**Науково-дослідний інститут інформатики і права**
**Національної академії правових наук України**
**Національна бібліотека України імені В. І. Вернадського**

# КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

## № 12 (грудень)

**Київ – 2019**

**Кібербезпека в інформаційному суспільстві:** Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І.Вернадського. – К., 2019. – №12 (грудень) . – 107 с.

Заснований Науково-дослідним інститутом інформатики і права Національної академії правових наук України та Національною бібліотекою України імені В.І. Вернадського у 2017 р. Видається щомісяця. Відповідальний редактор О. Довгань. Упорядники О. Довгань, Л.Литвинова, С.Дорогих. Дизайн обкладинки С.Дорогих.

Аналітичний дайджест покликаний надати інформацію з питань кібербезпеки, що є надзвичайно актуальними в контексті розвитку інформаційного суспільства, зростання кіберзлочинності, використання засобів кібертероризму у гібрідних війнах та необхідності розбудови системи забезпечення кібернетичної безпеки України відповідно до визначених стратегічних напрямків з урахуванням тенденцій розвитку кіберпростору, сучасних викликів та загроз його безпеці. Призначення дайджесту – ознайомлення широкого кола фахівців у сфері кібербезпеки, а також і всіх користувачів, які цікавляться цією проблематикою, з інформаційними джерелами мережі Інтернет та новими надходженнями до фондів НБУВ (монографії, автореферати дисертацій, підручники, збірники наукових праць, матеріали міжнародних конференцій, статті з періодичних видань), що висвітлюють сучасні проблеми кібербезпеки в Україні та за кордоном.

Ознайомитися з літературою із фондів НБУВ та онлайновими інформаційними ресурсами можна за адресою: проспект Голосіївський, 3, м. Київ, 03039.

# ЗМІСТ

**«Під час засідання Ради національної безпеки і оборони України було розглянуто три питання, пов'язані з безпекою та обороною. Про це заявив секретар РНБО України Олексій Данілов під час брифінгу…**

«Кібербезпека – дуже важливий на сьогоднішній день момент. Ми щодня відчуваємо атаки з певних територій на наш кіберпростір», — додав секретар РНБО…» ***(Оборона, реінтеграція та кібербезпека: що обговорювали на засіданні РНБО // Судово-юридична газета (https://sud.ua/ru/news/ukraine/156299-oborona-reintegratsiya-ta-kiberbezpeka-scho-obgovoryuvali-na-zasidanni-rnbo). 07.12.2019).***

***

**«Міністерство та комітет цифрової трансформації України планує кардинально "цифровізувати" українську освіту. Мета – підготовка українців для життя в сучасних умовах.**

Про плани "цифровізації" йдеться на офіційному сайті Міністерства та комітету цифрової трансформації України.

Майбутнє України належить соціально відповідальним, прогресивним та освіченим українцям. І ми рішуче налаштовані зробити майбутнє – теперішнім. Саме тому одним зі стрижневих напрямів нашої роботи є цифровізація української освіти в усіх її проявах, – йдеться на сайті міністерства.

Для цього розробили 4 головні завдання

100% електронного документообігу;

забезпечення закладів освіти е-підручниками та освітніми онлайн-ресурсами;

надання учням та батькам доступ до оцифрованих навчальних планів, матеріалів уроків, а також розкладу та оцінок в е-щоденнику;

створення факультативів у форматі змішаного навчання з таких предметів: цифровий маркетинг, кібербезпека, підприємництво і так далі.

Також у відомстві хочуть, щоб в університетах та училищах з'явились курси із "цифрових професій".

У міністерстві обіцяють, що українці стануть свідками національної кампанії з цифрової грамотності…» ***(Ростислав Струтинський. Кібербезпека та електронні підручники – які зміни чекають на освіту в Україні // Телеканал новин «24» (https://24tv.ua/education/kiberbezpeka_ta_elektronni_pidruchniki__yaki_zmini_chekayut_na_osvitu_v_ukrayini_n1244898). 06.12.2019).***

***

**«Украинское образование должно стать более цифровым, привлекая к учебному процессу современные технологии.**

…Министерство цифровой трансформации рассказало, какие приоритеты в этой трансформации.

Общеобразовательные школы в ближайшее время должны стать такими:

100% электронного документооборота;

использовать в учебном процессе электронные учебники и образовательные онлайн-ресурсы;

предоставлять учащимся и родителям доступ к оцифрованным учебным планам, материалам уроков, а также расписанию и оценкам в электронном дневнике;

создавать факультативы в формате смешанного обучения по таким предметам, как цифровой маркетинг, кибербезопасность, предпринимательство и тому подобное.

В профессиональных училищах и заведениях высшего образования планируется создать креативные специальности из списка «цифровых профессий». Эти организации также будут использовать в учебном процессе онлайн-курсы и электронные ресурсы.

Минцифры в рамках проекта «Действие: цифровое образование» занимается разработкой нового формата обучения. Им станут образовательные сериалы, сюжеты которых будут базироваться на принципах «эдьютейнмента». Это игровое обучение и форма учебного процесса, в которой участники реализовывают различные жизненные ситуации. Такой формат должен помочь усваивать знания, навыки, умения, эмоции и оценки.» ***(Евгений Радченко. Минцифры планирует учить при помощи сериалов // Независимый Регион (https://nr2.com.ua/tehnologii/2019/12/07/mincifry-planiryet-ychit-pri-pomoshi-serialov/). 07.12.2019).***

***

**«За даними Національної поліції України з січня по листопад 2019 року в Україні вчинено понад 4 тисяч кіберзлочинів.** Про це під час слухань комітету цифрової трансформації на тему Національної кібербезпеки та кіберзахисту України повідомив начальник департаменту кіберполіції Нацполіції України Олександр Гринчак.

"За даними Нацполіції прослідковується чітка тенденція збільшення кількості кіберзлочинів. У 2015 році вчинено 2900 злочинів. За 11 місяців 2019 року вчинено вже 4100 злочинів. Як свідчить практика, ні державний, ні приватний сектор не мають 100% захисту від протиправних посягань у кіберпросторі", - зазначив Гринчак.

В Україні кіберполіція стикається з такими злочинами як онлайн-шахрайство, викрадення коштів з банківських карток, розповсюдження дитячого порно тощо.

"Зупинюся коротко на тих видах злочинів, з якими стикається кіберполіція: онлайн-шахрайство, викрадення коштів з банківських карток, з банківських рахунків при використанні клієнтбанків, виготовлення та розповсюдження дитячої порнографії, втручання в електронні обчислювальні машини, отримання доступу до персональних даних", - сказав Гринчак.

За його словами, боротьба з кіберзлочинами має відбуватися шляхом налагодження співпраці з приватним державним сектором…». ***(Леся Диброва. Онлайн-шахрайство і дитяче порно: кіберзлочинність в Україні зростає // InfoKava.com (https://infokava.com/uk/72504-onlajn-shahrajstvo-ditjache-porno-kberzlochinnst-v-ukrayin-zrostaye.html). 25.12.2019).***

***

**«Все більше кіберзлочинців в Україні використовують для своїх атак штучний інтелект.** Про це повідомив заступник голови комітету з питань цифрової трансформації Олександр Федієнко, передає пресслужба ВРУ…

За його словами, у 2020 році будуть нові спроби злочинців атакувати об'єкти з відкритим кодом.

"Буде зростати потреба в таких процесах, як фонові перевірки розробників та відкриті джерела розробників. На даний час середовище з відкритим кодом повністю базується на довірі. Організації, як правило, не верифікують попередні проекти через репутацію розробників", - повідомив Федієнко…». ***(Антоніна Карташева. Кіберзлочинці для своїх атак використовують штучний інтелект – Федієнко // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1843226-kiberzlochintsi-dlya-svoyikh-atak-vikoristovuyut-shtuchniy-intelekt-fediyenko). 24.12.2019).***

***

**«Урядова команда реагування на комп'ютерні надзвичайні події посіла четверте місце на міжнародних навчаннях з кібербезпеки.**

Про це повідомляється на сайті Спеціалізованого структурного підрозділу Державного центру кіберзахисту України CERT-UA.

"Фахівці Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA посіли 4 місце на міжнародних навчаннях з кібербезпеки Cyber Shield 2019, які проводилися в Анкарі, Туреччина, 19-20 грудня 2019 року за підтримки Міністерства транспорту та інфраструктури Туреччини, Управління інформаційно-комунікаційних технологій Туреччини та Міжнародного союзу телекомунікацій(ITU)", - йдеться в повідомленні.

Всього на навчаннях було представлено 19 команд, що представляли 16 країн Європи, Близького Сходу та Азії. Навчання Cyber Shield 2019 проходили у вигляді змагань. Кожна команда контролювала свою мережу, яка імітувала мережу організації, на яку здійснювалися кібератаки. Бали нараховувались по 3 показникам: виявлення кібератак та усунення їх наслідків; доступність публічних сервісів організації та блокування доступу до приватних сервісів організації.

Найвищі сходинки за підсумками змагань посіли команди Іспанії, Литви та Туркменистану.

"Зазначенні навчання пропонують унікальну можливість взяти участь у численних технічних заходах із кібербезпеки", - наголосили в CERT-UA.

Основними завданнями навчань є підвищення можливостей реагування на кіберінциденти, розширення розуміння кібер-ризиків та пов'язаних з цим наслідків та забезпечення взаємодії серед міжнародних суб'єктів забезпечення кібербезпеки, особливо національних команд CERT. В навчаннях відпрацьовуються різні сценарії, що стосуються найбільш поширених типів кібератак. Крім того, були там й вправи із захисту критичних інфраструктур та складні загрози кібербезпеки, з якими можуть зіткнутися установи та організації». ***(Урядова команда посіла четверте місце на міжнародних навчаннях з кібербезпеки // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (http://day.kyiv.ua/uk/news/241219-uryadova-komanda-posila-chetverte-misce-na-mizhnarodnyh-navchannyah-z-kiberbezpeky). 24.12.2019).***

***

**«Комітет з питань цифрової трансформації рекомендував Верховній Раді України провести парламентські слухання щодо стану кібербезпеки в Україні та розробити нову стратегію на 2020-2025 роки.** Про це під час слухань комітету цифрової трансформації на тему Національної кібербезпеки та кіберзахисту України повідомив заступник голови комітету Олександр Федієнко…

"Рекомендувати провести парламентські слухання щодо стану кібербезпеки, питань критичної інфраструктури та питань електронної комунікації в Україні - це питання телекомунікацій", - зазначив Федієнко.

За його словами, варто також змінювати державну стратегію кібербезпеки.

"Логічним завданням було б розроблення принципово нової стратегії кібербезпеки України на період 2020-2025 років, як документ довгострокового планування, що визначає загрози кібербезпеки України, пріоритети на напрямки кібербезпеки України, що створюється на базі стратегій Нацбезпеки України", - сказав Федієнко.» ***(Антоніна Карташева. Раді рекомендували розробити нову стратегію кібербезпеки України // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1843068-radi-rekomenduvali-rozrobiti-novu-strategiyu-kiberbezpeki-ukrayini). 23.12.2019).***

***

**«Кабінет міністрів України виділив 12,3 млн гривень на створення єдиного центру зберігання та обробки даних у сфері національної безпеки та оборони, повідомив прем'єр-міністр України Олексій Гончарук у середу.**

За його словами, Кабмін працює над створенням єдиного центру даних у сфері нацбезпеки.

"Великий масив інформації буде оперативно аналізуватися та надходитиме до Апарату РНБО під надійним кіберзахистом. Це значно послабить ризики витоків інформації", - написав він у Telegram.

Раніше повідомлялося, що Кабінет міністрів запускає бета-версію мобільного додатку "Дія", який, зокрема, дасть змогу користуватися електронним водійським посвідченням і електронним технічним паспортом автомобіля. У той же час триває робота із впровадження інших електронних послуг…». ***(Кабмін виділив понад 12 млн гривень на створення єдиного центру даних у сфері нацбезпеки // Дзеркало тижня. Україна (https://dt.ua/UKRAINE/kabmin-vidiliv-ponad-12-mln-griven-na-stvorennya-yedinogo-centru-danih-u-sferi-nacbezpeki-333263_.html). 18.12.2019).***

***

**«Відомий український експерт з кібербезпеки, провідний розробник компанії ІТ-Лабораторія Олександр Галущенко виявив у відкритому доступі базу даних якоїсь «колекторської» фірми з даними тисяч громадян України.**

Про це повідомив в рамках флешмобу #fuckresponsibledisclosure, спрямованого на публічні сповіщення про порушення безпеки…

На сервері, що знаходиться у відкритому доступі в мережі – статистика дзвінків колекторів, метадані та номери телефонів боржників. Судячи з усього,

«Розшарені» в мережу виявилися дані телефонії однієї з колекторських фірм, що працюють з низкою великих банків.

– Банки. Кредити. Колектори. Дзвінки. Статистика. Компанія на аутсорс. Розшарені папки. Вільний доступ. Метадані в таблицях. Прямі посилання на бази даних, зашиті в скриптах. Сумно. Судячи з архіву, діяльність ця компанія веде багато років, – прокоментував Олександр Галущенко.

Також, як стало відомо, сервер колекторської компанії може бути заражений і, відповідно, чутливі дані могли «витекти» до зловмисників.

Судячи з опублікованих скриншотам, в базі даних – відомості про українців, які є боржниками таких банків як ПУМБ, монобанк, Альфа Банк, ІдеяБанк і багатьох інших.

У монобанк вже підтвердили, що витік стався в компанії, яка є його партнером:

– На щастя номерів телефону клієнтів моно [у відкритому доступі – Ред.] Немає, тільки звіти по дзвінках. Але вкрай неприємно від партнерів такі сюрпризи отримувати, – повідомив фахівець з безпеки і ризиків monobank Дмитро Ковалевський. – Це хоч і не фатальний удар по репутації, але неприємний інцидент, в результаті якого зараз запущено розгляд. Ми дуже багато інвестуємо в те, щоб витоків не було, і завжди вкрай негативно ставимося до передачі будь-яких даних про клієнтів стороннім (в тому числі по тристороннім договорами) організаціям, навіть операторам зв'язку, які і так знають хто чий клієнт.

Як розповів нашому виданню Олександр Галущенко, банки дуже активно вирішували проблему – протягом 10 хвилин після публікації на зв'язок з експертом вийшли представники цілого ряду банків, згаданих в запису.

