Используя эти подробные ключи, исследователи смогли получить доступ и осуществлять полный контроль чтения / записи / удаления базы данных через Интернет.

Получив уведомление от исследователей, Microsoft быстро отключила уязвимую функцию записной книжки, чтобы предотвратить утечку секретов. Компания также просит часть своих пользователей поменять свои ключи, чтобы гарантировать, что любые ключи, которые уже были украдены неавторизованными пользователями, стали бесполезными.

Согласно Reuters, в электронном письме Microsoft подчеркивается тот факт, что компания не нашла доказательств того, что уязвимость была использована». ***(Mayank Sharma. Microsoft Azure security flaw left thousands of cloud databases vulnerable to hackers // Future Publishing Limited Quay House, The Ambury, Bath BA1 1UA (https://www.techradar.com/in/news/microsoft-warns-thousands-of-azure-cloud-databases-may-have-been-exposed). 27.08.2021).***

***

**«Исследователи безопасности обнаружили еще одну критическую ошибку в системах камер безопасности IoT, которая может позволить злоумышленникам захватить устройства.**

Nozomi Networks обнаружила уязвимость удаленного выполнения кода CVE-2021-32941 в веб-службе сетевого видеорегистратора (NVR) Annke N48PBB, используемого потребителями и предприятиями.

Сетевые видеорегистраторы являются важной частью любой подключенной системы камер видеонаблюдения, поскольку они предназначены для захвата, хранения и управления входящими видеопотоками с IP-камер.

В случае эксплуатации уязвимость может вызвать переполнение буфера на основе стека, что позволит удаленному злоумышленнику, не прошедшему проверку подлинности, получить доступ к конфиденциальной информации и выполнить код, согласно рекомендациям ICS от Агентства по кибербезопасности и безопасности инфраструктуры (CISA).

Nozomi Networks заявила, что это может привести к потере конфиденциальности, целостности и доступности устройства. На практике это означает, что злоумышленники могут отслеживать или удалять отснятый материал, изменять конфигурацию сигналов тревоги детектора движения или вообще останавливать запись.

Таким образом, кибератака с использованием CVE-2021-32941 может быть использована для поддержки физического ограбления помещений, защищенных устройствами Annke.

Сама ошибка может быть использована злоумышленниками напрямую для повышения привилегий в системе и косвенно в атаках с загрузкой диска.

«Администратору, оператору или пользователю достаточно просмотреть специально созданную веб-страницу при одновременном входе в веб-интерфейс устройства, чтобы потенциально вызвать выполнение внешнего вредоносного кода на самом устройстве», - предупредил Nozomi.

К счастью, Аннке быстро решила проблему, выпустив новую прошивку для исправления проблемы всего через 11 дней после ответственного раскрытия Нозоми.

Это второй критический недостаток камер Интернета вещей, обнаруженный Nozomi Networks этим летом. Еще в июне он предупредил об ошибке в популярном программном компоненте от ThroughTek, который OEM-производители используют для производства IP-камер, а также камер для наблюдения за детьми и домашними животными.

Это также могло позволить злоумышленникам подслушивать пользователей.

Еще одна уязвимость была обнаружена в платформе Kalay от ThroughTek только на прошлой неделе, потенциально затрагивая миллионы устройств». ***(Phil Muncaster. Critical IoT Camera Flaw Allows for Device Hijacking // Reed Exhibitions Ltd. (https://www.infosecurity-magazine.com/news/critical-iot-camera-flaw-allows/). 27.08.2021).***

***

**Наиболее серьезная из ошибок, исправленных Cisco (рейтинг 9,1 из 10), может позволить удаленному злоумышленнику, не прошедшему проверку подлинности, читать или записывать произвольные файлы в интерфейс протокола приложения, используемый в коммутаторах серии Cisco 9000, предназначенных для управления его программно-определяемыми сетевыми данными. центральное решение.**

Эта критическая уязвимость, отслеживаемая как CVE-2021-1577, влияет на контроллер инфраструктуры политики приложений Cisco (APIC) и контроллер инфраструктуры политики облачных приложений Cisco (Cloud APIC). APIC - это основной архитектурный компонент инфраструктуры Cisco, ориентированной на приложения, которая работает на узле Cisco Nexus серии 9000.

«Эта уязвимость связана с неправильным контролем доступа. Злоумышленник может воспользоваться этой уязвимостью, используя определенную конечную точку API для загрузки файла на уязвимое устройство», - пишет Cisco в своем бюллетене по безопасности в среду. Затронутые продукты: Cisco APIC и Cisco Cloud APIC.

Как и в случае с каждой из ошибок и исправлений, объявленных в среду, Cisco заявила, что для каждой из уязвимостей доступны меры по их устранению, и ей не известно о каких-либо публично известных эксплойтах для этих исправленных ошибок. Выпуск в среду, который включал в себя всего 15

исправлений, был частью «объединенной публикации» Cisco исправлений безопасности для ее расширяемой операционной системы Firepower и является совместимым с ядром Linux программным обеспечением NX-OS.

*Связка исправлений ошибок*

Cisco также исправила две ошибки Nexus 9000 высокой степени серьезности (CVE-2021-1586, CVE-2021-1523) и три ошибки средней степени серьезности (CVE-2021-1583, CVE-2021-1584, CVE-2021-1591). Две ошибки с высокой степенью серьезности (обе с базовым баллом CVSS 8,6) - это ошибки отказа в обслуживании.

«Уязвимость в конфигурациях сети Multi-Pod или Multi-Site для коммутаторов Cisco Nexus серии 9000 в режиме инфраструктуры, ориентированной на приложения (ACI), может позволить неаутентифицированному удаленному злоумышленнику неожиданно перезапустить устройство, что приведет к отказу в обслуживании (DoS) условие», - написала Cisco.

Вторая уязвимость серии Nexus 9000 высокой степени серьезности описана Cisco как недостаток в ее Fabric Switches ACI Mode Queue Wedge.

«[Недостаток] может позволить неаутентифицированному удаленному злоумышленнику вызвать клин очереди на листовом коммутаторе, что может привести к отбрасыванию критически важного трафика уровня управления к устройству. Это может привести к удалению одного или нескольких оконечных коммутаторов из фабрики», - отметила Cisco.

Cisco отмечает, что устранение этой ошибки требует «ручного вмешательства для включения и выключения устройства для восстановления» после применения исправлений. Это затронуло фабричные коммутаторы серии N9K (Nexus 9000) поколения 1.

*Критические ошибки QNX 'BadAlloc' - здесь нечего смотреть*

В среду Cisco выпустила второй важный совет по своему оборудованию, связанный с ошибкой операционной системы QNX, о которой 17 августа сообщила BlackBerry. Эта ошибка, согласно BlackBerry, может позволить злоумышленникам захватить или запустить атаки типа «отказ в обслуживании» на устройства и критически важную инфраструктуру, используя так называемые ошибки BadAlloc. QNX - это ОС реального времени BlackBerry, используемая во встроенных системах, таких как автомобили, медицинские устройства и телефоны.

Хотя Cisco заявляет, что ни один из ее продуктов не подвержен ошибке QNX, она оценила эту рекомендацию как критическую. «Cisco завершила расследование своей линейки продуктов, чтобы определить, какие продукты могут быть подвержены этой уязвимости. Нет данных о каких-либо продуктах, которые могут быть затронуты», - говорится в сообщении.

В рекомендациях Cisco описаны коммутаторы и маршрутизаторы, которые «используют уязвимое программное обеспечение QNX», однако «Cisco подтвердила, что уязвимость не может быть использована на этих платформах».

Продукты Cisco, работающие под управлением QNX, включают:

Адаптеры общего порта с распределенными каналами (SPA) (CSCvz34866)

Эмуляция каналов через пакет (CEoP) SPA (CSCvz34865)

32-разрядное программное обеспечение IOS XR (CSCvz34871) Примечание. 64-разрядное программное обеспечение IOS XR не использует программное обеспечение QNX.

РЧ шлюз 10 (CSCvz34869)». ***(Tom Spring. Cisco Issues Critical Fixes for High-End Nexus Gear // Threatpost (https://threatpost.com/cisco-issues-critical-fixes-for-high-end-nexus-gear/168939/). 25.08.2021).***

***

**«Проект Ethreum призывает разработчиков применить исправление, чтобы устранить серьезную уязвимость.**

Уязвимость с разделением цепочки, отслеживаемая как CVE-2021-39137, затрагивает Geth, официальную реализацию протокола Ethereum на Golang.

Такие недостатки могут вызвать коррупцию в сервисах блокчейна и привести к массовым сбоям, таким как отключение сети Ethereum в прошлом году.

*Детали вектора атаки пока не разглашаются*

На этой неделе специалисты по сопровождению проекта Ethereum призывают разработчиков Go, использующих go-ethereum или Geth, перейти на версию 1.10.8, в которой исправлена уязвимость высокой степени опасности.

Уязвимость в проекте с открытым исходным кодом Geth может вызвать «расщепление цепочки», то есть уязвимые экземпляры Geth откажутся принимать канонические цепочки.

Эксперт по программной безопасности и крипто-фаззингу Гвидо Вранкен из фирмы Sentnl, занимающейся безопасностью блокчейнов, обнаружил уязвимость во время работы по обеспечению безопасности.

Разработчики Ethereum заранее предупредили всех о предстоящей версии на прошлой неделе, не раскрывая слишком много…

Пока у большинства разработчиков не будет возможности перейти на исправленную версию, подробности о том, как можно использовать уязвимость, не раскрываются из соображений осторожности:

«Точный вектор атаки будет предоставлен позже, чтобы дать операторам узлов и зависимым нижестоящим проектам время обновить свои узлы и программное обеспечение», - сказал Петер Силаджи, руководитель группы Ethereum.

«Все версии Geth, поддерживающие хард-форк в Лондоне, уязвимы (ошибка старше, чем в Лондоне), поэтому все пользователи должны обновиться», - продолжил Силагьи.

Уязвимости блокчейна с «разделением цепочки» опасны, поскольку их использование может вызвать сбои, влияющие на вывод криптовалюты и общую целостность блокчейна.

Это произошло в прошлом году, когда сервисы, полагающиеся на сеть Ethereum, пострадали от сбоев и ошибок вывода, опять же из-за уязвимого клиента go-ethereum.

Разделение цепочки происходит, когда разные клиенты Ethereum не соглашаются с тем, что является действительной транзакцией, а что нет.

Это означает, что в зависимости от того, какой клиент использует ваша платформа, исходная (каноническая) цепочка блоков может оказаться «разветвленной».

В Ethereum один «канонический компьютер», также называемый виртуальной машиной Ethereum (EVM), поддерживает общее состояние или набор записей, с которыми согласен каждый узел, присутствующий в сети Ethereum.

Каждый сервис Ethereum хранит копию того, что находится в EVM.

Но если происходит разделение цепочки, разные службы блокчейна теперь будут показывать несовпадающие записи, тем самым влияя на целостность и надежность сети криптовалюты…

«Вероятность того, что кто-то случайно сработает за это время, мала, - объясняет инженер-программист R3 Димос Раптис, который участвует в разработке блокчейна Corda и проанализировал сбой Ethereum в прошлом году.

Инженер, однако, не недооценивает возможность использования злоумышленниками уязвимостей, связанных с разделением цепочки.

«В отличие от этого, вероятность того, что кто-то злонамеренно запустит его, если он будет отмечен как проблема безопасности, не является незначительной», - предупреждает эксперт в своем отчете.

В ходе аудита блокчейн-платформы Telos обнаружен недостаток

Интересно, что недостаток был обнаружен во время аудита платформы Telos EVM после того, как Telos привлек Sentnl в качестве своего аудитора.

Telos - это блокчейн-платформа нового поколения, которая помогает «создавать быстрые масштабируемые распределенные приложения с бесплатными транзакциями».

«Чтобы найти уязвимости в Telos EVM, я провел глубокий и тщательный фаззинг и убедился, что его поведение в точности соответствует поведению go-ethereum», - сказал Вранкен.

«Несмотря на то, что go-ethereum имел выдающуюся репутацию, когда дело доходит до безопасности, процедура была настолько эффективной, что не только способствовала утверждению правильности EVM Telos, но и обнаружила серьезную проблему в go-ethereum», - заявил эксперт по крипто-фаззингу в пресс-релизе.

Блокчейн-сервисы и разработчики, использующие go-ethereum, должны перейти на версию 1.10.8 или выше. В настоящее время обходных путей нет». ***(Ax Sharma. Ethereum urges Go devs to fix severe chain-split vulnerability // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ethereum-urges-go-devs-to-fix-severe-chain-split-vulnerability/). 25.08.2021).***

***

**«Сегодня Microsoft наконец опубликовала руководство по активно эксплуатируемым уязвимостям ProxyShell, влияющим на несколько локальных версий Microsoft Exchange.**

ProxyShell - это набор из трех недостатков безопасности (исправленных в апреле и мае), обнаруженных исследователем безопасности Devcore Оранж Цай,

который использовал их для взлома сервера Microsoft Exchange во время хакерского конкурса Pwn2Own 2021:

CVE-2021-34473 - путаница в пути перед аутентификацией приводит к обходу ACL (исправлено в апреле KB5001779)

CVE-2021-34523 - Повышение привилегий в серверной части Exchange PowerShell (исправлено в апреле, KB5001779)

CVE-2021-31207 - запись произвольного файла после авторизации приводит к RCE (исправлено в мае KB5003435)

Хотя Microsoft полностью исправила ошибки ProxyShell к маю 2021 года, они не назначили идентификаторы CVE для уязвимостей до июля, не позволяя некоторым организациям с непропатченными серверами обнаружить, что в их сетях есть уязвимые системы.

*Microsoft умалчивает об активных атаках*

Исследователи безопасности и Агентство по кибербезопасности и безопасности инфраструктуры США (CISA) уже предупредили администраторов о необходимости исправления своих серверов Exchange для защиты от продолжающихся атак с использованием эксплойтов ProxyShell, которые начались в начале августа.

Однако, несмотря на все предыдущие предупреждения об активных атаках, до сегодняшнего дня Microsoft не сообщала клиентам, что их локальные серверы Exchange подвергаются атакам.

«На прошлой неделе исследователи безопасности обсудили несколько уязвимостей ProxyShell, в том числе те, которые могут быть использованы на незащищенных серверах Exchange для развертывания программ-вымогателей или выполнения других действий после эксплуатации», - заявили в команде Exchange. [курсив наш]

«Если вы установили обновления безопасности за май 2021 года или обновления безопасности за июль 2021 года на свои серверы Exchange, то вы защищены от этих уязвимостей. Клиенты Exchange Online также защищены (но должны убедиться, что все гибридные серверы Exchange обновлены)».

Microsoft говорит, что клиенты должны установить по крайней мере один из поддерживаемых последних накопительных обновлений и ВСЕХ соответствующих обновлений безопасности блокировать ProxyShell атаки.

Согласно Microsoft, серверы Exchange уязвимы, если выполняется одно из следующих условий:

На сервере работает более старый неподдерживаемый CU;

На сервере выполняются обновления безопасности для более старых неподдерживаемых версий Exchange, выпущенных в марте 2021 года; или

На сервере работает более старый, неподдерживаемый CU, к которому применены меры по снижению рисков EOMT от марта 2021 года.

*Активная эксплуатация несколькими злоумышленниками*

Предупреждение CISA в понедельник о том, что несколько злоумышленников активно используют уязвимости ProxyShell, появилось после того, как в марте аналогичные организации предупредили организации о защите своих сетей от волны атак.

Атаки March Exchange были организованы поддерживаемыми китайским государством хакерами, которые поразили десятки тысяч организаций по всему миру, используя эксплойты, нацеленные на четыре ошибки Exchange нулевого дня, известные под общим названием ProxyLogon.

Как и в марте, злоумышленники сканируют и взламывают серверы Microsoft Exchange с помощью уязвимостей ProxyShell после того, как исследователи безопасности и злоумышленники воспроизвели работающий эксплойт.

Если вначале полезные нагрузки ProxyShell, сбрасываемые на серверы Exchange, были безвредными, теперь злоумышленники развертывают полезные нагрузки вымогателя LockFile, доставляемые через домены Windows, скомпрометированные с помощью эксплойтов Windows PetitPotam.

Чтобы иметь представление о масштабах проблемы, компания по безопасности Huntress Labs недавно сообщила, что к пятнице на прошлой неделе она обнаружила более 140 веб-оболочек, развернутых злоумышленниками на более чем 1900 скомпрометированных серверах Microsoft Exchange.

Shodan также отслеживает десятки тысяч серверов Exchange, уязвимых для атак ProxyShell, большинство из которых расположены в США и Германии.

«Наблюдается новый всплеск эксплуатации серверов Microsoft Exchange», - предупредил на выходных директор по кибербезопасности АНБ Роб Джойс. «Вы должны убедиться, что вы исправлены и отслеживаете, если вы размещаете экземпляр».

АНБ также напомнило защитникам, что опубликованное в марте руководство по поиску веб-оболочек все еще может использоваться для защиты от продолжающихся атак ProxyShell.

До тех пор, пока Microsoft не выпустит дальнейшее руководство по защите и обнаружению уязвимых серверов от эксплуатации, вы можете найти подробную информацию о том, как идентифицировать непропатченные серверы Exchange и как обнаруживать попытки эксплуатации, в сообщении блога, опубликованном исследователем безопасности Кевином Бомонтом». ***(Sergiu Gatlan. Microsoft: ProxyShell bugs “might be exploited,” patch servers now! // Bleeping Computer® (https://www.bleepingcomputer.com/news/microsoft/microsoft-proxyshell-bugs-might-be-exploited-patch-servers-now/). 25.08.2021).***

***

**«Американская компания-производитель программного обеспечения Kaseya выпустила обновление безопасности для исправления серверных уязвимостей нулевого дня Kaseya Unitrends, обнаруженных исследователями безопасности из Голландского института раскрытия уязвимостей (DIVD).**

Kaseya Unitrends - это облачное корпоративное решение для резервного копирования и восстановления, предоставляемое как автономное решение или надстройка для платформы удаленного управления Kaseya VSA.