На даний момент сервер колекторської компанії вже відключений. За наявними у нас даними, юристи деяких банків уже готують позови до цієї компанії за недотримання правил обробки і зберігання даних». ***(База з тисячами боржників українських банків виявилася у відкритому доступі // Рідний край (http://ridnyi.com.ua/news/2019/12/18/post-37823). 18.12.2019).***

***

**«Группа компаний «Бакотек» в партнерстве с ObserveIT, Netwrix, Cloudflare и Flowmon провели роудшоу по кибербезопасности в Киеве, Днепре, Львове. Тематические семинары InfoSec MeetUp раскрывали вопросы борьбы с инсайдерами, внутренней безопасности организаций, выявления аномалий в сетевом трафике и защиты приложений с помощью облачных сервисов.**

О том, как бороться с инсайдерскими угрозами, а также о контексте действий пользователей с решением ObserveIT рассказал инженер по технической поддержке проектов Bakotech Group Максим Маковецкий. По его словам, продукт указывает именно на то, что делает пользователь, а не то, что делает компьютер.

Решение также сокращает время расследования инцидентов с дней – до считанных минут, дает возможность полного просмотра пользовательских логинов, учетных записей, конечных точек и приложений, помогает предупредить инсайдеров через оповещения для пользователей о несоответствующих действиях или действиях вне политик. ObserveIT дает возможность выявлять и исследовать

рискованную пользовательскую активность через выявление аномального поведения и многое другое.

65% опрошенных в ходе исследования ObserveIT понимают значение термина «внутренняя угроза», а 90% сотрудников в возрасте 45-64 лет и 66% в возрасте 18-24 лет утверждают, что следуют политике безопасности в компании. Несмотря на вышеуказанную статистику, аналитическая компания Ponemon Institute отмечает, что с 2016 г. среднее количество инцидентов ИБ, виновниками которых являются сотрудники компаний или подрядчики, увеличилось на 16%. Именно потому защита корпоративных данных играет в системе безопасности ведущую роль.

В свою очередь, менеджер корпоративных продаж в Bakotech Group Артем Семко раскрыл тему мониторинга событий в ИТ-инфраструктуре с помощью продукта Netwrix Auditor. Он рассказал, подробнее о платформе для обзора и анализа поведения пользователей, а также сокращения рисков из-за изменений, настроек и прав доступа в ИТ-инфраструктуре. По его словам, решение предоставляет данные для анализа и определения брешей в безопасности, аномалий в поведении пользователей и расследования инцидентов информационной безопасности. Кроме того, в ходе отдельной презентации, он рассказал о возможностях классификации данных с еще одним решением Netwrix Data Classification.

О выявлении аномалий в сетевом трафике с помощью решений Flowmon Networks рассказал Николай Брыков – инженер по технической поддержке проектов вендора. По его мнению, мониторинг сети – очень важен, поскольку без видимости на уровне сетевого трафика невозможно эффективно управлять сетью и защищать ее.

В ходе доклада он рассказал про основные технологии мониторинга сетевого трафика:

SNMP (мониторинг) – базовый уровень, отсутствует детальная информация;

Мониторинг потока (NetFlow/IPFIX мониторинг) – подробный обзор всех сообщений; в сети

Пакетный анализ – детальный, ресурсоемкий, необходим время от времени.

Кроме того, были представлены решения ведущего вендора в сфере доставки контента Cloudflare. Инженер по технической поддержке проектов в группе компаний «Бакотек» Илья Мельников представил облачную платформу вендора для защиты ИТ-инфраструктуры организаций. В частности, решение Cloudflare WAF способно защитить веб-приложения без изменения существующей инфраструктуры и модуль защиты от DDoS/ DoS-атак, обладающий емкостью в 30 Tbps, который может справиться с любой современной распределенной атакой, в том числе – на DNS-инфраструктуру. Также во время доклада была представлена подписка на комплексный сервис защиты предприятий – Cloudflare Enterprise Plan.

В ходе мероприятия специалисты «Бакотек» и вендоров провели демонстрацию решений Netwrix, ObserveIT и Flowmon. Таким образом, участники узнали, как расследовать инциденты кражи персональных данных и несанкционированных изменений в системе с помощью Netwrix, как бороться с инсайдерами с ObserveIT, технологические особенности технологии NetFlow и ее

применение для поведенческого анализа сети при помощи Flowmon, а также как минимизировать риски от DDoS-атак и предотвращать утечки данных с Cloudflare». ***(«БАКОТЕК» провел серию семинаров по кибербезопасности // Компьютерное Обозрение (https://ko.com.ua/bakotek_provel_seriyu_seminarov_po_kiberbezopasnosti_131306). 19.12.2019).***

***

**«У Комітеті з питань цифрової трансформації Верховної Ради відбулися слухання: «Національна кібербезпека та кіберзахист України, в тому числі у сфері критичної інфраструктури».**

До обговорення цієї актуальної теми також долучилися народні депутати парламентських комітетів з питань національної безпеки та оборони, правоохоронної діяльності, гуманітарної та інформаційної політики, представники центральних органів державної влади, громадських організацій, бізнесу, вчені.

Відкриваючи захід, заступник голови Комітету, голова підкомітету цифрової інфра-структури, електронних комунікацій та смарт-інфраструктури Олександр Федієнко (на знімку) наголосив на важливості проблеми для наших співгромадян. Адже нині кожен стикається з інформаційними технологіями — від соціальних мереж Інтернету до користування банкоматами, платіжними системами тощо.

«В Україні вже багато років ведеться мова про реформи для покращення життя кожного з нас. Цифрова трансформація суспільства, проголошена одним із пріоритетів Президента України, може і повинна стати базовою умовою для такого покращення», — зазначив Олександр Федієнко.

Доповідач пояснив, що комп'ютерні комунікаційні технології вже стали технологічною базою для здійснення діяльності на рівні держави, суспільства, у сферах енергетики, фінансів і транспорту, великого та малого бізнесу. Саме їх запровадження дає змогу значно підвищити ефективність будь-якої сфери. Але поряд з великою кількістю переваг цифролізація створює середовище для загроз.

Заступник голови комітету наголосив, що кількість та різноманітність кібератак у світі зростає, а держави та суспіль-ства у цьому плані стають дедалі уразливішими, тож потребують більше змістовного захисту. Олександр Федієнко нагадав, що чинним законодавством України визначено поняття «кібербезпека — захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі».

Задля розв'язання проблеми кіберзлочинів необхідно провести комплексний перегляд законодавства щодо питань інформаційної безпеки, сформувати узгоджену з міжнародними стандартами нормативно-правову базу та вдосконалити законодавство у сфері кіберзахисту. Важливим кроком є також розробка принципово нової Стратегії кібербезпеки України на період 2020—2025 років.

За словами Олександра Федієнка, «неможливо здійснювати масштабні та системні захисти у будь-якій сфері без знання її стану, без знання статистичних відповідних процесів. Тому в державі необхідно побудувати всеосяжну систему

регулярної оцінки стану кібербезпеки, постійного моніторингу та спостереження кіберінцидентів на основі надійних даних».

Дискусію підтримали представники центральних органів влади — Міністерства оборони, Служби безпеки України, Національної поліції, Національного банку.

Як повідомляє офіційний сайт Комітету Верховної Ради України з питань цифрової трансформації, за результатами виступів та обговорення комітет готує відповідні рекомендації органам державної влади щодо здійснення заходів для вдосконалення національного законодавства з кібербезпеки та кіберзахисту в Україні, зокрема у сфері критичної інфраструктури». ***(Іван ЛАЗНЮК. Інформаційна безпека: нормативна база потребує осучаснення // „Голос України (http://www.golos.com.ua/article/325773). 27.12.2019).***

***

## *Національна система кібербезпеки*

---

**«Президент Володимир Зеленський звільнив Миколу Кулешова з посади начальника Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ.**

Відповідний указ №886/2019 опублікований на сайті глави держави.

…Кулешова було призначено на цю посаду указом Президента №590/2019 від 9 серпня 2019 року…» ***(Зеленський звільнив керівника департаменту кібербезпеки СБУ // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (https://day.kyiv.ua/uk/news/051219-zelenskiy-zvilniv-kerivnika-departamentu-kiberbezpeki-sbu). 05.12.2019).***

***

**«У Раді національної безпеки та оборони відбулось засідання щодо вдосконалення роботи Головного ситуаційного центру…**

“Згідно з дорученням Президента України Володимира Зеленського в Апараті РНБО України відбулися засідання робочих груп щодо вдосконалення роботи Головного ситуаційного центру. Виконавцям було презентовано модель роботи Головного ситуаційного центру України, зокрема у частині вимог до інформації та даних, що передаються до нього, а також маршрутів передачі таких даних”, — йдеться у повідомленні.

Вказано, що під час засідання обговорили питання вдосконалення роботи ситуаційного центру і впровадження на рівні державних органів та компаній єдиного підходу до процесу збору, передачі та накопичення даних.

“Представники Апарату РНБО України наголосили на необхідності накопичення та узагальнення у Головному ситуаційному центрі виключно достовірних верифікованих даних, на підставі яких ухвалюватимуться стратегічні рішення у сферах національної безпеки”, — додали у пресслужбі…» ***(Дар'я Панченко. У РНБО взялись за вдосконалення Головного ситуаційного центру // Інформаційне агентство «Українські Національні Новини»***

***(https://www.unn.com.ua/uk/news/1839464-u-rnbo-vzyalis-za-vdoskonalennya-golovnogo-situatsiynogo-tsentru). 04.12.2019).***

***

**«Чи можна захиститися від технологій, які роблять нас і цілі держави дедалі прозорішими? Як не впійматися на вудку перших, куди ми роками добровільно зливаємо дані про себе, і захиститися від других, що безцеремонно зламують наші таємниці?** …розповів експерт по кібербезпеці, співзасновник компанії Hacken, конференції HackIT і Школи "білих" хакерів Єгор Аушев…

"Кілька років тому було прийнято закон про основи кібербезпеки, — продовжує Єгор Аушев. — Досить рамковий і неглибокий закон, у якому не торкнулися й не описали багатьох речей. Тому ми чекаємо нового закону. Тим часом ми розуміємо, що один закон ситуацію не змінить. В нас усе давно застаріло. Підходи, стандарти… держава підходить до цієї теми за абсолютно залишковим принципом. Попри те що ми вже прогриміли на весь світ з вірусом notPetya".

"У 2017 році я був радником з кібербезпеки Укроборонпрома, — уточнює Єгор Аушев. — Спочатку була цікава ідея створити окремий кіберцентр на базі Укроборонпрому. На сьогодні в Україні є один державний кіберцентр CERT-UA, який захищає всю державну інфраструктуру. У Німеччині, наприклад, таких центрів тридцять три. В Чехії — більше двадцяти, в Польщі — близько десятка. Ми почали працювати над проектом, виписувати систему й алгоритм її запуску, провели кілька аудитів підприємств, які вже можна було підключати до такого собі центру, але… справа застопорилася. З невідомих мені причин".

"Сьогодні обнадіює те, що з'явився окремий орган виконавчої влади — Міністерство цифрової трансформації. Ми почали спілкування і з міністерством, і з РНБО, і з ОП. Даємо рекомендації. Я не можу сказати, на якому рівні серйозності і розуміння з нами спілкується держава. Але поки немає якихось блокувань і небажання слухати", — завершив Єгор Аушев…» ***(Експерт вважає, що вірус notPetya не навчив державу захищати себе // Дзеркало тижня. Україна (https://dt.ua/UKRAINE/ekspert-virus-notpetya-ne-navchiv-derzhavu-zahischati-sebe-331709_.html). 03.12.2019).***

***

**«В Апараті РНБО України працюють над розвитком Національного координаційного центру кібербезпеки (НКЦК), який займатиметься прогнозуванням і виявленням потенційних і реальних кіберзагроз.**

Про це повідомили у прес-службі РНБО в суботу, 14 грудня.

Зазначається, що у наступні п’ять-десять років кіберзброя стане номером один у світі, навіть ядерна зброя відійде на другий план.

У глобалізованому світі, де війни стають дедалі гібридними, захист інформації та пристроїв для роботи з нею є вкрай важливим, оскільки для кіберзлочинів немає кордонів.» ***(В Україні створять Центр із прогнозування і виявлення кіберзагроз // Internetua (http://internetua.com/v-ukrayini-stvoryat-centr-iz-prognozuvannya-i-viyavlennya-kiberzagroz). 15.12.2019).***

***

**«Володимир Зеленський підписав ухвалену РНБО програму щодо посилення кібербезпеки.**

Президент Володимир Зеленський увів у дію рішення Ради національної безпеки та оборони України щодо посилення спроможностей держави у сфері кібербезпеки.

Відповідний Указ оприлюднено на сайті глави держави.

– Увести в дію рішення Ради національної безпеки і оборони України від 7 грудня 2019 року Про невідкладні заходи з посилення спроможностей держави у сфері кібербезпеки, – йдеться у документі.

Контроль за виконанням цього рішення покладено на секретаря РНБО Олексія Данілова…» ***(Зеленський увів у дію рішення РНБО щодо посилення кібербезпеки // ФАКТИ. ICTV (https://fakty.com.ua/ua/ukraine/20191221-zelenskyj-uviv-u-diyu-rishennya-rnbo-shhodo-posylennya-kiberbezpeky/). 21.12.2019).***

***

**«Секретар Ради національної безпеки та оборони Олексій Данілов назвав сферу кібербезпеки ключовою складовою національної безпеки.**

Про це передає пресслужба РНБО.

«У наступні п'ять-десять років кіберзброя стане номером один у світі, навіть ядерна зброя відійде на другий план», — сказав Данілов.

Він додав, що у глобалізованому світі, де війни стають гібридними, захист інформації та пристроїв для роботи з нею є вкрай важливим, бо для кіберзлочинів не існує кордонів.

Секретар РНБО повідомив про роботу над оновленою Стратегією кібербезпеки, і зазначив, що у відомстві триває робота над Національним координаційним центром кібербезпеки. Його головним завданням буде прогнозування та виявлення потенційних і реальних кіберзагроз.

Також заступник секретаря РНБО України Сергій Демедюк додав, що Національний координаційний центр взаємодіятиме з аналогічними центрами країн-партнерів». ***(Євгенія Луценко. У РНБО назвали кібербезпеку ключовою складовою нацбезпеки України // Громадське Телебачення (https://hromadske.ua/posts/u-rnbo-nazvali-kiberbezpeku-klyuchovoyu-skladovoyu-nacbezpeki-ukrayini). 14.12.2019).***

***

**«Секретарь СНБО отметил необходимость обеспечения физической и кибернетической безопасности объектов критической инфраструктуры**

При Совете национальной безопасности и обороны Украины будет создан Совет экспертов по вопросам энергетической безопасности. Об этом сообщил секретарь СНБО Алексей Данилов после заседания рабочей группы по вопросам преодоления угроз в энергетической сфере, сообщает пресс-служба СНБО.

«Совет экспертов по вопросам энергетической безопасности будет действовать как консультативный орган и решать вопросы безопасности в энергетической сфере. На данный момент уже разрабатывается проект Положения этого Совета и созданы рабочие группы по направлениям в энергетической сфере», - сказал секретарь СНБО…

Кроме того, рассматривая вопрос безопасности энергетического рынка Украины, секретарь СНБО отметил необходимость обеспечения физической и кибернетической безопасности объектов критической инфраструктуры.