Уязвимости (ошибка аутентифицированного удаленного выполнения кода и повышение привилегий от пользователя только для чтения до администратора) были обнаружены 2 июля и конфиденциально раскрыты Касее на следующий день.

Примерно две недели спустя, 14 июля, DIVD начал сканирование Интернета на предмет открытых экземпляров Kaseya Unitrends, чтобы сообщить владельцам, чтобы они отключили уязвимые серверы до тех пор, пока не будет выпущен патч.

26 июля DIVD публично раскрыл уязвимости в сообщении TLP: AMBER после того, как информация об этом просочилась в сеть после скоординированного раскрытия информации с участием 68 государственных CERT.

*Клиент unauth RCE все еще ждет патча*

Kaseya выпустила версию 10.5.5-2 Unitrends 12 августа, чтобы исправить две уязвимости сервера, но все еще работает над исправлением третьей ошибки удаленного выполнения кода без аутентификации, влияющей на клиента.

«Уязвимость на стороне клиента в настоящее время не исправлена, но Касея призывает пользователей смягчить эти уязвимости с помощью правил межсетевого экрана в соответствии с их лучшими требованиями и требованиями к межсетевому экрану», - говорится в сообщении DIVD, опубликованном сегодня.

«В дополнение к этому они выпустили статью в базе знаний с инструкциями по устранению уязвимости».

После выпуска исправленной версии Unitrends Касея обратилась к клиентам, посоветовав им исправить уязвимые серверы и применить меры защиты клиентов.

К счастью, в отличие от Kaseya VSA-REvil нулевого дня, использованного в начале июля в атаке программы-вымогателя, поразившей сотни клиентов Kaseya, эти три уязвимости труднее использовать.

Это связано с тем, что злоумышленникам потребуются действительные учетные данные для запуска атаки с удаленным выполнением кода или повышения привилегий на доступных в Интернете и уязвимых серверах Unitrends.

Кроме того, от злоумышленников также требуется, чтобы они уже проникли в сети своих целей, чтобы успешно использовать уязвимость RCE неавторизованного клиента.

Кроме того, председатель DIVD Виктор Геверс сказал BleepingComputer, что, несмотря на обнаружение в сетях организаций из чувствительных отраслей, количество уязвимых экземпляров Unitrends невелико». ***(Sergiu Gatlan. Kaseya patches Unitrends server zero-days, issues client mitigations // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/kaseya-patches-unitrends-server-zero-days-issues-client-mitigations/). 26.08.2021).***

***

**«Тайваньский производитель NAS компания Synology сообщила, что недавно обнаруженные уязвимости OpenSSL, связанные с удаленным выполнением кода (RCE) и отказом в обслуживании (DoS), влияют на некоторые из его продуктов.**

«Множественные уязвимости позволяют удаленным злоумышленникам проводить атаку типа «отказ в обслуживании» или выполнять произвольный код через уязвимую версию Synology DiskStation Manager (DSM), Synology Router Manager (SRM), VPN Plus Server или VPN Server», - поясняет компания. рекомендация по безопасности, опубликованная сегодня ранее.

Полный список устройств, подверженных уязвимостям безопасности, отмеченным как CVE-2021-3711 и CVE-2021-3712, включает DSM 7.0, DSM 6.2, DSM UC, SkyNAS, VS960HD, SRM 1.2, VPN Plus Server и VPN Server.

*Патчи появятся в течение следующих 90 дней*

Первая ошибка вызвана переполнением буфера на основе кучи в криптографическом алгоритме SM2, что обычно приводит к сбоям, но также может использоваться злоумышленниками для выполнения произвольного кода.

Второй недостаток - это переполнение буфера чтения при обработке строк ASN.1, что может быть использовано для сбоя уязвимых приложений при DoS-атаках или для получения доступа к содержимому частной памяти, например закрытым ключам или другой конфиденциальной информации.

Хотя группа разработчиков OpenSSL опубликовала OpenSSL 1.1.1l для устранения двух недостатков 24 августа, Synology сообщает, что выпуски уязвимых продуктов либо «текущие», либо «ожидающие».

Хотя Synology не предоставляет примерные сроки для этих входящих обновлений, компания сообщила BleepingComputer ранее в этом месяце, что обычно исправляет уязвимое программное обеспечение в течение 90 дней после публикации рекомендаций…

*Уязвимости DiskStation Manager также исследуются*

Производитель NAS также работает над обновлениями безопасности для нескольких уязвимостей DiskStation Manager (DSM) без присвоенных идентификаторов CVE и затрагивающих DSM 7.0, DSM 6.2, DSM UC, SkyNAS и VS960HD.

«Множественные уязвимости позволяют удаленным аутентифицированным пользователям выполнять произвольные команды или удаленным злоумышленникам записывать произвольные файлы через уязвимую версию DiskStation Manager (DSM)», - заявила компания Synology, публично раскрывая эти недостатки безопасности 17 августа.

«Наши команды все еще активно исследуют эту потенциальную уязвимость, и CVE будут назначены, когда будет раскрыта дополнительная информация», - заявила компания BleepingComputer на прошлой неделе, когда ее попросили поделиться информацией об этих ошибках DSM с идентификатором CVE.

Synology также добавила, что злоумышленники еще не воспользовались уязвимостями, раскрытыми в сообщении, опубликованном на прошлой неделе.

Ранее в этом месяце компания предупредила клиентов, что ботнет StealthWorker нацелен на их сетевые устройства хранения данных (NAS) с помощью грубой силы, которая приводит к заражению программами-вымогателями». ***(Sergiu Gatlan. Synology: Multiple products impacted by OpenSSL RCE vulnerability // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/synology-multiple-products-impacted-by-openssl-rce-vulnerability/). 26.08.2021).***

***

**«Злоумышленники активно используют критическую уязвимость обхода аутентификации, влияющую на домашние маршрутизаторы с прошивкой**

**Arcadyan, чтобы перехватить их и развернуть вредоносные полезные нагрузки ботнета Mirai.**

Уязвимость, обозначаемая как CVE-2021-20090, представляет собой уязвимость обхода критического пути (рейтинг 9.9 / 10) в веб-интерфейсах маршрутизаторов с прошивкой Arcadyan, которая может позволить неаутентифицированным удаленным злоумышленникам обойти аутентификацию.

Продолжающиеся атаки были обнаружены исследователями Juniper Threat Labs при мониторинге активности злоумышленника, известного своей атакой на сети и устройства IoT с февраля.

*Миллионы маршрутизаторов, вероятно, подвержены атакам*

Уязвимые устройства включают десятки моделей маршрутизаторов от различных поставщиков и интернет-провайдеров, включая Asus, British Telecom, Deutsche Telekom, Orange, O2 (Telefonica), Verizon, Vodafone, Telstra и Telus.

Исходя из количества моделей маршрутизаторов и длинного списка поставщиков, затронутых этой ошибкой, общее количество устройств, подверженных атакам, вероятно, достигнет миллионов маршрутизаторов.

Брешь в безопасности была обнаружена компанией Tenable, которая 26 апреля опубликовала рекомендации по безопасности и добавила доказательство концептуального кода эксплойта во вторник, 3 августа.

«Эта уязвимость в прошивке Аркадьяна существует не менее 10 лет и поэтому через цепочку поставок проникла как минимум в 20 моделей от 17 различных поставщиков, и это затронуто в официальном документе, выпущенном Tenable», - пояснил Эван Грант. Штатный инженер-исследователь Tenable, во вторник…

*Атаки начинаются через два дня после выхода эксплойта PoC*

С четверга Juniper Threat Labs «выявила несколько схем атак, которые пытаются использовать эту уязвимость в дикой природе, исходящую с IP-адреса, расположенного в Ухане, провинция Хубэй, Китай».

Злоумышленники, стоящие за этой продолжающейся деятельностью по эксплуатации, используют вредоносные инструменты для развертывания варианта ботнета Mirai, аналогичного тем, которые использовались в кампании Mirai, нацеленной на устройства IoT и сетевой безопасности, обнаруженные исследователями Unit 42 в марте.

«Сходство может указывать на то, что за этой новой атакой стоит один и тот же злоумышленник, который пытается модернизировать свой арсенал проникновения с помощью еще одной недавно обнаруженной уязвимости», - сказали в Juniper Threat Labs.

Впервые исследователи заметили активность злоумышленников 18 февраля. С тех пор они постоянно добавляли новые эксплойты в свой арсенал, причем один, нацеленный на CVE-2021-20090, был последним, включенным ранее на этой неделе, с большей вероятностью.

«Учитывая, что большинство людей могут даже не осознавать угрозы безопасности и не будут обновлять свои устройства в ближайшее время, эта тактика атаки может быть очень успешной, дешевой и простой в исполнении».

Индикаторы компрометации (IOC), включая IP-адреса, используемые для запуска атак, и образцы хэшей доступны в конце отчета Juniper Threat Labs». ***(Sergiu Gatlan. Actively exploited bug bypasses authentication on millions of routers // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/actively-exploited-bug-bypasses-authentication-on-millions-of-routers/). 07.08.2021).***

***

**«Новое исследование, проведенное консалтинговой фирмой Pen Test Partners, выявило ряд серьезных уязвимостей в зарядных станциях для электромобилей и зарядных устройствах для умного дома.**

Исследователи протестировали шесть марок домашних зарядных устройств (Project EV, Wallbox, EVBox, EO Hub, EO mini pro 2 и Hypervolt), а также две общедоступных зарядных сети (Chargepoint и EV Rolec), и выявили в большинстве из них явные уязвимости для кибератак.

Домашние зарядные станции для электромобилей позволяют владельцу автомобиля удаленно контролировать и управлять состоянием заряда с помощью мобильного приложения. Все мобильные приложения взаимодействуют с зарядным устройством через API и облачную платформу. Зарядные устройства обычно подключаются к домашней сети Wi-Fi владельца.

Исследователи обнаружили ряд уязвимостей. Они могли взломать аккаунты миллионов зарядных устройств для электромобилей. В некоторых они могли перехватывать аккаунты и включать и выключать дистанционное управление зарядкой.

В другом случае им удалось использовать точку зарядки как удаленный «черный ход» в домашнюю сеть пользователя, откуда потенциально можно взломать другие устройства в доме пользователя.

Что касается общедоступных зарядных устройств, команда обнаружила, что благодаря их способности удаленно включать и выключать зарядные устройства, недостатки кибербезопасности сети могут быть превращены в «кибероружие, которое другие могут использовать для повсеместных отключений электроэнергии».

К счастью, уязвимость обнаружили этичные хакеры, которые сообщили о них производителям зарядных станций. Согласно исследованию, эти уязвимости уже исправлены. Однако эксперты предупреждают, что вскоре могут появиться новые». ***(Виталий Маршак. Обнаружены серьезные уязвимости в зарядных станциях для электромобилей // Популярная механика (https://www.popmech.ru/technologies/news-737973-obnaruzheny-sereznye-uyazvimosti-v-zaryadnyh-stanciyah-dlya-elektromobiley/). 24.08.2021).***

***

**«Согласно новому исследованию, опубликованному в среду, ряд популярных коммерческих приложений в различных категориях, от браузеров до приложений для обмена сообщениями и встреч, содержал компоненты с открытым исходным кодом с уязвимостями безопасности.**

Исследование, проведенное Osterman Research для GrammaTech, также показало, что из самых популярных коммерческих браузеров, продуктов для электронной почты, обмена файлами, онлайн-встреч и обмена сообщениями 85% содержали по крайней мере одну критическую уязвимость.

«Коммерческие программные приложения часто включают компоненты с открытым исходным кодом, многие из которых содержат ряд известных уязвимостей, которые могут быть использованы вредоносными программами, однако поставщики часто не раскрывают их присутствие», - отметил старший аналитик Остермана Майкл Сэмпсон в отчете.

«Отсутствие прозрачности развернутых и подлежащих развертыванию приложений - это, по сути, бомба замедленного действия, которая увеличивает риск безопасности предприятия, увеличивает площадь атаки и возможность взлома со стороны киберпреступников», - добавил он.

Онлайн-встречи и почтовые клиенты, которые содержат самый высокий процент уязвимостей, были наиболее уязвимыми категориями, изучаемыми исследователями.

«Многие из приложений для онлайн-встреч были быстро вытеснены из-за пандемии. Вот почему в таких приложениях больше компонентов с открытым исходным кодом и больше уязвимостей», - пояснил Кристиан Симко, директор по маркетингу продуктов GrammaTech, компании по тестированию безопасности приложений со штаб-квартирой в Бетесде, штат Мэриленд.

Он добавил, что приложения для электронной почты и мессенджеры могут содержать множество уязвимостей, так как они зависят от Open SSL, протокола связи с открытым исходным кодом.

«Открытый SSL очень распространен, и это чрезвычайно уязвимый компонент с открытым исходным кодом», - говорит эксперт.

По словам Остермана, на Open SSL приходится 9,6% уязвимостей с открытым исходным кодом, обнаруженных во всех приложениях.

*Необходим лучший мониторинг*

Сариу Найяр, генеральный директор Gurucul, компании по анализу угроз из Эль-Сегундо, Калифорния, утверждает, что программное обеспечение с открытым исходным кодом так же безопасно или даже более безопасно, чем большинство коммерческих программ.

«Краудсорсинговый подход к программному обеспечению обычно позволяет быстро выявлять и устранять уязвимости», - говорит эксперт.

«Однако организации, использующие библиотеки с открытым исходным кодом или другое программное обеспечение, обязаны отслеживать использование открытого исходного кода в своем ПО, а также исправлять или иным образом заменять программное обеспечение с открытым исходным кодом, которое имеет уязвимости», - продолжает эксперт.

«Организации будут тщательно проверять свой собственный код, но не так строго как с открытым исходным кодом или коммерческим кодом», - добавил директор по маркетингу GrammaTech Энди Мейер.

Он пояснил, что производители коммерческого программного обеспечения используют компоненты с открытым исходным кодом и сторонние компоненты,

чтобы уложиться в ограничения по времени и стоимости, в которых они могут находиться.

«Тот факт, что они используют эти компоненты без их тестирования, говорит о проблеме скорости и необходимости ускорения циклов выпуска», - сказал эксперт в интервью.

*Открытый исходный код не дает гарантии*

Риск, который компоненты с открытым исходным кодом представляют для приложений, связан не столько с самим компонентом, сколько с цепочкой поставок, которая его поддерживает, утверждает Цви Коррен, технический директор Aqua Security, компании по обеспечению безопасности контейнеров, базирующейся в Рамат-Гане, Израиль.

«Все сводится к степени управления и надзора, которых часто не хватает проектам с открытым исходным кодом», - говорит он.

«Нам нужно различать проекты, которые спонсируются и поддерживаются организациями - компаниями-разработчиками программного обеспечения или некоммерческими организациями - и проекты, которые были начаты и все еще поддерживаются отдельными лицами или неорганизованными группами», - продолжил он.

«Последняя категория представляет наибольший риск для приложений, потому что эти проекты не могут инвестировать в тестирование безопасности, не предоставляют соглашения об уровне обслуживания для исправлений и потенциально могут стать целью для злоумышленников, которые пытаются« внедрить свой вредоносный код и сделать его частью проекта», - сказал он.

Поскольку организации не могут проконтролировать изменения, вносимые в компоненты с открытым исходным кодом, им необходимо знать, когда в них вносятся изменения, - говорит Шон Смит, директор по инфраструктуре nVisium, поставщика безопасности приложений из Херндона, штат Вирджиния.

«Использование зависимостей с открытым исходным кодом совершенно нормально, если вы должным образом проверяете источник на наличие проблем, в дополнение к постоянному аудиту каждый раз, когда вы обновляете эту зависимость на своей платформе», - сказал он TechNewsWorld.

«Многие организации будут укомплектовывать свои собственные внутренние группы, чтобы сосредоточиться на устранении проблем безопасности, о которых сообщалось в их компонентах с открытым исходным кодом», - добавил Кевин Данн, президент Pathlock, поставщика унифицированного доступа во Флемингтоне, штат Нью-Джерси.

«Преимущество компонентов с открытым исходным кодом состоит в том, что команды могут создавать свои собственные патчи для исправления проблем, которые их беспокоят, но за это приходится платить», - говорит эксперт.

*Спецификация программного обеспечения*

Ключом к снижению риска использования компонентов с открытым исходным кодом в программном обеспечении является повышение прозрачности процесса проверки.

«Решение проблемы начинается с видимости», - заметил Дэн Нурми, технический директор Anchore, компании по обеспечению безопасности контейнеров в Санта-Барбаре, Калифорния.

Один из способов защиты - использовать ведомость материалов по программному обеспечению (SBOM), в которой перечислены все компоненты и зависимости в приложении.

«Спецификация программного обеспечения может помочь в обеспечении прозрачности и видимости всего ландшафта сторонних и четвертых сторон, а также может помочь лучше понять, что связано с использованием конкретного инструмента», - говорит Деми Бен-Ари, соучредитель и технический директор Panorays, Tel Авив, Израиль, который автоматизирует, ускоряет и масштабирует сторонние процессы безопасности.

«Иметь список компонентов всегда полезно для организаций и их команд для осуществления контроля за опубликованными и недавно обнаруженными уязвимостями» добавил Purandar Дас, генеральный директор и соучредитель Сотеро.

Нурми объяснил, что создание ведомостей материалов для программного обеспечения - обычная практика в отрасли, но она не получила официального оформления.

«Существует не так много указаний о том, какие виды информации имеют отношение к обмену информацией между организациями», - сказал он.

Коррен отметил, что в хорошей ведомости материалов по программному обеспечению должны быть точно указаны компоненты, используемые в программном обеспечении.

«Прозрачность лучше, чем сокрытие этих компонентов, но их раскрытие не снижает риска в программном обеспечении», - заметил он.