«Наша критическая энергетическая инфраструктура должна быть полностью защищена не только от физических угроз, но и от потенциальных кибератак. Более того, это звено не должно пострадать после окончательного анбандлинга НАК «Нафтогаз», - отметил он…». ***(При СНБО будет создан Совет по вопросам энергобезопасности // Українські медійні системи (https://glavcom.ua/ru/news/pri-snbo-budet-sozdan-sovet-ekspertov-po-voprosam-energobezopasnosti-649383.html). 26.12.2019).***

***

## *Правове забезпечення кібербезпеки в Україні*

---

**«Крупнейшая в стране отраслевая организация, объединяющая операторов и провайдеров телекоммуникаций, – Интернет Ассоциация Украины, – направила письма в Госспецсвязи, Государственную регуляторную службу и Минюст с просьбой не согласовывать проекты постановлений КМУ «Об утверждении Порядка отнесения объектов к критической инфраструктуры» и об утверждении порядков формирования перечня ОКИ.** В ИнАУ утверждают: документы не соответствуют европейскому законодательству…

ГСССЗИ опубликовала проект постановления Кабинета Министров Украины «Об утверждении порядка отнесения объектов к объектам критической инфраструктуры». Документом предлагается утвердить сам порядок отнесения объектов к объектам критической инфраструктуры, перечень секторов основных услуг критической инфраструктуры государства и методику категоризации ОКИ. За информационным сектором ОКИ закреплено Минцифры. Также в конце ноября был опубликован проект постановления Кабинета Министров Украины «Об утверждении порядков формирования перечня объектов критической информационной инфраструктуры, внесение объектов критической информационной инфраструктуры в государственный реестр объектов критической информационной инфраструктуры, его формирование и обеспечение функционирования»

– Анализ этих проектов показал, что перечень предлагаемых типов основной услуги критической инфраструктуры в них не соответствует перечню, определенному в Директиве Европейского Парламента и Совета (ЕС) 2016/1148 от 6 июля 2016 года, – объясняют свою позицию в ИнАУ.

В частности, объясняют в Интернет Ассоциации Украины, речь идет о безосновательноем расширении этого перечня, а также о невыполнении позиции Евродирективы об избежании возложения непропорционального финансового и административного бремени на операторов основных услуг и поставщиков цифровых услуг, где, в частности, говорится, что в случае поставщиков цифровых

услуг, такие требования не должны применяться к малым и микропредприятиям. Также в письмах приводится ряд других несоответствий законодательству.

Письма содержат предложения учесть замечания ИнАУ и не согласовывать проект постановления КМУ в предложенной разработчиком редакции как таковой, не в полной мере соответствует законодательству.» ***(Владимир Кондрашов. ИнАУ: два проекта постановления кабмина прямо противоречат европейскому законодательству // Internetua (http://internetua.com/inau-dva-proekta-postanovleniya-kabmina-pryamo-protivorecsat-evropeiskomu-zakonodatelstvu). 12.12.2019).***

***

## *Кібервійна проти України*

---

**«Суб'єкти національної системи кібербезпеки щодня фіксують і нейтралізують кіберінциденти, за останній місяць відбито 11 кібератак.**

Про це повідомив Секретар Ради національної безпеки і оборони України Олексій Данілов на брифінгу по завершенні закритого засідання РНБО України…

За його словами, кібератакам постійно піддаються, зокрема, банківська система, офіційний веб-сайт Глави держави.

«Суб'єкти національної системи кібербезпеки працюють у режимі «24/7/365», відбиваючи ці загрози, - сказав О. Данілов. - Це зброя майбутнього, і Президент України приділяє питанню кіберзахисту дуже велику увагу». «Якщо ми говоримо про діджиталізацію та цифровізацію держави, маємо розуміти, що ця цифра має бути захищена», - додав він.

При цьому Секретар РНБО України високо оцінив професіоналізм співробітників служб, які працюють у сфері кібербезпеки.» ***(Український кіберпростір за місяць атакували 11 разів // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (http://day.kyiv.ua/uk/news/081219-ukrayinskyy-kiberprostir-za-misyac-atakuvaly-11-raziv). 08.12.2019).***

***

**«Вибори у США 2016 року є болючою темою для американців. Неодноразово висловлювалися думки про вплив на їхній хід інших держав.** Директор Федерального бюро розслідувань (ФБР) США Крістофер Рей вніс ясність у питання щодо можливого втручання України у президентські вибори в США 2016 року.

У ФБР немає ніяких підстав вважати, що Україна прямо або опосередковано втручалася в американські вибори 2016 року, заявив директор ФБР у недавньому інтерв'ю виданню ABC News.

На думку Рея, США на чергових президентських виборах 2020 року треба боятися Росії. У ФБР вважають, що саме Російська Федерація представляє найбільшу загрозу для США.

Якщо вплив України на вибори було лише припущенням, то втручання Росії є вже доведеним фактом. Ще 25 липня 2019 року Комітет Сенату з розвідки оприлюднив свій звіт про втручання Росії в американські вибори 2016 року.

У звіті уточнюється, що вплив Росії на процеси, що відбуваються у США, тільки посилюється. Тому є велика ймовірність того, що РФ планує вплинути на вибори президента США, які будуть проходити у 2020 році…» ***(Доказів втручання України у вибори в США немає — ФБР // Ракурс (https://racurs.ua/ua/n130610-dokaziv-vtruchannya-ukrayiny-u-vybory-v-ssha-nemaie-fbr.html). 10.12.2019).***

***

**«Чиновник високого рангу спростував звинувачення на адресу України**

Розслідування про можливе втручання України в президентські вибори в США все впевненіше доводить, що такого не було. Це починають розуміти навіть найстійкіші прихильники цього звинувачення.

Заступник держсекретаря США з політичних питань Девід Гейл у вівторок рішуче спростував теорію про те, що у виборах 2016 втручалася Україна, а не Росія…

Коли сенатор-демократ Роберт Менендес запитав Гейла, чи є в нього докази українського втручання, дипломат відповів: "Ні".

Негативну відповідь він дав на запитання про те, чи було російське втручання у вибори "фальсифікацією", як часто говорить президент Дональд Трамп.

"Так, за оцінками розвідувального співтовариства, російський президент Володимир Путін розпорядився вести кампанію впливу в 2016 році, націлену на наші президентські вибори", - сказав Гейл, виступаючи в сенатському Комітеті з міжнародних відносин.

За словами Гейла, у нього немає підстав сумніватися в достовірності свідчень колишньої співробітниці Ради національної безпеки Фіони Хілл, яка сказала, що теорія про українського втручання - пропаганда, поширювана Росією…

У США відразу кілька державних відомств, включаючи Пентагон опублікували спільну заяву, в якій говориться, що РФ, Китай та Іран можуть спробувати втрутитися в президентські вибори 2020 року, повідомляє прес-служба штаб-квартири Міністерства оборони США.

"Росія, Китай, Іран та інші іноземні недружні суб'єкти будуть намагатися втручатися у виборчий процес чи впливати на рішення виборців", - йдеться в заяві.

За даними уряду і американських спецслужб, втручання у вибори буде здійснюватися за допомогою різних засобів, включаючи кампанії в соціальних мережах, заходи з метою дезінформації суспільства, або здійснюючи руйнівні кібератаки на федеральну і місцеву виборчу інфраструктуру"…» ***("Теорія змови" про втручання України в американські вибори продовжує розсипатися // Дзеркало тижня. Україна (https://dt.ua/POLITICS/teoriya-zmovi-pro-vtruchannya-ukrayini-v-amerikanski-vibori-prodovzhuye-rozsipatisya-331807_.html). 04.12.2019).***

***

**«Служба безопасности пресекла деятельность группы лиц, которые организовывали массовую регистрацию и дальнейшее продвижение фейковых аккаунтов в любых сервисах интернет.**

Как сообщает пресс-центр СБУ, установлено, что злоумышленники активно предоставляли услуги российской стороне и лицам, причастным к деятельности так называемой «ДНР». Аккаунты затем использовались заказчиками для установления и поддержания легендированных контактов с украинскими гражданами, проведения незаконных финансовых операций, пересылку через операторов почтовой связи товаров, изъятых из законного оборота.

«Ботоферма» также использовалась организаторами для массового распространения деструктивных публикаций в соцсетях и мессенджерах, рассылки ложных сообщений о «минировании», а также других действий, направленных на дестабилизацию общественной обстановки в Украине.

В Киеве правоохранители изъяли специальное техническое оборудование для создания и обеспечения деятельности «ботоферм». Оно руководило массивом SIM-карт, виртуальными мобильными телефонами, рассылкой СМС-сообщений и тому подобное. В работе комплекса использовались также SIM-карты иностранных мобильных операторов связи, в большинстве стран можно приобрести только при наличии паспорта или кураторства ФСБ РФ.

В рамках уголовного производства проведены обыски по месту расположения специального технического оборудования, во время которых получено бесспорные доказательства причастности конкретных лиц к противоправной деятельности. Продолжается следствие. Операция проводилась в ходе выполнения задач по контрразведывательной защиты интересов государства в сфере информационной безопасности.» ***(СБУ блокировала «ботоферму», предоставлявшую услуги РФ и боевикам // ForUm (https://for-ua.com/article/1188418). 04.12.2019).***

***

**«В сеть попали персональные данные украинских военнослужащих, принимавших участие в боевых действиях на Донбассе, которые потом лечились в психиатрических больницах Днепропетровской области.** Об этом говорится на странице общественной организации «Форпост» в Facebook.

Сведения распространили российские хакеры.

По данным «Форпоста», в сети были обнародованы данные о 623 пациентах. Общественности стали известны имена, фамилии и номера удостоверений УБД ветеранов.

В организации считают, что обнародование конфиденциальной информации — один из методов информационной войны, которую Россия ведет против Украины…» ***(Российские хакеры заполучили данные нескольких сотен участников АТО: что об этом известно // Факты и комментарии® (https://fakty.ua/327765-rossijskie-hakery-zapoluchili-dannye-neskolkih-soten-uchastnikov-ato-chto-ob-etom-izvestno). 13.12.2019).***

***

**«Сотрудники правоохранительных органов Украины разоблачили преступную группу, торговавшую секретной информацией.** Как сообщает пресс-служба департамента Киберполиции национальной полиции Украины, злоумышленники создали сайт, через который продавали заинтересованным лицам данные об экспорте и импорте товаров на территорию Украины, в том числе о закупках и перемещениях военной техники.

В настоящее время следствие пытается установить источник, из которого преступники получали вышеупомянутую информацию. По предварительным данным, они покупали ее в даркнете, а затем перепродавали. Клиентская база преступников насчитывала порядка полусотни человек. В целях замести следы злоумышленники разместили свой сайт на сервере заграницей…

Инцидент квалифицирован по двум статьям УК Украины: ч.2 ст.361 («Несанкционированное вмешательство в работу компьютеров, автоматизированных систем, компьютерных сетей или сетей электросвязи, приведшее к утечке потере, подделке, блокированию информации, искажению процесса обработки информации или к нарушению установленного порядка ее маршрутизации») и ч.2 ст.361-2 («Несанкционированный сбыт или распространение информации с ограниченным доступом, хранящейся в компьютерах, автоматизированных системах, компьютерных сетях или на носителях такой информации»)». ***(Украинские киберпреступники торговали данными о закупках военной техники // SecurityLab.ru (https://www.securitylab.ru/news/503366.php). 12.12.2019).***

***

**«Сотрудники украинской киберполиции задержали участников хакерской группировки, промышлявшей взломами серверов на заказ.** Преступники компрометировали удаленные серверы, принадлежащие компаниям и частным лицам, и продавали доступ к ним. Им удалось скомпрометировать более 20 тыс серверов по всему миру.

В состав группировки входили трое граждан Украины и один иностранец. Все они были участниками известных хакерских форумов и занимались заказными взломами серверов, расположенных на территории Украины, Европы и США.

Группа действовала с 2014 года. Злоумышленники получали доступ к серверам с помощью брутфорс-атак и использовали специальные программы для эксплуатации уязвимостей в серверах на базе Windows. Часть взломанных серверов они использовали в собственных целях, в частности, для осуществления DDoS-атак, организации командных центров для управления троянами-инфостилерами, а также для проведения брутфорс-атак на новые сетевые узлы.

Кроме того, группировка продавала доступ к некоторым взломанным серверам другим хакерам, которые задействовали их для вымогательских атак, кражи денег с банковских карт, майнинга и пр.

От действий киберпреступников пострадали компьютерные сети в различных странах, в том числе в Украине, России, Франции, Китае, Болгарии, Индии, Бразилии, Малайзии и странах Северной Европы.

Для координации действий преступники использовали защищенные мессенджеры, а заработанные деньги поступали на криптовалютные и электронные кошельки. На нескольких из них сотрудники полиции обнаружили в общей сложности почти $80 тыс…

По данному факту полиция начала уголовное дело по ч. 2 ст. 361 УК Украины (Несанкционированные сбыт или распространение информации с ограниченным доступом, которая сохраняется в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или на носителях такой информации).» ***(Киберпреступники из Украины взламывали серверы на заказ // SecurityLab.ru (https://www.securitylab.ru/news/503744.php). 29.12.2019).***

***

**«Сотрудники Киберполиции Украины совместно со следователями Черновицкой полиции разоблачили 22-летнего жителя Черновицкой области, похитившего данные 250 тыс. пользователей игрового сервиса.**

Являюсь участником разных тематических форумов злоумышленник самостоятельно научился основам разработки вредоносного ПО и применил обретенные знания для заработка денег, сообщает пресс-служба Национальной полиции Украины.

Преступная схема заключалась в следующем: пользователю игрового сервиса приходило сообщение о выигрыше промо-кода, предоставляющего бонусы в игре, однако для его получения необходимо было перейти по ссылке. Ссылка перенаправляла пользователя на подконтрольный злоумышленнику фишинговый сайт, замаскированный под оригинальный ресурс.

Для авторизации пользователю необходимо было ввести логин и пароль, которые затем отправлялись злоумышленнику. Собранные базы данных преступник впоследствии продавал на подпольных форумах, заработав таким образом около 250 тыс. гривен (примерно 670 тыс. рублей)…

По данному факту было возбуждено уголовное дело по ч.2 ст.361 (несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи) УК Украины.» ***(Украинский преступник продал данные 250 тыс. пользователей игрового сервиса // SecurityLab.ru (https://www.securitylab.ru/news/503735.php). 27.12.2019).***

***

## Міжнародне співробітництво у галузі кібербезпеки

**«Канада допомагає Британії відбивати "передвиборчі" кібератаки. Ідеться про співробітництво у рамках розвідувального альянсу "Five Eyes"…**

До альянсу, окрім Канади і Британії, входять США, Австралія та Нова Зеландія. Канадські спецслужби, які відповідають за радіоелектронну розвідку, криптографію та захист урядових інформаційних і комунікаційних мереж,

регулярно обмінюються з британцями зібраними даними…» ***(Сас Ольга. Канада допомагає Британії відбивати "передвиборчі" кібератаки // ООО "Национальные информационные системы" (https://podrobnosti.ua/2329855-kanada-dopomaga-britan-vdbivati-peredviborch-kberataki.html). 09.12.2019).***

***

**«Секретар Ради національної безпеки і оборони Олексій Данілов і тимчасовий повірений у справах США в Україні Вільям Тейлор обговорили під час зустрічі перспективні напрями співробітництва.**

Про це повідомляє пресслужба РНБО…

Зокрема, сторони наголосили, що важливо діяти спільно у сфері кібербезпеки.

“Сьогодні кіберзагрози виходять на перший план, і всі країни мають бути готові протидіяти їм”, – зазначив секретар РНБО України.

Крім цього, Данілов і Тейлор обговорили поточну безпекову ситуацію в Європі та світі в контексті агресії проти України і підсумки переговорів у Нормандському форматі.

Тимчасовий повірений у справах США наголосив, що Сполучені Штати незмінно підтримують Україну і готові надалі поглиблювати двосторонню співпрацю.» ***(Секретар РНБО обговорив з Вільямом Тейлором співпрацю у сфері кібербезпеки // UA|TV (https://uatv.ua/sekretar-rnbo-obgovoryv-z-vilyamom-tejlorom-spivpratsyu-u-sferi-kiberbezpeky/). 18.12.2019).***

***

**«Секретарь СНБО Украины Алексей Данилов во время встречи с делегацией сотрудников Сената Соединенных Штатов заявил, что сфера кибербезопасности является одним из важнейших приоритетов деятельности СНБО Украины…**

Данилов назвал сферу кибербезопасности ключевой составляющей национальной безопасности.

“В следующие пять-десять лет кибероружие станет номером один в мире, даже ядерное оружие отойдет на второй план”, – заявил он.

При этом секретарь СНБО добавил, что в глобализированном мире, где войны все больше становятся гибридными, защита информации и устройств для работы с ней является крайне важным, поскольку для киберпреступлений не существует границ.

“В этом контексте секретарь СНБО Украины сообщил о работе над обновленной Стратегией кибербезопасности, и отметил, что в Аппарате СНБО Украины продолжается работа над развитием Национального координационного центра кибербезопасности (НКЦК) в соответствии с современными вызовами, главной задачей которого определено, в частности, прогнозирование и выявление потенциальных и реальных киберугроз, а также обеспечение СНБО Украины аналитическими материалами”, – говорится в сообщении.

Данилов также подчеркнул, что Владимир Зеленский уделяет много внимания вопросам кибербезопасности, и по итогам заседания СНБО Украины 7 декабря принят ряд решений в этой сфере.

“В свою очередь, члены американской делегации отметили, что Украина дает отпор кибератакам. Сотрудники Сената США отметили созвучна поддержке Украины в Конгрессе и Сенате, свидетельством чего, в частности, является выделение 300 млн долл. военной помощи, а также введение санкций в отношении российской энергетик””, – говорится в сообщении». ***(Виктория Мартынюк. В СНБО назвали главную угрозу мировой безопасности // KopirkiN (https://www.kopirkin.com.ua/v-snbo-nazvali-glavnuyu-ugrozu-mirovoj-bezopasnosti/). 15.12.2019).***

***

## Світові тенденції в галузі кібербезпеки

**«Облачная платформа по разработке кибербезопасности Rezilion привлекла инвестиции в размере 8 миллионов долларов при участии Kindred Capital, LocalGlobe и Samsung NEXT, а также инвесторов-ангелов Рона Цукермана, Гая Шори и других инвесторов.**

Компания планирует продавать свою продукцию на рынке Израиля и США. Особенность их продукции заключается в том, что она не требует ручных настроек, в отличие от других программ на рынке. На эту функции учредители компании ставят самые большие ставки.

Компанию основали генеральный директор по кибербезопасности Лиран Танкман и технический директор Шломи Бутнару, чья первая компания, CyActive, была приобретена PayPal в 2015 году.» ***(Израильский стартап по кибербезопасности привлек 8 млн долл // Jewishnews (https://jewishnews.com.ua/economics-and-business/izrailskij-startap-po-kiberbezopasnosti-privlek-8-mln-doll). 11.12.2019).***

***

**«Аналитики Goldman Sachs прогнозируют на ближайшие пять лет двузнаяные показатели годового темпа роста премиального дохода в кибернетическом страховании.**

Как стало известно интернет ресурсу Укрстрахование, на сегодняшний день среднегодовой показатель премиального дохода киберстрахования составляет до $5 млрд, что менее 1% глобального коммерческого страхового рынка.

Вместе с тем, по мнению аналитиков Goldman Sachs, киберстрахование пока не сможет претендовать на роль глобального драйвера роста для страхового рынка из-за небольшого удельного веса на мировом рынке. Однако, авторы отчета подчеркивают продолжающийся рост спроса на страховые продукты в секторе киберзащиты. «Согласно оценкам Центра стратегических и международных исследований и McAfee, ущерб, связанный с киберпреступлениями во всем мире, оценивается в $600 млрд в год, или 1% мирового ВВП», — говорится в отчете.

В отчете также отмечается существующий большой разрыв между экономическими и застрахованными потерями в секторе кибербезопасности, что свидетельствует об ограниченном охвате, который предлагается в страховании

киберрисков». ***(Годовой темп роста в секторе кибернетического страхования будет иметь двузначные показатели: Goldman Sachs // Страхование Украины (https://www.ukrstrahovanie.com.ua/news/godovoj-temp-rosta-v-sektore-kiberneticheskogo-strahovaniya-budet-imet-dvuznachnye-pokazateli-goldman-sachs). 23.12.2019).***

***

## *Сполучені Штати Америки*

**«За последние два года значительно сократилось число граждан Соединённых Штатов, у которых ядерная программа Северной Кореи вызывает страх.** Об этом свидетельствуют результаты опроса, проведённого исследовательским центром Pew, в котором приняли участие свыше 1,5 тыс. человек...

Теперь на первое место среди внешних страхов жителей страны вышла угроза кибератак из других стран. На сегодняшний день их опасаются 74% опрошенных вместо 72% в 2017 году…» ***(PRC: на первое место среди внешних страхов жителей США вышла угроза кибератак из других стран // mResearcher (https://mresearcher.com/2019/12/prc-na-pervoe-mesto-sredi-vneshnih-strahov-zhitelej-ssha-vyshla-ugroza-kiberatak-iz-drugih-stran.html). 08.12.2019).***

***

## *Країни ЄС*

**«В Германии более 38 тыс. студентов придется лично простоять в очередях, чтобы получить новый пароль к университетской электронной почте…**

Согласно сообщению, администрации университета Юстаса Либига пришлось пойти на такой шаг, чтобы подтвердить личность студентов из-за "юридического требования" после кибератаки на учебное заведение.

Как отмечается, атака произошла еще 8 декабря и лишила весь университет доступа к интернету. Из-за инцидента было проведено специальное расследование с привлечением Немецкого исследовательского центра по кибербезопасности.

В официальном сообщении университета говорится о том, что все сотрудники и студенты должны лично получить свой новый личный пароль. Для этого их просят принести удостоверение личности в спортзал университета в специальное время, определенное по их дате рождения. Для обработки всех студентов надо аж пять дней.

Кроме этого, университетским персоналом были также предоставлены 1200 USB-накопителей, чтобы студенты смогли проверить компьютеры на наличие вирусов…». ***(В Германии тысячам студентов надо постоять в очереди, чтобы получить пароль к электронной почте // Западная информационная корпорация***

***(https://zik.ua/ru/news/2019/12/19/v_germanii_tysyacham_studentov_nado_postoyat_v_ocheredi_chtoby_poluchit_parol_k_elektronnoy_pochte_950833). 19.12.2019).***

***

## *Російська Федерація та країни ЄАЕС*

**«Российский оператор стал единственным участником конкурса на получение субсидии на создание киберполигона для обучения специалистов, экспертов и руководителей в области инфобезопасности**

Правила выделения субсидий на создание киберполигона для обучения и тренировки специалистов разного профиля, руководителей в области информационной безопасности и IT современным практикам обеспечения информбезопасности российское Правительство утвердило в середине октября текущего года.

Киберполигон – это инфраструктура для отработки практических навыков специалистов, экспертов разного профиля, руководителей в области информбезопасности и информтехнологий, а также для тестирования программного и аппаратного обеспечения путем моделирования компьютерных атак и отработки реакций на них.

На днях Минцифры провело конкурс на предоставление субсидии для создания киберполигона, где единственным претендентом и победителем стал Ростелеком. Первым на это событие обратил внимание канал «Телеком-ревью».

Извещение о проведении Минцифры открытого конкурсного отбора было размещено в конце ноября.

Согласно разработанным кабмином правилам, организации, подавшие заявки на конкурс для получения субсидии должны обладать собственной вычислительной инфраструктурой для создания и функционирования киберполигона; опытом оказания услуг по мониторингу информационной безопасности; опытом взаимодействия с организациями высшего профессионального образования в сфере подготовки кадров по направлениям, связанным с информбезопасностью.» ***(Ростелеком создаст киберполигон // РосКомСвобода (https://roskomsvoboda.org/53137/). 06.12.2019).***

***

**«…Крупнейшие операторы: Мегафон, Вымпелком («Билайн») и МТС поддержали идею Ростелекома о запуске на сетях связи «ханипотов» — специальных программ, имитирующих уязвимые сервисы или компьютеры.** Госоператор предложил коллегам обмениваться выявляемыми методами кибератак, а затем отрабатывать методы противодействия им. Степень заинтересованности операторов в инициативе Ростелекома разнится, но никто из «большой сотовой тройки» от идеи не отказался.

Как следует из материалов рабочей группы по направлению «Информационная безопасность» нацпрограммы «Цифровая экономика», за недавнем заседании была рассмотрена концепция создания системы раннего предупреждения о компьютерных атаках на телекоммуникационную

инфраструктуру России. Это следует из материалов группы, копия которых есть у РБК, их подлинность подтвердил руководитель группы и президент компании InfoWatch Наталья Касперская.

Как пояснила представитель Ростелекома Наталья Лезина, речь идет о создании на инфраструктуре операторов так называемых ханипотов (от англ. honeypot — «горшочек с медом») — специального софта, который имитирует работу уязвимого устройства или сервера. Обнаружив приманку, злоумышленники, вероятнее всего, попытаются проникнуть в сеть компании именно через нее. Программа записывает все действия хакеров на сервере, затем их анализируют специалисты по кибербезопасности. Также «Ростелеком» предложил наладить информационный обмен о новых методах кибератак между операторами связи.

Идея «Ростелекома» не предполагает государственного финансирования проекта, операторы установят системы сбора данных о кибератаках самостоятельно. Точную стоимость системы в компании не раскрывают, отмечая, что она зависит от метода реализации. По мнению руководителя российского исследовательского центра «Лаборатории Касперского» Юрия Наместникова, в масштабе бизнеса эти расходы будут не очень значительны, большая часть средств уйдет на подбор специалистов и на улучшение системы защиты на основании полученных данных.

Специалисты в сфере информационной безопасности называют телеком-операторов одними из наиболее заинтересованных пользователей ханипотов. Эксперт в области безопасности телекоммуникационных систем Positive Technologies Дмитрий Касымов говорит, что опорные сети операторов в принципе нельзя назвать защищенными. «При проведении аудитов безопасности мы выявляем множество уязвимостей, которые позволяют злоумышленникам оставить абонентов без связи, прослушать их разговоры и перехватить SMS, пользоваться услугами связи за их счет и даже обойти системы тарификации оператора. Эти недостатки безопасности уже эксплуатируются хакерами, в том числе для кражи денег с банковских счетов абонентов», — объяснил он.

При этом опасность для телеком-операторов могут представлять и сами ханипоты, отмечала ранее «Лаборатория Касперского». Степень угрозы зависит от сложности установленной технологии. Например, приманка верхнего уровня — это реальная зараженная система, для которой специалисты используют дополнительные меры защиты. Но при правильной настройке ханипота риск можно нивелировать.

«Мы разворачиваем софт (ханипоты и управляющие сервера), поддерживаем инфраструктуру и отдаем заказчикам статистику и вредоносные программы, которые попадают на ханипоты. Заказчики же предоставляют нам IP-пространство и вычислительные мощности, чтобы это все запустить», — сказал глава российского исследовательского центра «Лаборатории» Юрий Наместников.

Данная концепция предполагает, что операторы связи оплатят запуск сети ловушек и работу специалистов по безопасности. Наместников назвал расходы на инициативу не очень значительными, в масштабах операторского бизнеса. Самая дорогая расходная статья — оплата труда аналитиков.» ***(Операторы поддержали***

***идею Ростелекома заманивать хакеров на сервера-ловушки // РосКомСвобода (https://roskomsvoboda.org/53006/). 04.12.2019).***

***

**«В 2020 году в российской армии будут созданы специальные mesh-сети для «военного интернета», устойчивые ко взлому и подавлению.**

Данные информационные системы могут охватить площадь в тысячи километров, а их настройка не займет много времени. Военное ведомство уже готовит специальные протоколы и ПО для создания новых сетей…

Первые mesh-сети были протестированы в ходе учений «Центр-2019». Данная технология обеспечивает обмен данными на значительных расстояниях с помощью разделения одного большого маршрута на несколько коротких переходов между узлами. Для передачи информации используются радиоканалы, исключая необходимость в кабельном соединении. Передачу данных осуществляют беспроводные станции, которые и формируют так называемые «ячейки».

«Ячейки соединяются друг с другом по принципу «каждая с каждой», что дает возможность при необходимости легко найти альтернативу подавленным радиоканалам или станциям, обойдя места «обрыва». Это позволяет обеспечивать качественную голосовую связь, обмен видео и другой информацией, а также доступ к специальным приложениям», — рассказал военный эксперт Дмитрий Болтенков.

В случае необходимости новые информационные сети способны обеспечить доступ к гражданской сотовой, кабельной связи или к «военному интернету» — закрытому сегменту передачи данных (ЗСПД), по которому Минобороны отправляет секретные сообщения». ***(У российских военных появится устойчивый ко взлому интернет // SecurityLab.ru https://www.securitylab.ru/news/503376.php (https://www.securitylab.ru/news/503376.php). 12.12.2019).***

***

**«Больше всего отраженных кибератак в 2019 году были направлены против ракетно-космической, оборонной и химической отраслей**, рассказали «РИА Новости» в созданном ФСБ Национальном координационном центре по компьютерным инцидентам. Крупных инцидентов, способных повлиять на госструктуры России, в текущем году не произошло. За год было центр получил 182 уведомления об уязвимостях.