«Что может сделать BOM, так это оказать давление на поставщиков и пользователей, чтобы они обратили внимание на риски безопасности и управление в компонентах с открытым исходным кодом», - сказал он.

«Пользователям программного обеспечения будет легче найти уязвимости в этих компонентах и работать над их устранением», - пояснил он.

«Раскрытие также укажет, идет ли поставщик в ногу с выпусками компонентов с открытым исходным кодом», - продолжил он.

«Но все это требует работы, - добавил он, - и сейчас существует тенденция игнорировать проблему, чтобы программное обеспечение могло продолжать двигаться по конвейеру». ***(Романов Роман. Отчет: большинство коммерческих приложений содержат уязвимости безопасности в коде // Internetua (http://internetua.com/otcset-bolshinstvo-kommercseskih-prilojenii-soderjat-uyazvimosti-bezopasnosti-v-kode). 06.08.2021).***

***

**«Утром в четверг, 19 августа, некоторые владельцы 3D-принтеров пришли в ужас – проснувшись, они обнаружили, что их устройства напечатали табличку с надписью «TSD небезопасен. Я подключился к вам наугад. Извините, но я должен был вас предупредить».**

Как оказалось, причиной несанкционированной печати послужила уязвимость в плагине The Spaghetti Detective (TSD) для web-интерфейса OctoPrint 3D-принтеров. По словам разработчика TSD Кеннета Цзяна (Kenneth Jiang), в ночь перед печатью загадочных табличек он внес изменения в конфигурацию облака TSD с целью повышения скорости и производительности. Однако в процессе Цзян допустил ошибку, в результате которой в течение восьми часов пользователи, подключившие свои 3D-принтеры к учетной записи TSD, могли видеть принтеры друг друга через функцию автообнаружения и даже подключаться к ним. Проблема затронула 73 пользователя, на момент сбоя подключившихся к учетным записям TSD.

Один из способов подключения 3D-принтеров к учетной записи – воспользоваться функцией автообнаружения TSD. Работа данной функции основывается на факте, что у устройств в одной локальной сети общий IP-адрес. Поэтому сервер TSD может сопоставить Raspberry Pi с компьютером/смартфоном, находящимся в той же локальной сети, тем самым позволяя им обнаруживать друг друга.

Когда разработчик попытался изменить настройки балансировщика нагрузки, он по ошибке пропустил настройку, позволяющую балансировщику передавать IP-адрес подключающегося клиента к конечному серверу TSD. Вместо этого балансировщик передавал на сервер только собственный IP-адрес. В итоге сервер получал IP-адреса пользователей, подключивших свои 3D-принтеры к TSD в одно и то же время. Сервер решил, что все они находятся в одной локальной сети и поэтому позволял им подключаться друг к другу.

По словам Цзяна, инцидент не затронул никакой личной информации, и учетные данные не пострадали.

TSD – выпущенный в 2019 году плагин для web-интерфейса OctoPrint, предназначенный для выявления сбоев в работе принтеров с помощью камеры». ***(Сбой в работе плагина привел к несанкционированной печати 3D-принтеров // SecurityLab.ru (https://www.securitylab.ru/news/523587.php). 20.08.2021).***

***

**«Специалисты Mandiant обнаружили опасную уязвимость, затрагивающую десятки миллионов видеорегистраторов в видеонянях и камерах видеонаблюдения по всему миру.** Уязвимость существует в протоколе связи Kalay от китайского поставщика IoT-устройств ThroughTek. С ее помощью злоумышленники могут перехватывать видеопоток в режиме реального времени.

Эксплуатация уязвимости предполагает осуществление атаки «человек посередине», другими словами, злоумышленник сначала должен получить доступ к сети Wi-Fi, к которой подключено атакуемое устройство.

Хотя уязвимость является очень опасной и потенциально затрагивает 83 млн видеорегистраторов по всему миру, использующих протокол Kalay, пользователи могут избежать ее эксплуатации, установив надежный пароль для домашней/офисной сети Wi-Fi. Производителю известно о проблеме, и он призывает пользователей установить обновление еще с 2018 года.

Проблема получила идентификатор CVE-2021-28372 и оценку 9,6 балла из максимальных 10 по шкале оценивания опасности CVSSv3.1.

Протокол Kalay реализован в качестве Software Development Kit (SDK), встроенного в программный клиент (то есть, мобильное или десктопное приложение) и IoT-устройства наподобие смарт-камер.

Для подключения нового видеорегистратора к сети Kalay запрашивает только уникальный идентификатор устройства (UID). Злоумышленник, который знает этот идентификатор, может зарегистрировать собственное устройство вместо настоящего, и соединение будет осуществляться с этим устройством, а не с настоящим.

Когда пользователь попытается получить доступ к видеорегистратору через протокол Kalay (например, через мобильное приложение), имя пользователя и пароль передадутся зарегистрированному UID. Перехватив их с помощью атаки «человек посередине», злоумышленник может переадресовать запрос на соединение и преспокойно просматривать видео и прослушивать аудио с атакуемого устройства.

Пользователям настоятельно рекомендуется обновить Kalay SDK до версии 3.3.1.0 или более поздней, а также включить DTLS». ***(datagram transport layer security – по сути, TLS для потокового видео) и технологию Kalay Authkey. (Опасная уязвимость затрагивает 83 млн видеорегистраторов по всему миру // SecurityLab.ru (https://www.securitylab.ru/news/523509.php). 18.08.2021).***

***

## *Технічні та програмні рішення для протидії кібернетичним загрозам*

---

**«Вместе с международной командой экспертов из Технологического института Вирджинии (Virginia Tech), Университета Квинсленда (Австралия) и Института науки и технологий Кванджу (Корея), исследователи из Лаборатории армейских исследований (ARL) Команды развития боевых возможностей армии США (DEVCOM) разработали метод под названием DESOLATER, который оптимизирует хорошо известную стратегия кибербезопасности, так называемую защиту движущейся цели.**

«Идея состоит в том, что движущуюся цель поразить труднее, — пояснил доктор Терренс Мур (Terrence Moore), математик ARL. — Если перетасовывать IP-адреса достаточно быстро, то информация, присвоенная IP-адресу, быстро теряется, и злоумышленнику приходится искать её снова».

DESOLATER (Deep reinforced learning based rESOurce aLlocation And moving Target defense dEployment fRamework) помогает бортовой сети боевого транспортного средства определить оптимальную частоту переключения IP-адресов и распределение полосы пропускания для обеспечения эффективной и долгосрочной защиты методом движущихся целей.

Исследовательская группа использовала глубокое обучение с подкреплением, чтобы постепенно формировать поведение алгоритма на основе различных функций вознаграждения, таких как время воздействия и количество упущенных пакетов, чтобы DESOLATER в равной степени стремился обеспечить как безопасность, так и эффективность.

Кроме того, DESOLATER не ограничивается определением оптимальных частоты перетасовки IP и распределения полосы пропускания. Поскольку этот подход реализован как фреймворк машинного обучения, прочие исследователи могут модифицировать его для достижения других целей в проблемном пространстве…». ***(Новый метод защиты заставляет хакеров «стрелять» по движущимся целям // Компьютерное Обозрение (https://ko.com.ua/novyj_metod_zashhity_zastavlyaet_hakerov_strelyat_po_dvizhushhimsya_celyam_138306). 09.08.2021).***

***

**«Разработчики Microsoft Edge, специализирующиеся на кибербезопасности, рассказали о новом, экспериментальном режиме под весьма необычным названием — «Super Duper Secure Mode».** Он усложняет злоумышленникам использование уязвимостей в браузере Microsoft путем отключения некоторых оптимизаций.

В «супер-пупер безопасном режиме» Microsoft Edge отключена функция движка JavaScript под названием Just-In-Time (JIT). Это технология увеличения производительности программных систем путем динамической компиляции байт-кода в машинный код или в другой формат. Она достаточно эффективна, но в то же время имеет чрезвычайно сложную техническую структуру — это чревато частыми ошибками и, следовательно, уязвимостями.

Microsoft ссылается на исследование Mozilla. Оно указывает, что с 2018 года более половины браузерных эксплойтов в той или иной степени были связаны с динамической компиляцией JIT…

Отказ от JIT позволил включить другие защитные механизмы — Controlflow-Enforcement Technology (CET) от Intel и Arbitrary Code Guard (ACG).

В официальном блоге говорится, что отключение JIT может привести к значительному снижению результатов тестов JavaScript. Но на практике пользователи едва ли заметят разницу, заверяют разработчики.

Обозреватель The Verge подтвердил, что не заметил существенного снижения быстродействия с режимом Super Duper Secure Mode. Но очевидно, что здесь все будет зависеть от сценариев использования и в более ресурсоемких веб-приложениях отключение JIT будет ощущаться сильнее. В будущем разработчики хотят сделать режим «умным» — система сможет самостоятельно оценивать риски и активировать режим только на подозрительных веб-сайтах.