Основные центры распространения вредоносного ПО находятся за пределами России. С начала 2019 году удалось пресечь деятельность 12 тыс. зарубежных ресурсов, используемых для проведения кибератак в отношении России. Целью трети всех атак в 2019 году было хищение не информации, а денег.

Для хищения денег и кражи персональных данных используют практически все типы вредоносного ПО, а также методы социальной инженерии, фишинг и мошенничество». ***(В ФСБ назвали наиболее подверженные кибератакам отрасли // Открытые системы (https://www.computerworld.ru/news/V-FSB-nazvali-naibolee-podverzhennye-kiberatakam-otrasli). 20.12.2019).***

***

**«У понеділок, 23 грудня, у РФ провели "навчання з кібербезпеки в інтернеті"…**

Заступника міністра зв'язку РФ Олексій Соколов заявив, що завданням навчань є забезпечення надійної роботи інтернету в Росії за будь-яких умов. Про це Соколов сказав у телевізійному виступі з Центру моніторингу та відображення кіберзагроз.

Російський пропагандистський телеканал "Россия-24" повідомив, що влада "тестувала нові технічні можливості" упродовж двох тижнів.

Водночас російські громадські активісти назвали ініційовані владою "навчання" одним із можливих засобів посилення цензури…» ***(У РФ провели "навчання з кібербезпеки", активісти кажуть про цензуру // Espreso.tv (https://espreso.tv/news/2019/12/24/u_rf_provely_quotnavchannya_z_kiberbezpekyquot_aktyvisty_kazhut_pro_cenzuru). 24.12.2019).***

***

**«Президент РФ Владимир Путин на своем ПК пользуется устаревшей операционной системой Windows XP**

Об этом пишет британская газета The Guardian…

"Российских агентов обвиняют в хакерских операциях по всему миру. Но кое-кто в Кремле, очевидно, забыл объяснить Владимиру Путину о важности кибербезопасности", - саркастически отмечают авторы.

Фото, опубликованные пресс-службой Кремля, показали, что на компьютерах в офисе президента России, а также в его резиденции в Ново-Огарево, установлена Windows XP. На всех компьютерах в качестве "заставки" на рабочем столе установлено изображение башен Кремля.

Отмечается, что Microsoft прекратил выпускать обновления безопасности для Windows XP и Office 2003 в апреле 2014 года. Однако, похоже, российские правительственные регуляции не позволили Путину обновиться до последней версии операционной системы. Американская технологическая компания на своем сайте предупреждает, что Windows XP "уязвим перед рисками безопасности и вирусами"…» ***(Спецслужбы забыли просветить: Британская газета поиздевалась над компьютером Путина // DsNews (https://www.dsnews.ua/world/spetssluzhby-zabyli-prosvetit-britanskaya-gazeta-poizdevalas-18122019142300). 18.12.2019).***

***

## Протидія зовнішній кібернетичній агресії

**«Підрозділ британських спецслужб, відповідальний за кібербезпеку, розслідує можливу хакерську атаку, в результаті якої в інтернеті були поширені секретні торговельні документи Британії і США…**

Крім побоювань, що Росія могла знову втрутитися у вибори, розкриття секретних документів викликало питання про безпеку делікатних дискусій між Сполученими Штатами і одним з їхніх найближчих союзників.

Британська опозиційна Лейбористська партія отримала документи, заявивши, що згідно з ними, консерватори прем'єр-міністра Бориса Джонсона замишляли продати частину державної Національної служби охорони здоров'я (NHS) у торговельних переговорах з президентом США Дональдом Трампом.

Джонсон неодноразово заперечував це твердження, тоді як Трамп, який в липні заявив, що NHS буде предметом переговорів, сказав минулого тижня, що він не зацікавлений у медичній службі, навіть якщо вона буде запропонована йому Британією на "срібній таці".

Британський Національний центр кібербезпеки допомагає уряду розслідувати, як документи потрапили в мережу. Він відмовився коментувати розслідування.

Два джерела повідомили, що одна з ліній розслідування полягає в тому, щоб визначити, чи опинилися документи в інтернеті в результаті хакерської атаки…» ***(У Британії розслідують причетність Кремля до витоку секретних даних // Європейська правда (https://www.eurointegration.com.ua/news/2019/12/9/7104005/). 09.12.2019).***

***

**«…Дослідники Google дійшли висновку, що на початку березня 2017 року перед першим туром виборів президента Франції дві хакерські групи почали розробку операції зі злому штабу Макрона. Згідно з дослідженнями, в атаці винні групи APT28 (Fancy Bear) і Sandworm…**

Група APT28 відома з розслідування спецпрокурора США Роберта Мюллера, за даними якого вона пов'язана з підрозділом 26165 ГРУ РФ.

Sandworm спеціалізується на участі в операціях з високим ризиком в умовах обмежених часових рамок, її пов'язують з підрозділом ГРУ 74455, який часто працює з підрозділом 26165.

На думку журналістів Le Monde, замовник атаки, під час якої випливло багато інформації, зокрема, офіційних листів і документів, звернувся спочатку до APT28. Потім він вирішив "перестрахуватися" і підключив до роботи Sandworm.Ф…» ***(Google знайшов докази причетності російських хакерів до злому пошти Макрона в 2017 році // iPress (https://ipress.ua/news/google_znayshov_dokazy_prychetnosti_rosiyskyh_hakeriv_do_zlomu_poshty_makrona_v_2017_rotsi_304051.html). 08.12.2019).***

***

**«На Дніпропетровщині Служба безпеки України блокувала діяльність хакерського угруповання, організованого спецслужбами РФ для проведення кібератак на українські державні органи.**

Оперативники та слідчі спецслужби встановили, що група місцевих мешканців розробляли на замовлення російських кураторів програмне забезпечення, для ураження комп’ютерів та отримання прихованого віддаленого доступу до інформації, що на них зберігається.

Фахівці Служби з кібербезпеки також встановили, що учасники ліквідованого хакерського угрупування причетні до масштабної кібератаки на обласні державні адміністрації, яка була проведена в липні 2019 року. Зловмисники здійснювали масштабні розсилки електронних листів із комп'ютерними вірусами. Проведення акції кібершпигунства співпало з призначенням нових керівників обласних адміністрацій та підготовкою до проведення виборів до Верховної Ради України. Спеціалісти СБУ тоді блокували цю спробу хакерської атаки.

За розробку та збут програмного забезпечення, призначеного для негласного отримання інформації, слідчі спецслужби оголосили про підозру одному з учасників хакерського угруповання. Матеріали документування злочину скеровано до суду.

Наразі вживаються заходи із встановлення всіх учасників хакерського угруповання та їх російських кураторів…» ***(Банду підконтрольних ФСБ хакерів знешкодила СБУ на Дніпропетровщині // Магнолія-ТВ (https://magnolia-tv.com/news/26060-bandu-pidkontrolnikh-fsb-khakeriv-zneshkodila-sbu-na-dnipropetrovschini?prov=ukrnet). 06.12.2019).***

***

**«Міністерство США ввело санкції стосовно кількох росіян і 7 російських компаній, пов'язаних з кібербезпекою…**

В список організацій увійшли «Бізнес-Столиця», Evil Corp (Dridex Gang), «Оптима», «Трейд-Інвест», «ЦАО», «Вертикаль», «Юніком».

Обмеження також введені відносно 17 осіб, серед яких Максим Якубець та Ігор Турашев. Вони звинувачуються в шахрайстві з комп'ютерним програмним забезпеченням.

У повідомленні відомства говориться, що діяльність Evil Corp призвела до збитку понад 100 мільйонів доларів, від її дій постраждали фінансові організації 40 країн. Її власника Максима Якубца заарештували заочно. За інформацію, яка приведе до його арешту, влада США призначили нагороду в п'ять мільйонів доларів…» ***(США ввели нові санкції проти РФ: у списку – компанії, пов'язані з кібербезпекою // Чорноморські новини (https://www.blackseanews.net/read/158488). 06.12.2019).***

***

**«У НАТО вважають, що дії Росії становлять одну з головних загроз для Північноатлантичного альянсу.**

Про це йдеться в заяві НАТО, ухваленій за підсумками саміту, що відбувся у Лондоні 3-4 грудня.

«Ми стикаємося з виразними загрозами та викликами, що виходять з усіх стратегічних напрямів. Агресивні дії Росії загрожують євроатлантичній безпеці», — йдеться в документі. Серед загроз також названо тероризм та кібератаки.

Окремо згадується зростаючий вплив Китаю… За словами генсека НАТО Єнса Столтенберга, союзники по НАТО погодилися з необхідністю включити Китай в нову майбутню угоду про контроль над озброєннями. «Зараз ми почали обговорювати, яким чином ми можемо підключити Китай до домовленостей з контролю над озброєннями в майбутньому», — наголосив Столтенберг…» ***(Дії***

***Росії є загрозою для НАТО // Голос України (http://www.golos.com.ua/article/324976). 06.12.2019).***

***

**«НАТО визнає зростання впливу Китаю та вважає, що його міжнародна політика несе як можливості, так і виклики.**

…про це йдеться у лондонській декларації, ухваленій лідерами за підсумками дводенної зустрічі.

"Ми визнаємо, що зростаючий вплив та міжнародна політика Китаю несуть як можливості, так і виклики, які нам потрібно приймати разом як Альянсу", - сказано в документі.

Щоб залишатися в безпеці, "ми повинні дивитись у майбутнє разом", заявляють лідери НАТО. "Ми звертаємось до широти та масштабів нових технологій, щоб підтримувати свої технологічні переваги, зберігаючи наші цінності та норми. Ми будемо продовжувати підвищувати стійкість наших суспільств, а також критичної інфраструктури та енергетичної безпеки. НАТО та союзники в межах своїх відповідних повноважень зобов'язані гарантувати безпеку наших комунікацій, зокрема 5G, визнаючи необхідність покладатися на безпечні та стійкі системи", - йдеться в заяві.

НАТО оголосило космос оперативною сферою, "визнаючи його важливість у безпеці та врегулюванні проблем безпеки, дотримуючись міжнародного права".

"Ми розширюємо наші інструменти для реагування на кібератаки та зміцнюємо нашу здатність до готовності, стримування та захисту від гібридних тактик, які прагнуть підірвати нашу безпеку та суспільство. Ми посилюємо роль НАТО в безпеці людини", - зазначається в лондонській декларації…» ***(Зростання впливу Китаю несе як можливості, так і виклики - лідери НАТО // Європейська правда (https://www.eurointegration.com.ua/news/2019/12/4/7103841/). 04.12.2019).***

***

**«Расследование спецпрокурора Мюллера под кодовым названием «Crossfire Hurricane» («Шквальный огонь») началось в июле 2016 года. Американские спецслужбы утверждают, что Россия совершала кибер-атаки на различные политические организации США.**

В течение весны и начала лета 2016 года ФБР стало известно о конкретных кибер-вторжениях, за которые несут ответственность российские власти. Эти данные подтвердились в результате расследования, проведённого кибер-отделом ФБР совместно с отделом контрразведки ФБР, — говорится в докладе.

Также уточняется, что фишинговая компания проводилась со стороны Главного управления Генерального штаба ВС РФ, более известного как Главное разведывательное управление (ГРУ). Американские спецслужбы утверждают, что с марта по август 2016 года Россия совершала многочисленные попытки взломать государственные избирательные системы. ФБР получило информацию о разговоре между советником Дональда Трампа Джорджем Пападопулосом и послом Австралии в Великобритании в мае 2016 года. Тогда он рассказал, что «команда Трампа получила предложение из России», чтобы раскрыть информацию, которая будет разрушительной для Хиллари Клинтон и Барака Обамы. В докладе отмечают,

что ФБР начало расследование по данному факту спустя три дня после получения этой информации.

1 августа 2016 года агент ФБР по вопросам контрразведки Питер Стржок и специальный агент по надзору отправились в Европу, чтобы поговорить с чиновниками, с которыми Пападопулос обсуждал «предложение России» в мае 2016 года. Они сообщили, что советник Трампа не говорил о наличии прямого контакта с русскими. Стржок выяснил, что Пападопулус не указал никаких других лиц, которые получили русское предложение…» ***(Минюст США обнародовал доклад о вмешательстве России в американские выборы // Новости Великобритании на русском языке (https://theuk.one/minyust-ssha-obnarodoval-doklad-o-vmeshatelstve-rossii-v-amerikanskie-vybory/). 09.12.2019).***

***

**«Кандидат в депутаты от Лейбористской партии Бен Брэдшоу заявил, что он стал жертвой предполагаемой российской кибератаки после того, как он получил электронное письмо «из Москвы» с вложениями, содержащими вредоносные программы…**

Брэдшоу ранее неоднократно поднимал вопрос о вмешательстве Кремля в британскую политику, в том числе Brexit. Он получил письмо на свою электронную почту. Отправитель — «Андрей» — утверждал, что был разоблачителем из администрации Владимира Путина. В письме было несколько явно подлинных документов, которые показали, как Кремль создал секретное «поддельное информационное подразделение» в дальневосточном регионе России, которое используется для подавления негативных историй и усиления проправительственных настроений. Однако два документа содержали вредоносный код. Сначала Брэдшоу отправил электронное письмо экспертам по кибербезопасности, которые подтвердили, что файлы были подозрительными. Затем он сообщил об этом электронном письме в Национальный центр кибербезопасности (NCSC) — часть Центра правительственной связи Великобритании, и в парламент. NCSC подтвердил, что рассматривает дело во вторник. В настоящее время эксперты изучают полученную информацию. По словам специалистов британской разведки, атака была технически сложной и специально предназначенной для предполагаемого кандидата от лейбористской партии. Эти файлы включают в себя подпись действительного регионального представителя на бумаге президента и подробный слайд PowerPoint на русском языке с акциями протеста, «по-видимому, составленный российским ФСБ». Брэдшоу отметил, что письмо пришло на его личный аккаунт Gmail, который более уязвим, чем его парламентский. Та информация, о которой писал отправитель, была потенциально чрезвычайно полезной и могла оказаться «политическим динамитом».