Super Duper Secure Mode — экспериментальный режим, который все еще находится на очень ранней стадии. Желающие могут протестировать в версиях Canary, Dev и Beta — функция включается в служебном разделе настроек по адресу edge://flags. Когда планируется ее запуск, не уточняется. Разработчики предупредили, что на данный момент есть «довольно много технических

сложностей», которые предстоит решить для широкого запуска. Но поскольку актуальный Edge основан на Chromium и использует тот же движок, что и Chrome, в будущем (в случае успеха), «супер-пупер безопасный режим» может появиться и в других браузерах. Но от шуточного названия в стиле Tesla, вероятно, придется отказаться. Как объяснил руководитель команды Джонатан Норман, отчасти потому, что объяснить юристам, насколько безопасно то, что описывается как «супер-надежный», будет очень непросто». ***(Владимир Скрипин. Microsoft разработала для браузера Edge «супер-пупер безопасный режим» // ООО «ХОТЛАЙН» (https://itc.ua/news/microsoft-razrabotala-dlya-brauzera-edge-super-puper-bezopasnyj-rezhim/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+itc-ua+%28ITC.ua%29). 09.08.2021).***

***

**«IBM анонсировала новое решение Secure Access Service Edge (SASE), разработанное для поощрения подхода к безопасности с нулевым доверием на предприятии.**

В среду технический гигант заявил, что новая услуга IBM Security Services для SASE будет использовать технологию, предоставляемую в рамках партнерства с фирмой Zscaler, занимающейся кибербезопасностью, о которой было объявлено в мае.

Новое предложение было «разработано, чтобы помочь организациям ускорить внедрение облачной безопасности на периферии, ближе к пользователям и устройствам, имеющим доступ к корпоративным ресурсам», по словам IBM, а также для продвижения доступа к сети с нулевым доверием (ZTNA) на предприятии.

IBM Security Services для SASE включает в себя протоколы стратегии нулевого доверия, схемы SASE, современную сетевую архитектуру и возможности Zscaler, включая создание процессов и политик для управления SASE, а также поддержку IBM Managed Security Services.

По заявлению компании, IBM Security Services для SASE поможет поддерживать теперь уже гибридную рабочую силу, сторонние системы доступа, осуществление слияний и поглощений и обновления сети для упрощения использования облачных, 5G и устройств Интернета вещей (IoT).

«Традиционные подходы к сетевой безопасности больше не жизнеспособны в цифровом мире, где пользователи и приложения распределены», - прокомментировала Мэри О'Брайен, генеральный менеджер IBM Security. «Мы наблюдаем, как эта трансформация происходит прямо на наших глазах, поскольку многие организации планируют работать по гибридной модели в обозримом будущем. Этот новый подход требует сдвига в культуре, процессах и сотрудничестве между командами наряду с новой технологической архитектурой».

Новое решение теперь коммерчески доступно…». ***(Charlie Osborne. IBM launches new SASE service to bolster zero-trust enterprise security // ZDNet (https://www.zdnet.com/article/ibm-launches-new-sase-service-to-bolster-zero-trust-security/). 25.08.2021).***

***

**«Новая кнопка и надстройка для учетных записей Microsoft 365 / Office 365 и Outlook позволяет сотрудникам сообщать о мошеннических электронных письмах непосредственно в Национальный центр кибербезопасности Великобритании (NCSC).**

Эта кнопка является обновлением существующей службы отчетов о подозрительных электронных письмах (SERS) NCSC, которая с момента запуска в апреле 2020 года получила более 6,6 миллиона отчетов. По состоянию на 30 июня NCSC удалил более 50 500 мошеннических сообщений и 97 500 URL-адресов.

В то время как системы фильтрации электронной почты могут остановить некоторые фишинговые атаки, достигающие почтовых ящиков сотрудников, мошенники всегда ищут способы обойти фильтры - например, размещая мошенничество в облачных сервисах Google, создавая фишинговые страницы Office 365 или взламывая сайты SharePoint, чтобы обманом заставить жертв войти в систему. учетные данные своей рабочей учетной записи.

«Типичные» фишинговые URL-адреса, которые обрабатывает NCSC, включают в себя обман персонала, который щелкает ссылку, которая загружает вредоносное ПО на рабочий компьютер, создает клонированные страницы входа и электронную почту с поддельными предупреждениями о рабочем программном обеспечении, таком как Microsoft Teams.

«Оппортунистическое мошенничество во время пандемии продемонстрировало, как киберпреступники постоянно находят новые способы нацеливаться на нас», - сказал технический директор NCSC Ян Леви.

«Хорошая новость заключается в том, что вы можете помочь защитить свое рабочее место, пересылая электронные письма с подозрением на мошенничество в Службу сообщений о подозрительных сообщениях электронной почты (SERS) со своей рабочей учетной записи электронной почты одним нажатием кнопки».

NCSC предоставил администраторам руководство по включению надстройки Office 365 «Сообщить о фишинге» для Outlook.

Инструмент Report Phishing создан Microsoft и может быть установлен с сайта Microsoft AppSource. После установки надстройки администраторам необходимо создать правило потока обработки почты, чтобы сообщать о фишинговых случаях в SERS. После включения на главной панели инструментов Outlook появляется новая кнопка «Сообщить о фишинге». Для Outlook в Интернете кнопка Сообщить о фишинге отображается на боковой панели.

«Служба сообщений о подозрительных электронных письмах NCSC (SERS) позволяет общественности сообщать о подозрительных электронных письмах, отправляя их по адресу report@phishing.gov.uk. SERS анализирует электронные письма и, если обнаруживает, что они содержат ссылки на вредоносные сайты, пытается удалить эти сайты из Интернет, чтобы предотвратить распространение вреда », - отмечает NCSC.

Отчеты отправляются как в Microsoft, так и в NCSC.

Для организаций, которые не могут установить кнопку «Сообщить о фишинге» для Outlook, NCSC по-прежнему рекомендует предприятиям пересылать

или прикреплять мошеннические электронные письма на адрес report@phishing.gov.uk». ***(Liam Tung. Microsoft 365: This new one-click button lets businesses report scam emails // ZDNet (https://www.zdnet.com/article/microsoft-365-this-new-one-click-button-lets-businesses-report-scam-emails/). 16.08.2021).***

***

**«Стартап по облачной безопасности Monad, предлагающий платформу для извлечения и соединения данных из различных инструментов безопасности, запустился незаметно с финансированием серии А в размере 17 миллионов долларов, возглавляемым Index Ventures.**

Monad был основан на убеждении, что кибербезопасность предприятия является растущей проблемой управления данными, поскольку организации пытаются понять и интерпретировать массивы информации, хранящейся в отключенных журналах и базах данных. После того, как организация извлечет данные из своих инструментов безопасности, платформа данных безопасности Monad позволяет им централизовать эти данные в выбранном хранилище данных, а также нормализовать и обогащать данные, чтобы группы безопасности обладали знаниями, необходимыми для эффективной защиты своих систем и данных.

«Безопасность - это принципиально проблема больших данных, - сказал Кристиан Альменар, генеральный директор и соучредитель Monad. «Клиенты часто не могут получить доступ к своим данным безопасности в оптимизированной форме, которая необходима командам DevOps и облачных инженеров для быстрого создания своих приложений, а также для решения самых насущных проблем безопасности и соответствия нормативным требованиям. Мы основали Monad, чтобы решить эту проблему безопасности данных и освободить данные о безопасности клиентов из разрозненных инструментов, чтобы сделать их доступными через любое хранилище данных по выбору».

Раунд финансирования стартапа серии А, который также был поддержан Sequoia Capital, доводит его общую сумму инвестиций до 19 миллионов долларов и наступает через 12 месяцев после начального раунда, возглавляемого Sequoia. По словам стартапа, эти средства позволят Monad масштабировать свои усилия по разработке облачной платформы данных безопасности…». ***(Carly Page. Monad emerges from stealth with $17M to solve the cybersecurity big data problem // Verizon Media (https://techcrunch.com/2021/08/26/monad-emerges-from-stealth-with-17m-to-solve-the-cybersecurity-big-data-problem/). 26.08.2021).***

***

**«От сети и безопасности данных до управления идентификацией и унифицированного управления угрозами (UTM) стартапы предлагают решения по кибербезопасности для выявления уязвимостей, предотвращения атак и обеспечения безопасности сетей**. На этом фоне модель прогнозирования единорогов GlobalData, ведущей компании, занимающейся данными и аналитикой, опубликовала список из 50 стартапов в области кибербезопасности, которые могут стать единорогами (более 1 миллиарда долларов).

Апурва Баджадж, руководитель практики финансовых рынков в GlobalData, говорит: «Поскольку мы вступаем в эру кодовой войны, когда каждое цифровое устройство, независимо от его размера, может быть «вооружено», а кибератаки распространяются по всему миру, инвесторы вкладывают значительные средства в поддержку кибербезопасность стартапов. В то же время пандемия COVID-19 создала для отрасли попутный ветер, поскольку компании приняли парадигму удаленной работы с большим количеством приложений и данных, хранящихся в облаке, вероятно возникновение потока новых угроз, что сделает инвестиции в кибербезопасность необходимостью.»

Последний отчет GlobalData «Будущие единороги кибербезопасности - 18 августа 2021 года» показывает, что во втором квартале 2021 года отрасль сообщила об инвестициях в размере более 8,1 миллиарда долларов, охватывающих 209 сделок по всему миру. В отчете также отмечается всплеск венчурных инвестиций в стартапы в области кибербезопасности во втором квартале 2021 года, в основном за счет таких стартапов, как Transmit Security, Trulioo и Forter, которые привлекли финансирование в диапазоне от 300 до 550 миллионов долларов. Во втором квартале 2021 года на долю Северной Америки пришлось более 58% объема сделок, за ней следует Европа (17%).

Некоторые из стартапов в области кибербезопасности в списке потенциальных единорогов GlobalData включают BetterCloud, Guardicore, Deep Instinct и Swimlane.

BetterCloud, американская платформа управления «программное обеспечение как услуга» (SaaS), позволяет специалистам в области информационных технологий (ИТ) обнаруживать, управлять и защищать растущий стек приложений SaaS на цифровом рабочем месте. Недавно компания запустила BetterCloud Discover, новую централизованную платформу, которая дает предприятиям представление о внедрении SaaS и полную видимость санкционированных и несанкционированных приложений в среде с несколькими SaaS.

Guardicore, стартап, предлагающий решения для облачной безопасности, сосредоточен на предоставлении более эффективных способов защиты критически важных приложений от компрометации с помощью прозрачности, микросегментации, а также обнаружения угроз и реагирования в реальном времени.

Deep Instinct, американский поставщик решений для кибербезопасности, использует технологии глубокого обучения и кибербезопасности. Недавно компания добавила новые функции и возможности в свое решение, ориентированное на предотвращение, в том числе повышенную устойчивость к злонамеренным атакам машинного обучения, защиту от кражи учетных данных и отчеты о злонамеренном поведении.

Swimlane, поставщик решений для автоматизации кибербезопасности, помогает организациям выполнять все требования к операциям безопасности (SecOps), включая приоритезацию предупреждений, управление инструментами и автоматизацию устранения угроз. Недавно компания привлекла 40 миллионов долларов для ускорения партнерских отношений и альянсов, расширения исследований и разработок и обеспечения дальнейшего глобального расширения.

Баджадж заключает: «Увеличение числа сделок венчурного капитала вкупе со значительным увеличением числа выданных патентов, наряду с положительными новостями и растущим упоминанием кибербезопасности в документах публичных компаний, указывают на то, что эта технология представляет значительный интерес как для венчурных капиталистов, так и для корпораций. Пандемия COVID-19 создает для этой отрасли попутный ветер, поскольку компании переходят на модель удаленной работы. Поскольку облачное резервное копирование становится предпочтительным вариантом для сохранения приложений и данных, вероятно, возникнет ряд новых онлайн-угроз, которые сделают инвестиции в кибербезопасность необходимостью». ***(GlobalData predicts future cybersecurity unicorns // CFE Media and Technology (https://www.industrialcybersecuritypulse.com/globaldata-predicts-future-cybersecurity-unicorns/). 26.08.2021).***

***

**«Panda Security, при поддержке родительской компании WatchGuard, разработала и предлагает простое и бесплатное решение – сервис Dark Web Scanner, который сканирует «теневой» Интернет и проверяет, не была ли взломана или украдена информация, связанная с вашими аккаунтами.** Доступ к этому сервису можно получить через аккаунт My Panda. Для его использования не обязательно быть клиентом Panda Security.

Реальные кибер-атаки не похожи на кино, потому что обычно проводятся скрытно и остаются незаметными для жертвы. Во многом благодаря этому взломы остаются успешными. В ходе атаки на какой-нибудь онлайн-сервис хакеры могут похитить данные сотен тысяч пользователей. Причем большинство из них даже не заподозрят, что их цифровая личность уже продается в даркнете.

А ведь если преступники завладеют данными чьего-то аккаунта, то они смогут выдавать себя за этого человека, чтобы получить доступ к другим его персональным и конфиденциальным данным, аккаунтам на других веб-сервисах или попытаться украсть деньги с банковских счетов». ***(Dark Web Scanner – бесплатный сервис проверки защищенности учетных данных // Компьютерное Обозрение (https://ko.com.ua/dark_web_scanner_besplatnyj_servis_proverki_zashhishhennosti_uchetnyh_dannyh_138323). 10.08.2021).***

***

**«Сотрудники Санкт-Петербургского федерального исследовательского центра Российской академии наук (СПб ФИЦ РАН) обучили искусственный интеллект выявлять в социальных сетях группы вредоносных ботов через анализ публичных данных о них, независимо от того, на каком языке они пишут посты и комментарии.**

Данный подход может использоваться компаниями, которые используют соцсети в коммерческих целях, для выявления и противодействия информационным атакам. Результаты исследования опубликованы в международном журнале JoWUA.

Программа поможет выследить бота по неявным «социальным связям». При этом искусственному интеллекту будет абсолютно неважно, на каком языке и в какой социальной сети придется работать — от сможет легко подстроиться под любую из них.

Точность распознания варьируется от 60% до 90%, а на лживые срабатывания приходятся 5-10%. Зависеть это будет от заполненности социальной сети ботами. Что же касается сложных программ, которые интеллект не сможет распознать, то тут тоже все продумано — проверка всех аккаунтов проводится регулярно и в одну из них бот точно даст о себе знать.

Метод, созданный учеными СПб ФИЦ РАН, может не только определять ботов, но и оценивать их качество и примерно рассчитать стоимость атаки. Эти данные могут использоваться для расследования инцидентов безопасности.

Например, если в аккаунте соцсети какого-нибудь ресторана оставлена масса негативных комментариев. Новый метод поможем выявить, боты их оставили или реальные люди. В случае, если комментарии оставили боты, ресторан поймет, что на него осуществляется атака.

Кроме того, программа может определить качество и возможности ботов и понять, сколько денег было вложено в эту атаку. Исходя из этих данных, бизнесу будет проще принять меры чтобы эффективно отреагировать на инцидент». ***(Питерские ученые научили нейросеть выявлять вредоносные боты в соцсетях // SecurityLab.ru (https://www.securitylab.ru/news/523616.php). 22.08.2021).***

***

## Питання криптографії

**«Чтобы защитить наши личные коммуникации от будущих атак со стороны квантовых компьютеров, Verizon испытывает использование ключей шифрования нового поколения для защиты виртуальных частных сетей (VPN), которые ежедневно используются компаниями по всему миру для предотвращения взлома.**

Verizon реализовал то, что он описывает как «квантово-безопасный» VPN между одной из лабораторий компании в Лондоне, Великобритания, и центром в США в Эшберне, штат Вирджиния, используя ключи шифрования, которые были сгенерированы с помощью методов постквантовой криптографии что они достаточно надежны, чтобы противостоять атакам квантового компьютера.

Согласно Verizon, испытание успешно продемонстрировало возможность замены текущих процессов безопасности на квантово-защищенные протоколы.

VPN - это распространенный инструмент безопасности, используемый для защиты подключений через Интернет путем создания частной сети из общедоступного Интернет-соединения. Когда пользователь просматривает Интернет с помощью VPN, все его данные перенаправляются через специально настроенный удаленный сервер, запущенный хостом VPN, который действует как фильтр, шифрующий информацию.

Это означает, что IP-адрес пользователя и любые его действия в Интернете, от отправки электронных писем до оплаты счетов, кажутся потенциальным хакерам чушью - даже в незащищенных сетях, таких как общедоступный Wi-Fi, где подслушивание намного проще.

Особенно в последние несколько месяцев, когда многие сотрудники перешли на постоянную работу из дома, VPN стали все более популярным инструментом для обеспечения конфиденциальности и безопасности в Интернете.

Однако эта технология основана на протоколах криптографии, которые нельзя взломать. Для шифрования данных хосты VPN используют ключи шифрования, которые генерируются хорошо зарекомендовавшими себя алгоритмами, такими как RSA (Ривест – Шамир – Адлеман). Сложность взлома ключа и, следовательно, чтения данных напрямую связана со способностью алгоритма создать настолько сложный ключ, насколько это возможно.

Другими словами, известные нам протоколы шифрования по сути представляют собой огромную математическую задачу, которую нужно решить хакерам. С существующими компьютерами решить уравнение чрезвычайно сложно, поэтому на данный момент VPN по-прежнему являются безопасным решением. Но ожидается, что квантовые компьютеры принесут огромное количество дополнительных вычислительных мощностей, а вместе с тем и возможность взломать любой криптографический ключ за считанные минуты.

«Многие безопасные коммуникации полагаются на алгоритмы, которые десятилетиями успешно предлагали безопасные ключи шифрования», - сказал ZDNet Венката Джосюла, директор по технологиям Verizon. «Но существует достаточно исследований, говорящих о том, что их можно сломать, когда есть квантовый компьютер с определенной мощностью. Когда он доступен, вы хотите защитить всю свою инфраструктуру VPN».

Один из подходов, над которым работают исследователи, заключается в разработке алгоритмов, которые могут генерировать ключи, которые слишком сложно взломать даже с помощью квантового компьютера. Эта область исследований известна как постквантовая криптография и особенно востребована правительствами во всем мире.