Политик также напомнил, что был первым депутатом, который поднял вопрос о роли России ву референбуме по Brexit, и с тех пор постоянно говорил о том, что Кремль пытается подорвать политический строй в Великобритании. При этом письмо было написано на хорошем английском языке, с несколькими переведенными оригинальными русскими документами. Оно было отправлено с анонимного аккаунта с использованием ProtonMail — зашифрованной электронной

почты. Отправитель «Андрей» сказал, что хотел бы раскрыть подробности пилотного проекта по пропаганде, потому что подобные «фальшивые новостные практики» использовались «с Brexit и США» в 2016 году, и дал ссылку на операцию Кремля в социальных сетях в поддержку Brexit и Дональда Трампа. «Моя мотивация для связи с вами заключается в том, что я лично возражаю против методов, которые используют мои начальники в администрации президента России… Они ценят текущее состояние дел, которое позволяет им хранить деньги в Великобритании, так что разоблачение может создать сильную правильную реакцию в Москве», — писал «Андрей». Отправитель сказал, что его документы могут стать «политическим капиталом» для лейбористов перед выборами, «особенно с учетом последних статей о консерваторах, работающих с деньгами России». Схожее письмо получила организация Bellingcat, рассказал один из ее исследователей Арик Толер. Он отметил, что он и его коллеги не открывали ни одно из вложений.» ***(Британский политик и Bellingcat получили вредоносные письма. Их автор представился «разоблачителем из администрации Путина» // Новости Великобритании на русском языке (https://theuk.one/britanskij-politik-i-bellingcat-poluchili-vredonosnye-pisma-ix-avtor-predstavilsya-razoblachitelem-iz-administracii-putina/). 04.12.2019).***

***

**«В Великобритании нашли еще один повод обвинить "российских хакеров" в кибератаках. На этот раз Центр правительственной связи Соединенного королевства расследует возможную причастность "киберпреступников" к утечке документов британского министерства международной торговли.**

…секретариат кабмина обратился к представителям GCHQ, которая отвечает за защиту информации органов правительства с просьбой выявить источник утечки документов. Расследование должно дать понять, есть ли ответственность за эти атаки у хакеров, "поддерживаемых государством". Кроме того, специалисты должны узнать, принимали ли участие в этом британские госслужащие.

До этого на сайте Reddit, а также трех интернет-порталах на немецком языке и одном Twitter-аккаунте были опубликованы документы британского министерства. В них шла речь о переговорах Лондона и Вашингтона по торговле.» ***(В Британии расследуют "причастность РФ" к утечке документов правительства // Новости Великобритании на русском языке (https://theuk.one/v-britanii-rassleduyut-prichastnost-rf-k-utechke-dokumentov-pravitelstva/). 08.12.2019).***

***

**«Користування соцмережею коротких роликів TikTok на мобільних пристроях, виданих урядом, нібито становить «загрозу кібербезпеці»…**

Зазначається, що керівництво Військово-морських сил США повідомило про блокування доступу до внутрішньої мережі морського корпусу ВМС для тих пристроїв, які не видалили TikTok.

У ВМС не уточнювали, яку саме загрозу становить мобільний додаток, проте речник Пентагону зазначив, що рішення має на меті «подолати чинні та можливі подальші загрози».

У TikTok наразі не прокоментували заборону.

Відеосервіс TikTok користується величезною популярністю серед американських підлітків, але в останні місяці він перебуває під ретельним наглядом американських регуляторів та законодавців. Сенатори Чак Шумер та Том Коттон написали листа американським розвідникам із проханням розслідувати TikTok, який належить китайській компанії ByteDance. Вони висловили занепокоєння можливими загрозами національній безпеці з боку платформи…». ***(У США військовим заборонили користуватися соцмережею TikTok на службових гаджетах // MediaSapiens (https://ms.detector.media/web/cybersecurity/u_ssha_viyskovim_zaboronili_koristuvatisya_sotsmerezheyu_tiktok_na_sluzhbovikh_gadzhetakh/). 21.12.2019).***

***

**«В связи с новой утечкой информации Wikileaks опубликует меморандум, в котором говорится, что 20 инспекторов уверены, что версия «не отражает взгляды членов команды, находящихся в Сирии».** Так, в документах идет речь о том, что один из фельдшеров миссии фактически представил окончательный вариант доклада ОЗХО…

Помимо него, весь доклад ОЗХО собирала совершенно новая команда, которая даже не посещала предполагаемый участок, где сообщалось об атаки с применением химического оружия. «Эта новая команда была укомплектована людьми, которые «работали только в стране Х», - говорится в меморандуме. Неясно, о какой стране идет речь. Понятно, что это, вероятно, не Сирия. Возможно, хотя это только предположения, что «страна Х» — это Турции. ОЗХО направила туда группы в лагери беженцев, чтобы опросить выживших из Думы.

Автор меморандума заявляет, что именно ему первоначально поручили провести анализ и оценку двух баллонов, обнаруженных на месте предполагаемой химической атаки. Это была задача, которую он взял на себя, понимая, что был явно самым квалифицированным членом команды, находясь в Думе и благодаря его опыту в металлургии, химическом машиностроении (включая проектирование сосудов под давлением), артиллерии и обороны.

«В последующие недели я обнаружил, что меня исключают из работы по непонятным причинам», — сказал он. Автор объясняет, что он часто просил предоставить ему обновленную информацию о ходе работы над окончательным докладом и разрешить ему рассмотреть проект, но ему было отказано по обоим пунктам. Ответ был: «совершенно секретно». ОЗХО еще не выпустила комментарий относительно этих последних утечек информации». ***(Wikileaks опубликует новую порцию утечки из ОЗХО. На этот раз о фейковой химатаке в Сирии // SecureNews (https://securenews.ru/wikileaksopublicuet-novuyu-utechcu/). 16.12.2019).***

***

**«Попри постійну російську пропаганду в Естонії навчилися їй протидіяти. В цій країні створили спеціальні кібервійська, які захищають урядові сайти від хакерських атак. А своїх громадян там вчать виявляти фейки, щоб не потрапити на російський гачок.**

В Естонії, як і в багатьох колишніх республіках СРСР залишилась велика російська громада. Нерідко тут виникають міжетнічні тертя які підігріває роспропаганда. Та на відміну від України чи тієї ж сусідньої Латвії тут російські канали чи соцмережі не блокують.

На думку президента Естонії владі вдалось отримати лояльність неестонського населення завдяки почуттю безпеки та комфорту. Оскільки рівень життя в Естонії найвищий серед пострадянських країн.

Та незадоволених росіян навіть у ситому Таллінні знайти неважко. У 2007 році Естонією прокотились масові протести та сутички за участі російської молоді. Вони були обурені перенесенням із центру Таллінна пам'ятника радянським солдатам.

Одна людина загинула, сотні отримали поранення, більше тисячі було заарештовано. В історію ті дні увійшли як Бронзова ніч. Протести підтримувала Москва. Діяла їхня пропаганда та хакери, які організовували атаки на естонські урядові сайти. Через соцмережі людей підбурювали до протестів.

Після цих трагічних подій при Міністерстві оборони Естонії були створені кібервійська. Також були значно вдосконалені урядові сайти та система моніторингу, щоб заздалегідь виявляти небезпеку і вчити громадян як правильно користуватись інтернетом аби не потрапити на гачок.

Вміти відрізнити брехню від правди та чесність від маніпуляції навчають сусідів естонців – фінів мало не з пелюшок. Фінляндія – один із технологічних лідерів у світі. Її компанії є об'єктами комерційного шпигунства, а на державні органи регулярно проводяться кібератаки. За даними місцевої розвідки найбільша загроза походить від Китаю та сусідньої Росії.

Основним полем бою стали соцмережі і псевдоновинні сайти, які поширювали фейкову інформацію про мігрантів зі сходу які нібито захоплюють Європу. Завдання – посіяти напругу, розбрат та істерію довкола гарячої теми.

Хоч фейкові новини і боти сіють напругу, але на фінське суспільство вони мають обмежений вплив. На останніх виборах популісти, яким накручували популярність фейки, так і залишились опозицією.

Можливість застосувати фінський та естонський досвід боротьби з дезінформацією та кіберзлочинністю в інших пострадянських країнах обговорювали зокрема на медіаконференції, яка пройшла днями в Гельсінкі.

Захід, який був організований за підтримки Єврокомісії, зібрав учасників з країн Східного партнерства – зокрема й України.

Один зі спікерів форуму керівник організації СтопФейк Євген Федченко каже, що Україну не раз занижували у рейтингу свободи слова через блокування російських ЗМІ. Але в умовах війни це найдієвіший спосіб боротьби із пропагандою.

Медіаграмотність як в Естонії чи Фінляндії в Україні вже викладають в кількох школах, але це довгострокова перспектива.

Кількість брехливої інформації за підрахунками експертів зростає з року в рік. Лише у соцмережі Twitter російська фабрика тролів наплодила від початку війни з Україною понад 10 млн фейків. У цьому морі брехні годі загубитись і медіаграмотній людині». ***(Як не потрапити на гачок пропаганди Кремля – досвід Естонії та Фінляндії // ФАКТИ. ICTV (https://fakty.com.ua/ua/svit/20191224-yak-ne-potrapyty-na-gachok-propagandy-kremlya-dosvid-estoniyi-ta-finlyandiyi/). 24.12.2019).***

***

**«Глава МЗС Нідерландів Стеф Блок заявив, що попри спроби Росії грати проти держав-членів ЄС, її відхід від міжнародного правопорядку, з Москвою необхідно підтримувати діалог.**

Про це він заявив у викладеній у листі стратегії щодо Росії, представленій парламенту у відповідь на запит депутатів…

У листі міністр вказує, що Росія навмисно поширює дезінформацію і здійснює кібератаки. "У Росії є наступальна кіберпрограма" – зазначив Блок.

Він наводить як приклади дезінформації про катастрофу МН17 і спробу злому організації по забороні хімічної зброї (ОЗХЗ) в Гаазі.

"Стратегічне значення голландської політики і правосуддя значно зросло для Росії після рішення Нідерландів та Австралії притягнути РФ до відповідальності за її участь у збитті рейсу МН17", - заявив Блок.

Але загроза, за його словами, не тільки цифрова. "Росія продовжувала в останні роки вкладати значні кошти у військовий потенціал і стримування. Зокрема, в європейській частині Росії звичайні і ядерні сили значно покращилися як в кількісному, так і в якісному відношенні", – зазначив Блок.

На думку міністра, російська "напористість" означає, що ситуація з безпекою в Європейському Союзі стала менш передбачуваною, менш стабільною і менш безпечною.

Блок також стурбований ситуацією в самій Росії. За його словами, держава ще більше зміцнила свій вплив на політику, ЗМІ та суспільство. "У результаті ситуація з правами людини в останні роки, в тому числі в окупованому Криму, погіршилася" – йдеться у листі.

Незважаючи ні на що, міністр виступає за продовження дискусій з Росією і спільної роботи, зокрема, в економічній сфері.

"Якщо Росія перетне наші кордони, Нідерланди, наскільки це можливо в міжнародному контексті, займуть позицію і будуть діяти відповідним чином", - заявив Блок.

"Водночас Росія є важливим геостратегічним гравцем на європейському континенті. Саме тому вкрай важливо продовжувати розмову з Росією", – вважає він». ***(Глава МЗС Нідерландів виклав стратегію щодо РФ: з Москвою потрібен діалог // Європейська правда (https://www.eurointegration.com.ua/news/2019/12/23/7104550/). 23.12.2019).***

***

**«Громадський мовник Іспанії показав інтерв'ю з каталонським лідером сепаратистів Карлесом Пучдемоном після того, як хакери зламали його канал новин і замінили контент на відео російського державного мовника RT…**

В інтерв'ю Пучдемон знову наполягав на тому, що "каталонську проблему не врегулювати без надання незалежності".

Бос RT Маргарита Симоньян сказала, що її мережа не несе відповідальності.

"Хакери проникли в іспанський канал +24 і переключили передачу на нашу", - сказала вона.

"Ми закінчили інтерв'ю з Пучдемоном. Наша передача тривала цілий вечір. Ми не знаємо, хто це зробив, але це було красиво", - зазначила вона…». ***(Іспанський канал після кібератаки показав російське інтерв'ю з Пучдемоном // Європейська правда (https://www.eurointegration.com.ua/news/2019/12/18/7104369/). 18.12.2019).***

***

**«Британські та американські кіберрозвідники ідентифікували особи двох російських хакерів, які завдали серйозної шкоди як США, так і Великій Британії.**

За їх видачу Сполучені Штати призначили рекордну суму винагороди – 5 мільйонів доларів. Цікаво, що самі хакери нікуди не ховаються: вони перебувають в Росії під захистом Кремля, з яким чи то співпрацюють, а чи то просто є офіційними російськими службовцями.

Група, яка має назву Evil Corp. та позначається американськими офіційними установами, як "найнебезпечніша хакерська група світу", протягом свого доволі недовгого існування встигла завдати шкоди на сотні мільйонів доларів. Вона складається з російських хакерів, які дивним чином мають суперсучасне обладнання – таке, як зазначають фахівці з кібероборони, яке можуть дозволити собі хіба що офіційні розвідницькі підрозділи. Група спеціалізується на економічних кіберзлочинах – лише в США шкода від її діяльності вимірюється не менш, ніж 100 мільйонами доларів.

Тепер американським слідчим, здається, вдалося завдати принаймні одного удару у відповідь: вони ідентифікували щонайменше двох керівників Evil Corp., а також кількох хакерів з цієї групи. Вони виявилися росіянами. Всі перебувають на території Росії й, таким чином, залишаються недоступними для американського судочинства.

За даними британського Національного агентства з криміналістики (NCA), Evil Corp. несе відповідальність за численні кібератаки по всьому світу. У Великій Британії шкода від їх діяльності вимірюється сотнями мільйонів фунтів стерлінгів. Окрім того, грабуючи фірми та корпорації, банда не гребувала й приватними заощадженнями "маленьких людей", поцупивши в приватних персон десятки мільйонів доларів – про це офіційно заявило Міністерство юстиції США. Загалом, ця команда залишила свій слід в 40 країнах світу.

Тепер грошова винагорода призначена за самих хакерів – звичайно, це не така велика сума, яку награбували собі кібербандити, але у світовому порівнянні – наразі рекордна: 5 мільйонів доларів не призначали ще за жодного хакера. Окрім того, уряд США запровадив санкції проти компаній (знову ж таки – переважно

російських), які доведеним чином співпрацювали або співпрацюють із Evil Corp., а також проти 17 осіб, які вважаються членами цього угрупування або пов'язані з ним. 5 мільйонів же, про які йдеться – це винагорода за надання інформації або за передачу американським офіційним установам двох осіб, які вважаються керівниками банди – Максима Якубця та Ігоря Турашева.

Міністр фінансів США Стівен Мнучін заявив:

Ця скоординована акція спрямована на те, щоб зупинити розпочату цією російською групою хакерів масивну кампанію фішингу (незаконного отримання приватної інформації з перехоплених емейлів – 24 канал).

Робота американських слідчих ускладнюється тим, що лідер Evil Corp. Максим Якубець доведеним чином є співробітником російських офіційних установ – зазначається в урядовому повідомленні США. Звинувачуваний ще в 2018 році був ідентифікований, як офіцер ФСБ, який навіть має доступ до секретної інформації. Збиранням приватних даних осіб та компаній він займається на завдання ФСБ, як "державний хакер". За словами Стівена Мнучіна, американським установам відомі конкретні завдання, які були дані Якубцю, але їх суть міністр фінансів не розкривав.