В США, например, Национальный институт стандартов и технологий (NIST) в 2016 году начал глобальное исследование, призвав исследователей представить идеи для алгоритмов, которые были бы менее восприимчивы к квантовой атаке. Несколько месяцев назад организация выбрала группу из 15 алгоритмов, которые показали себя наиболее многообещающими.

«NIST возглавляет процесс стандартизации, но мы не хотели ждать его завершения, потому что заставить криптографию измениться по всему миру - довольно сложная задача», - говорит Джосюла. «Это может занять 10 или даже 20 лет, поэтому мы хотели заняться этим как можно раньше, чтобы выяснить последствия».

Джосюла добавляет, что Verizon обладает значительным объемом инфраструктуры VPN, и компания продает продукты VPN, поэтому команда начала изучать, как включить постквантовую криптографию прямо сейчас и в существующих сервисах.

Для тестирования был выбран один из 15 алгоритмов, определенных NIST, под названием Sabre. Sabre генерировал квантово-безопасные криптографические ключи, которые доставлялись на конечные точки - в Лондоне и Эшберне - типичного IPsec VPN через дополнительный уровень инфраструктуры, предоставленный сторонним поставщиком.

Достигнет ли Sabre финального этапа процесса стандартизации NIST, в данном случае не имеет значения, объясняет Джосюла. «Мы пробовали Sabre здесь, но мы будем пробовать другие. Мы можем переключаться с одного алгоритма на другой. Мы хотим иметь такую гибкость, чтобы иметь возможность адаптироваться в соответствии с процессом стандартизации».

Другими словами, тест Verizon показал, что сейчас возможно реализовать кандидатов постквантовой криптографии на каналах инфраструктуры с возможностью миграции по мере необходимости между разными кандидатами на квантово-защищенные алгоритмы.

Это важно, потому что, хотя крупномасштабный квантовый компьютер может появиться более чем через десять лет, все еще существует вероятность того, что данные, которые в настоящее время зашифрованы с помощью существующих протоколов криптографии, находятся под угрозой.

Угроза известна как «собрать сейчас, расшифровать позже» и относится к возможности того, что хакеры могут собрать огромные объемы зашифрованных данных и сидеть на них, ожидая появления квантового компьютера, который мог бы прочитать всю информацию.

«Если это ваша корзина для покупок на Amazon, вам может быть все равно, увидит ли ее кто-нибудь через десять лет», - говорит Джосюла. «Но вы можете распространить это на свой банковский счет, личный номер и вплоть до государственных секретов. Речь идет о том, насколько далеко в будущем вы видите ценность данных, которыми вы владеете, - а некоторые из них имеют очень долгий срок службы».

Для этого типа данных важно начать думать о долгосрочной безопасности прямо сейчас, что включает в себя риск, связанный с квантовыми компьютерами.

Квантово-безопасный VPN может стать хорошим началом - хотя, как объясняет Джосюла, многие элементы все еще необходимо сгладить. Например, Verizon по-прежнему полагался на стандартные механизмы в своих испытаниях для доставки квантово-защищенных ключей к конечным точкам VPN. Это может стать камнем преткновения, если окажется, что эта фаза процесса не неуязвима для квантовой атаки.

Однако идея состоит в том, чтобы предпринять активные шаги для подготовки, а не ждать худшего сценария. Подключение Лондона к Эшберну было первым шагом, и теперь Verizon рассматривает возможность распространения своей квантово-безопасной VPN на другие места». ***(Daphne Leprince-Ringuet. Quantum computers could read all your encrypted data. This 'quantum-safe' VPN aims to stop that // ZDNet (https://www.zdnet.com/article/quantum-computers-could-read-all-our-encrypted-data-this-quantum-safe-vpn-is-trying-to-prevent-that/). 26.08.2021).***

***

**«Команда из Технологического университета Мюнхена (TUM) разработала и ввела в эксплуатацию производство компьютерного чипа, который очень эффективно реализует постквантовую криптографию.** Такие чипы могут обеспечить защиту от будущих хакерских атак с использованием квантовых компьютеров. Исследователи также включили в чип аппаратных троянов, чтобы изучить методы обнаружения этого типа «вредоносного ПО с фабрики микросхем».

Хакерские атаки на промышленные предприятия больше не являются научной фантастикой. Злоумышленники могут украсть информацию о производственных процессах или отсановить деятельность целых предприятий. Чтобы предотвратить это, обмен данными между микросхемами в отдельных компонентах зашифрован. Однако вскоре многие алгоритмы шифрования станут неэффективными. Установленные процессы, которые могут отражать атаки, запущенные с помощью современных компьютерных технологий, будут беззащитны против квантовых компьютеров. Это особенно важно для оборудования с длительным сроком службы, такого как промышленные объекты.

По этой причине эксперты по безопасности во всем мире работают над разработкой технических стандартов для «постквантовой криптографии». Одна из проблем связана с огромной вычислительной мощностью, необходимой для этих методов шифрования. Команда, работающая с Георгом Зиглом, профессором безопасности информационных технологий в TUM разработала и ввела в эксплуатацию высокоэффективный чип для постквантовой криптографии.

*Скорость и гибкость за счет комбинации аппаратного и программного обеспечения*

Профессор Зигл и его команда использовали подход, основанный на совместном проектировании аппаратного и программного обеспечения, в котором специализированные компоненты и управляющее программное обеспечение дополняют друг друга. «Наш чип является первым чипом для постквантовой криптографии, который полностью основан на подходе совместного проектирования аппаратного и программного обеспечения», - говорит профессор Зигл.

«В результате он примерно в 10 раз быстрее при шифровании с помощью Kyber - одного из наиболее многообещающих кандидатов для постквантовой криптографии - по сравнению с чипами, полностью основанными на программных решениях. Он также потребляет примерно в восемь раз меньше энергии и почти такой же гибкий»

*На основе стандарта с открытым исходным кодом*

Чип представляет собой специализированную интегральную схему (ASIC). Такие специализированные микроконтроллеры часто производятся в больших количествах по спецификациям компаний. Команда TUM изменила дизайн микросхемы на основе стандарта RISC-V с открытым исходным кодом. Он используется все большим числом производителей микросхем и может заменить проприетарные подходы крупных компаний во многих областях. Возможности постквантовой криптографии микросхемы упрощаются за счет модификации ядра

процессора и специальных инструкций, которые ускоряют необходимые арифметические операции.

В конструкцию также входит специально разработанный аппаратный ускоритель. Он не только поддерживает алгоритмы постквантовой криптографии на основе решетки, такие как Kyber, но также может работать с алгоритмом SIKE, который требует гораздо большей вычислительной мощности. По словам команды, чип, разработанный в TUM, может реализовать SIKE в 21 раз быстрее, чем чипы, использующие только программное шифрование. SIKE рассматривается как наиболее многообещающая альтернатива, если придет время, когда подходы на основе решеток уже не бдут безопасными. Подобные меры предосторожности имеют смысл в приложениях, где чипы будут использоваться в течение длительного времени.

*Аппаратные трояны избегают постквантовой криптографии*

Еще одна потенциальная угроза, наряду с ростом числа обычных атак, связана с аппаратными троянами. Компьютерные чипы обычно производятся в соответствии со спецификациями компаний и производятся на специализированных заводах. Если злоумышленникам удастся внедрить троянскую схему в конструкцию микросхемы до или во время стадии производства, это может иметь катастрофические последствия. Как и в случае внешних хакерских атак, целые фабрики могут быть закрыты или секреты производства украдены. Более того: трояны, встроенные в оборудование, могут уклоняться от постквантовой криптографии.

«Мы все еще очень мало знаем о том, как аппаратные трояны используются настоящими злоумышленниками», - объясняет Георг Зигл. «Чтобы разработать защитные меры, нам нужно думать как злоумышленник и пытаться разработать и скрыть наши собственные трояны. Поэтому в нашем постквантовом чипе мы разработали и установили четыре аппаратных трояна, каждый из которых работает совершенно по-своему».

*Чип должен быть протестирован, а затем уничтожен*

В ближайшие месяцы профессор Зигл и его команда будут интенсивно тестировать криптографические возможности и функциональность чипа, а также обнаруживаемость аппаратных троянов. Затем чип будет уничтожен - в исследовательских целях. В сложном процессе дорожки контура будут постепенно сбриваться при фотографировании каждого последующего слоя. Цель состоит в том, чтобы опробовать новые методы машинного обучения, разработанные на кафедре профессора Зигла, для восстановления точных функций микросхем даже при отсутствии документации. «Эти реконструкции могут помочь обнаружить компоненты микросхемы, которые выполняют функции, не связанные с реальными задачами микросхемы, и которые, возможно, были незаконно внесены в конструкцию», - говорит профессор». ***(Романов Роман. Чип с открытым исходным кодом обеспечит защиту от хакерских атак с применением квантовых компьютеров // Internetua (http://internetua.com/csip-s-otkrytym-ishodnym-kodom-obespecsit-zasxitu-ot-hakerskih-atak-s-primeneniem-kvantovyh-kompuaterov). 05.08.2021).***

***