Загалом же, за даними американців, Якубець діє, як хакер на завдання російського уряду, з 2017 року, а команда Evil Corp. "прославилася" ще в 2015, коли почала розсилати по всьому світові через емейли "троянський" вірус Dridex. Він таємно встановлював на заражені комп'ютери так звані Malware – тобто, шкідливі програми, які автоматично копіювали та надсилали своїм розробникам приватну інформацію: номери та паролі банківських рахунків, номери та коди кредитних карток тощо. Після отримання цієї інформації, хакери, звичайно, просто грабували відповідні рахунки, перекидаючи звідти гроші до власних "електронних кишень". Британські установи недарма назвали Evil Corp. "найшкідливішою у світі групою кіберзлочинців" – вона вкрала більше грошей, ніж будь-яка інша подібна банда.

За даними слідства, Evil Corp. діє переважним чином з Москви, причому Якубець є керівником групи, а Турашев – адміністратором. Обидва злочинці, за інформацією NCA, так і живуть в російській столиці й "отримати" їх звідти офіційним чином нема жодної можливості – як пояснюють британці, "через відсутність угоди про видачу між США/ЄС та Росією". Насправді, скоріш за все, якби навіть така угода й існувала – навряд чи ФСБ просто так взяла та видала власних співробітників, скільки б грошей вони не накрали та якої б шкоди не завдали. Але, скажімо, літати за кордон у відпустку їм тепер, м'яко кажучи, не рекомендовано». ***(Борис Немировський. Хакери Путіна: хто вони та чому США обіцяє за них п'ять мільйонів доларів // Телеканал новин «24» (https://24tv.ua/hakeri_putina_hto_voni_ta_chomu_ssha_obitsyaye_za_nih_pyat_milyoniv_dolariv_n1250238). 17.12.2019).***

***

**«На цьому тижні відбулася кібератака на співробітників державних установ Латвії. Кіберзлочинці розсилали електронні листи від імені Посольства Росії…**

"…низка державних чиновників та політиків протягом останніх днів зазнавали цілеспрямованих кібератак. Атака була здійснена шляхом надсилання шкідливих електронних листів від імені посольства Росії у відповідь на попередню кореспонденцію. Електронні листи містили посилання для завантаження документа, призначеного для зараження комп'ютера жертв", - йдеться у повідомленні.

Так, усі одержувачі електронної пошти розпізнавали фрагменти попередньої кореспонденції з посольством, які використовувались для підвищення довіри адресату, до листа надісланого зловмисниками.

Зазначається, що це вже друга хвиля подібних атак за останні 3 місяці, коли від імені посольства Росії надсилаються шкідливі електронні листи.

У рамках цієї атаки не використовували критичних уразливостей системи, проте завантажені документи містили функціонал Macros, що і мав заразити комп'ютер.

Координаційний центр застерігає від відкриття листів та скачування документів без попередньої перевірки…». ***(Наталія Рябцева. Кіберзлочинці розсилали держустановам Латвії заражені листи від імені посольства РФ // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1841235-kiberzlochintsi-rozsilali-derzhustanovam-zarazheni-listi-vid-imeni-posolstva-rf). 13.12.2019).***

***

**«Соединенные Штаты Америки готовят специальную операцию против российской политической и экономической элиты в случае ее вмешательства в проведение выборов президента США осенью 2020 года.** При этом, президента РФ Владимира Путина эта операция не затронет, поскольку такие меры будут считаться "слишком провокационными"…

Отмечается, что правительство США приступило к подготовке операции после того, как разведка предоставила в ноябре секретный доклад, согласно которому "Россия при помощи хакеров попытается сеять разногласия среди американцев и намеренно обострять существующие противоречия в обществе".

Некоторые меры киберкомандование США уже приняло в отношении так называемых троллей, которые действовали в соцсетях от имени американских граждан. В Вашингтоне убеждены, что действуют они по заданию Агентства интернет-исследований РФ.

…речь может пойти о получении доступа и использовании конфиденциальной информации о представителях руководства РФ. Еще один способ информационной операции - поиск разногласий между людьми из российской элиты…». ***(В США готовят операцию на случай кибератаки России в ходе президентских выборов // Зеркало недели. Украина (https://zn.ua/WORLD/v-ssha-gotovyat-operaciyu-protiv-rosii-v-sluchae-kiberataki-v-hode-prezidentskih-vyborov-340441_.html). 26.12.2019).***

***

**«США, Канада, Німеччина, Франція, Велика Британія, Україна виступили проти нової резолюції ООН по кібербезпеці.** У цих країнах вважають,

що нова резолюція ООН узаконить репресивні методи боротьби проти інакомислення і сприятиме запровадженню цензури в інтернеті, передає ONLINE.UA з посиланням на DW.

Критики нової резолюції ООН впевнені, що документ являє загрозу свободі висловлювань в інтернеті. У представництві США при ООН, зокрема, заявили, що прийнята резолюція може "підірвати міжнародне співробітництво з метою боротьби проти кіберзлочинності за часів, коли необхідно зміцнення координації".

У міжнародній правозахисній організації Human Rights Watch підкреслили, що авторами резолюції виступили країни, уряди яких вдаються до репресивних методів боротьби проти інакомислення. Там переконані, що даний документ дозволить країнам відключати інтернет і цензуру під легальним прикриттям, і при цьому створить можливість для криміналізації свободи слова…» ***(У США і ЄС раптово виступили проти нової резолюції ООН // ONLINE.UA (https://novyny.online.ua/815759/u-ssha-i-es-raptovo-vistupili-proti-novoyi-rezolyutsiyi-oon/). 29.12.2019).***

***

**«Киберэксперты рассказали, что новая "холодная война" начнется в 2020 году.** Об этом сообщают зарубежные СМИ со ссылкой на исследование IT-компания Check Point…

Отмечается, что "холодная война" будет происходить в интернет среде.

"Новая холодная война произойдет в онлайн-мире. Кибератаки будут все чаще использоваться в качестве косвенных конфликтов между небольшими странами", — заявляется в сообщении.

Уточняется, что финансирование этим странам будут предоставлять крупные государства, которые стремятся "консолидировать и расширять свои сферы влияния".

Также прогнозируется рост кибератак на критически важные инфраструктуры, например коммунальные, поскольку в этих сферах используются устаревшие технологии. Кроме того, ожидается увеличение атак на конкретные предприятия, органы власти и организации сферы здравоохранения.» ***(О новой "холодной войне" рассказали киберэксперты // Багнет (http://www.bagnet.org/news/tech/415070/o-novoy-holodnoy-voyne-rasskazali-kibereksperty). 28.12.2019).***

***

## *Створення та функціонування кібервійськ*

---

**«В Эстонии на базе Академии Сил обороны (Тарту) стартовали масштабные киберучения НАТО Cyber Coalition, в которых участвуют представители 27-ми из 29-ти стран НАТО, а также 6 партнеров Альянса — Япония, Алжир, Австрия, Финляндия, Ирландия и Швеция. Учения будут проходить до 6 декабря…**

В Тарту на базе Академии Сил обороны начались масштабные киберучения НАТО. Учения Cyber Coalition проводятся в Эстонии в седьмой раз.

Страны-участницы представят почти 700 специалистов по кибербезопасности, технологов, военных и правительственных чиновников, представителей бизнеса.

Во время учений будет разыгрываться приближенный к реальности сценарий кибератаки, чтобы в тесной координации друг с другом участники предотвратили ее воздействие на жизненно важные системы государства, а также отработали взаимодействие экспертов на внутригосударственном и международном уровнях…» ***(В Эстонии стартовали масштабные киберучения НАТО // journalist (https://journalist.today/v-jestonii-startovali-masshtabnye-kiberuchenija-nato/). 03.12.2019).***

***

**«По словам военных, Армия обороны Израиля в среду начала неожиданные учения по киберзащите, имитирующие последствия атаки, заблокировавшей критически важные компьютерные системы.**

Это уже третья неожиданная проверка готовности военных с тех пор, как почти год назад на должность начальника штаба ЦАХАЛа заступил Авив Кохави (Aviv Kohavi). "Во время учений сотни командных и контрольных компьютерных станций были отключены в подразделениях ЦАХАЛа", - сказали военные.

В ЦАХАЛе заявили, что учение предназначалось для проверки "функционирования армии во время кибератаки и отключения жизненно важных информационных систем". Хотя конкретный враг не был указан, предполагается, что им является Иран и его марионетки, которые работают над созданием передовых возможностей для прорыва заслона кибербезопасности.» ***(ЦАХАЛ провел учения по защите от кибератак // ISRAland Online Ltd (http://www.isra.com/news/239050). 18.12.2019).***

***

## Захист персональних даних

**«Нещодавно журналіст та фахівець з кібербезпеки Брайан Кребс повідомив, що нові iPhone 11 Pro збирають дані про розташування, навіть коли всі дозволи вимкнені…**

За заявою Apple, "винуватцем" появи іконки геолокації на екрані смартфонів стала нова технологія ультраширокополосної передачі даних (UWB), яка з'явилася в нових моделях iPhone…

Її застосування регламентується міжнародними вимогами, які вимагають відключати цю функцію в місцях, де робота такого обладнання заборонена. Представники компанії стверджують, що iOS іноді визначає місцеположення лише для того, щоб дотримуватися цієї вимоги. При цьому дані про місцезнаходження обробляються на самому пристрої і не передаються Apple.

У нових iPhone використовується чіп U1, що дозволяє швидко обмінюватися даними з сумісними пристроями на близькій відстані без використання супутників, вишок мобільного зв'язку та іншого обладнання за допомогою функції AirDrop. Очікується, що в майбутньому UWB також буде використовуватися спільно з «маячками» Apple Tag, які призначені для пошуку невеликих втрачених об'єктів…

За наявною інформацією, в одному з майбутніх оновлень Apple додасть в iOS окремий вимикач для UWB, хоча такий крок може викликати труднощі, якщо буде заважати міжнародним нормативним вимогам.

В якості тимчасового рішення користувачам пропонується повністю відключити служби геолокації в меню налаштувань. Це, на відміну від ручного вимикання GPS для різних додатків, деактивує функцію збору даних чіпом U1.» ***(Apple відповіла на чергові звинувачення у шпигунстві // Телеканал новин «24» (https://24tv.ua/techno/techno/apple_vidpovila_na_chergovi_zvinuvachennya_u_shpionazhi_n1245102). 06.12.2019).***

***

**«Тайна личной переписки в мессенджерах сегодня очень актуальна для любого пользователя интернета…**

Мессенджер Telegram был запущен в 2013 году. Его разработчиком стали Павел и Николай Дуровы. Но глобальная популярность к мессенджеру пришла несколько позже, когда у него начались проблемы с российским Роскомнадзором. Именно он много раз пытался заблокировать сервера, используемые Telegram для работы и шифрования, передаваемых пользователями данных. Как показала практика, это привело лишь к небольшим перебоям в работе мессенджера, но на сегодняшний день он полностью стабилен, и что самое главное для многих пользователей, независим от контролирующих правительственных органов.

В Telegram используется собственный уникальный протокол шифрования MTProto. Его особенностью является совмещение сразу нескольких технологий кибербезопасности. Предусмотрено не только симметричное (с одним ключом) шифрование AES с размерами блоков 256 бит, но и дополнительное асимметричное 2048-битное шифрование RSA. Это позволяет передавать по открытому протоколу только публичные ключи. То есть, вся информация расшифровывается непосредственно уже на гаджете пользователя. Сквозное шифрование (end-to-end encryption) считается сегодня самым защищенным.

Но важно понимать, что максимум безопасными в Telegram являются только секретные чаты. Обычные переписки передаются через стандартный сервер. Поэтому в теории их можно перехватить и без особого труда расшифровать. Согласно утверждениям разработчиков, это необходимо для резервного копирования в облако, чтобы пользователь мог получить доступ к своим перепискам с любого своего гаджета.

Еще одним преимуществом секретных чатов является блокировка скриншотов в них. Таким образом, ваш собеседник не сможет оставить себе вашу переписку в виде изображений и после завершения беседы она будет попросту удалена.» ***(Насколько безопасен мессенджер Telegram? // RUpor.info (https://www.rupor.info/news/153516/naskolko-bezopasen-messendzher-telegram). 11.12.2019).***

***

**«Недавно на официальном сайте ФБР появилась информация о том, что через камеры современных «умных» телевизоров возможно следить за человеком.** В частности, предупреждение было направлено на граждан США, но вряд ли кого-то остановят территориальные рамки в этих условиях.

Главная опасность Smart-TV заключается в том, что они подобно ноутбукам и телефонам подключаются к локальной сети и имеют доступ в интернет. Таким образом, как и с любым устройством, при определенных навыках и умениях можно установить связь, и получить доступ к камере и микрофону. Соответственно хакеры смогут увидеть и услышать все, что происходит в доме.

Как правило, подобные способы вторгаться в чужую личную жизнь, осуществляют с целью наживы. Узнать персональную информацию, номера банковских счетов, коды, пароли и другие конфиденциальные данные.

Кроме того, могут установить личное наблюдение за жителями помещения, а как правило, телевизоры устанавливают в трех местах: кухне, гостиной и спальне. Самое безобидное, что могут сделать хакеры, так это удалить список каналов или открыть доступ детям для видео +18.

В связи с этим, ФБР настоятельно рекомендует особо не рассчитывать на заводские настройки и операционную систему техники. Камеру, если такова имеется, стоит заклеить непрозрачным скотчем…» ***(Дарья Марченко. ФБР предупредило: следить за человеком могут даже через экран телевизора // Hyser Media (https://hyser.com.ua/tehnology/121627-fbr-predupredilo-sledit-za-chelovekom-mogut-dazhe-cherez-ekran-televizora). 11.12.2019).***

***

**«…Операторы попросили законодательно запретить использование данных их абонентов теми компаниями, которые будут поставлять специальное оборудование для исполнения закона «о суверенном интернете». Это обсуждалось в конце ноября текущего года в Совете Федерации…**

Один из источников рассказал, что сейчас сохранность данных, обрабатываемых в рамках закона, законодательно не защищена, поэтому компании, получившие доступ к данным, могут использовать их в коммерческих целях.

Представители Минкомсвязи и Роскомнадзора, а также соавтор закона сенатор Людмила Бокова отказались от комментариев…» ***(Операторы хотят изменить закон «о суверенном Рунете» во избежание утечек данных // РосКомСвобода (https://roskomsvoboda.org/52946/)/. 03.12.2019).***

***

**«Выяснилось, что после установки антивирусные продукты Avast и AVG дополнительно устанавливают расширения для Firefox и Chrome под названиями Avast Online Security, AVG Online Security, Avast SafePrice и AVG SafePrice, собирающие дополнительные данные о юзерах**

Mozilla удалила четыре расширения Firefox, созданные Avast и ее дочерней компанией AVG, после получения достоверных отчетов о том, что эти расширения собирали как пользовательские данные, так и историю просмотров пользователей.

Были удалены следующие расширения: Avast Online Security, AVG Online Security, Avast SafePrice и AVG SafePrice. Первые два показывают предупреждения, когда пользователи переходят на известные вредоносные или подозрительные сайты, в то время как два других показывают сравнение цен и сделок для онлайн-покупателей.

Данные расширения действительно были бы весьма полезны, если бы не одно обстоятельство, ещё в конце октября текущего года выявленное создателем Adblock Plus Владимиром Палантом. Как оказалось, они отправляют большие массивы данных об активности пользователей в интернете на сайт https://uib.ff.avast.com/v5/urlinfo.

В частности, расширения отправляют посещенные пользователями URL-адреса, названия страниц, реферер (строка, передающаяся серверу от клиента и определяющая источник запроса), сведения о версии ОС, уникальный идентификатор пользователя, данные о том, посещал ли пользователь эту страницу ранее и пр.

По мнению Паланта, подобная информация позволяет Avast и AVG восстанавливать историю браузинга

Видя, что его первоначальное сообщение в блоге не получило поддержки, на которую он надеялся, и ни один из разработчиков браузеров не вмешался, чтобы убрать сомнительные расширения самостоятельно, Палант сказал, что он сообщил о проблемах разработчикам Mozilla, надеясь, что организация примет меры. Mozilla отреагировала в течение 24 часов. Палант также предупредил Google, но расширения до сих пор есть в магазине плагинов для Chrome. Такое же сообщение он выслал в адрес Opera и ждёт, что компания отреагирует на него быстрее, чем Google.» ***(Mozilla удалила расширения Avast и AVG из-за слежки за пользователями // РосКомСвобода (https://roskomsvoboda.org/52996/). 04.12.2019).***

***

**«Немецкая телекоммуникационная компания 1&1 Telecom оштрафована на крупную сумму за нарушение «Общего регламента по защите данных» (GDPR).** Федеральный комиссар по защите данных и свободе информации Германии (BFDI) оштрафовал 1&1 на €9,55 млн за непринятие в колл-центрах необходимых мер по защите персональных данных клиентов от постороннего доступа.

Как сообщает BFDI, кто угодно мог в полном объеме получить персональную информацию любого клиента 1&1, просто позвонив в службу поддержки и назвав его имя и дату рождения. Это является прямым нарушением ст. 32 «Общего регламента по защите данных», обязывающей компании принимать меры по обеспечению безопасности персональных данных.

Несмотря на то, что инцидент затронул небольшое количество клиентов 1&1, BFDI счел необходимым оштрафовать компанию на крупную сумму, поскольку под угрозой оказалась вся ее клиентская база. Более того, сумма штрафа могла быть выше, но регулятор принял дополнительные меры безопасности – теперь сотрудники колл-центра запрашивают больше сведений для подтверждения личности звонящего. Компания также пообещала ввести новую систему аутентификации, призванную существенно усилить защиту данных клиентов.

После инцидента с 1&1 комиссар инициировал расследование для выявления подобных случаев в других телекоммуникационных компаниях». ***(Немецкая телеком-компания оштрафована на €10 млн за нарушение GDPR // SecurityLab.ru (https://www.securitylab.ru/news/503386.php). 12.12.2019).***

***

**«В 2019 году персональные данные россиян стали утекать через ИТ-специалистов…** На долю системных администраторов в 2019 году впервые пришлось 2% слива. Причиной является то, что профессия ИТ-специалиста из элитной становится массовой, что влечет снижение уровня доходов и требований к соискателям, полагают аналитики.

В остальных 98% случаях утечки данных произошли при помощи специалистов других подразделений банков и компаний, включая специалистов бэк-офиса и клиентской поддержки.

По объему на слив информации сисадминами приходится более четверти всех утечек». ***(DeviceLock: ИТ-специалисты — новый канал утечек персональных данных // Открытые системы (https://www.computerworld.ru/news/DeviceLock-IT-spetsialisty--novyy-kanal-utechek-personalnyh-dannyh). 16.12.2019).***

***

**«Дослідники виявили масштабну базу даних, яка містить особисту інформацію про користувачів Facebook. Інформацію можуть використовувати для масштабних спам-розсилок, кажуть експерти.**

Дослідникам у сфері кібербезпеки вдалося виявити велику базу даних з інформацією про 267 мільйонів користувачів Facebook. Інформація про облікові записи, телефонні номери та імена була доступна у відкритому вигляді без пароля.

Про це повідомили самі дослідники Comparitech у своєму публічному звіті.

На думку експертів, виявлена база даних з'явилася в результаті «роботи» в'єтнамських кіберзлочинців. Вони могли отримати її нелегальним шляхом через існуючу «діру» в системі Facebook або зловживаючи інтерфейсом доступу Facebook, який працював до 2018 року.

Більшість даних належали користувачам зі США. Експерти перевірили вміст бази, і вона виявилася актуальною. Кожен із записів містив унікальний номер облікового запису Facebook ID, номер телефону, повне ім'я користувача, дату народження.

Інформація, яка міститься в базі, могла використовуватися для проведення масштабних спам-кампаній, фішингу та інших кібератак. Також її могли використовувати для повного розкриття особистості користувача, допускають дослідники…» ***(267 млн акаунтів і телефонних номерів з Facebook опинилися у відкритому доступі // MediaSapiens (https://ms.detector.media/web/cybersecurity/267_mln_akauntiv_i_telefonnikh_nomeriv_z_facebook_opinilisya_u_vidkritomu_dostupi/). 20.12.2019).***

***

**«Эксперты UpGuard обнаружили в открытом доступе более терабайта незащищенных пользовательских данных, хешированных паролей и корпоративных документов. Утечка коснулась сразу нескольких крупных компаний, включая GE, Xerox, Nasdaq и Dunkin'.**

Причиной инцидента стали неправильные настройки облачного хранилища Amazon. Исследователи обнаружили незащищенный S3-контейнер 15 октября. Когда аналитики поняли, что заключенная в нем информация не должна быть доступна всему Интернету, они сообщили о находке владельцу хранилища, маркетинговой компании iPR Software.

Представители этой организации подтвердили, что знают о проблеме, однако корзина еще три недели оставалась открытой. Лишь 26 ноября, после того как ИБ-эксперты сообщили о своей находке журналистам, администраторы хранилища закрыли общий доступ.

*Содержимое обнаруженной базы*

Исследователи заключили, что контейнер представлял собой внутреннюю базу платформы, с которой работают заказчики iPR Software. Ее содержимое включало 477 тыс. контактов СМИ, более 35 тыс. хешированных паролей, резервные копии баз MongoDB, администраторские учетные данные, корпоративные документы и прочие файлы. Контейнер оказался таким большим, что система зависала при подсчете его точного объема. Известно лишь, что он превышает терабайт.

По словам экспертов, многие данные в скомпрометированной базе так или иначе предназначались для публичного использования. Это в первую очередь разнообразные маркетинговые материалы. В то же время аналитики увидели в папках и закрытые данные — например, кризисные PR-стратегии.

Кроме того, в некоторых случаях в хранилище обнаружились данные для доступа к сторонним сервисам, включая учетную запись iPR Software в Twitter и некий ключ Google API. Эксперты не проверяли работоспособность этих аккаунтов, тем не менее допуская, что злоумышленники могли успеть завладеть этой информацией, чтобы использовать ее в атаках…». ***(Maxim Zaitsev. Более терабайта корпоративных данных попали в Интернет // Threatpost (https://threatpost.ru/ipr-software-amazon-s3-bucket-exposing-data-on-half-million-media-contacts/34998/). 10.12.2019).***

***

**«Уряд Об'єднаних Арабських Еміратів використовує популярний у країні додаток для обміну текстовими повідомленнями ToTok для стеження за користувачами.**

Про це заявили американські чиновники, ознайомлені з відповідними розвідданими…

"Додаток ToTok насправді є шпигунським інструментом... Він використовується урядом ОАЕ для спроби відстеження кожної розмови, пересування, взаємовідносин, зустрічей, звуків та фото тих, хто встановлює його на свій телефон", - йдеться у повідомленні.

Як зазначається, ToTok було створено лише кілька місяців тому. Однак в Еміратах, де влада блокує доступ до аналогічних додатків Apple і Facebook, він став

доволі популярною альтернативою безкоштовним месенджерам і був завантажений на мільйони пристроїв у країні.

Технічний аналіз та інтерв'ю з експертами з комп'ютерної безпеки показали, що компанія-розробник ToTok - Breej Holding, найімовірніше, пов’язана з еміратською компанією DarkMatter, яка займається кібербезпекою і має тісний зв’язок з урядом.

У ЦРУ відмовилися коментувати цю інформацію.

Коли NYT звернувся до представників Apple і Google з питаннями про зв'язок ToTok з урядом Еміратів, в компаніях сказали, що вони проведуть власне розслідування.

В результаті компанія Google видалила додаток зі свого магазину Google Play, встановивши, що ToTok порушує правила. Apple також вилучила ToTok зі свого магазину додатків, заявивши, що вони все ще аналізують його.

Зазначається, що користувачі ToTok, які вже завантажили додаток, зможуть ним користуватися, поки не видалять його зі своїх гаджетів». ***(Влада ОАЕ стежила за громадянами через додаток для смартфону // ТОВ «УКРАЇНСЬКА ПРЕС-ГРУПА» (http://day.kyiv.ua/uk/news/241219-vlada-oae-stezhyla-za-gromadyanamy-cherez-dodatok-dlya-smartfonu). 24.12.2019).***

***

**«Зловмисники викрали базу даних компанії “LifeLabs” - найбільшої у Канаді мережі медичних лабораторій.**

Про це президент “LifeLabs” Чарльз Браун написав у відкритому листі до користувачів компанії.

“Завдяки активному спостереженню “LifeLabs” нещодавно виявила кібератаку, яка відкрила неавторизований доступ до наших комп’ютерних систем з інформацією про користувачів, що могла містити: ім’я, адресу, електронну скриньку, логін, пароль, дату народження, номер картки державного медичного страхування та результати лабораторних тестів”, - написав Браун.

Він наголосив, що після отримання інформації про кіберзлам компанія “повернула дані, зробивши платіж”.

“Ми зробили це у співпраці з експертами, знайомими із кібератаками й перемовинами з кіберзлочинцями”, - зазначив директор, не уточнивши виплачену злодіям суму.

За його словами, пов’язані зі злочином проблеми комп’ютерної системи були виправлені “й ми цілодобово працювали, аби створити додаткові застороги для захисту інформації”.

“Компанії із кібербезпеки повідомили нам, що ризик для наших користувачів через цю кібератаку є низьким, і що упродовж розслідувань вони не виявили жодних публічних витоків даних користувачів, у тому числі в “дарк неті” та інших онлайн локаціях”, - зауважується у листі.

Браун підсумував, що загалом зловмисники отримали доступ до даних близько 15 млн користувачів, переважна більшість яких проживають у канадських провінціях Онтаріо та Британська Колумбія.

Зауважимо, що сукупне населення Онтаріо та Британської Колумбії становить 20 млн осіб, тобто жертвами кіберзлочинців потенційно стали 75% їх

мешканців». ***(У Канаді хакери викрали дані 15 мільйонів користувачів // Укрінформ (https://www.ukrinform.ua/rubric-technology/2840232-u-kanadi-hakeri-vikrali-dani-15-miljoniv-koristuvaciv.html). 18.12.2019).***

***

**«Microsoft представила итоги очередного исследования Security Intelligence Report, целью которого стал поиск скомпрометированных учетных данных в ее системах.** В его рамках с января по март было проверено более 3 млрд учетных данных, полученных из различных источников, включая общедоступные базы данных. Исследование показало, что более чем в 44 млн случаев пользователи устанавливали один и тот же пароль для Azure AD и служб Microsoft.

Если в руки злоумышленников попадает одна подобная пара логин-пароль, то в 30% случаев подобрать частично измененный пароль (например, с добавлением порядкового номера) к другим учетным записям можно не более чем с десяти попыток, что может быть использовано для атак на облачные сервисы, DDoS-атак, рассылки фишинговых писем или майнинга криптовалют.

Согласно аналогичному исследованию 2018 г., проведенному «Политехническим университетом Виргинии», из 30 млн пользователей 52% пренебрегали правилами безопасности и использовали один и тот же или частично измененный пароль. В 2019 г. число подобных пользователей снизилось, но цифры все еще остаются внушительными.

Постоянной целью для кибератак становятся облачные провайдеры, и платформа Microsoft Azure не является исключением. Злоумышленники создают виртуальные машины, которые затем используются для рассылки спама, фишинговых и DDoS-атак.

Помимо общей угрозы функциональности объекта такой атаки, DDoS часто служит «дымовой завесой» для более сложных атак. Подходы к организации DDoS-атак продолжают усложняться, при этом затраты и сложность запуска таких атак не возрастают. Это увеличивает частоту и легкость, с которой преступники могут нанести ущерб бизнесу и пользователям. Средняя мощность TCP DDoS-атак, обнаруженных и нивелированных Azure DDoS Protection за 2019 г. (апрель-октябрь) составляла 120,51 ГБ/сек (самая крупная из них – 363,01 ГБ/сек), а средняя мощность DDoS-атак на основе UDP – 16,44 ГБ/сек. (самая крупная – 89,12 ГБ/сек).

Drive by Download (DBD) предполагает непреднамеренную загрузку вредоносного кода на устройство пользователя при посещении им зараженного сайта или при клике на баннер, ведущий на такой сайт. Более продвинутые DBD-кампании даже могут устанавливать программное обеспечение для майнинга криптовалют на устройстве жертвы. По итогам анализа страниц, индексируемых Bing, максимальный среднемесячный объем вредоносных страниц зафиксирован во Французской Полинезии (3,15 страниц на тысячу страниц).

Опасность таких атак – не только в снижении производительности системы, но и в том, что злоумышленник может в любой момент использовать другой, более опасный для жертвы, сценарий. Всего в мире в 2018-2019 гг. с незаконной установкой ПО для майнинга столкнулись 0,11% компьютеров во всем мире. В России эти цифры составили 0,88% в 2018 г. и 0,17% в 2019 г., что свидетельствует об успешной борьбе с недобросовестными майнерами, но не о победе над ними.

Несмотря на повышенное внимание к этому виду атак, они по-прежнему очень эффективны и приносят огромные убытки компаниям. Сейчас злоумышленники чаще всего используют подмену доменных имен, чтобы выдать свои сообщения за электронные письма от известных брендов или коллег жертвы, а также броские темы, чтобы заставить пользователя открыть письмо. Максимальный всплеск фишинговой активности в мире в 2019 г. наблюдался в январе, когда доля зараженных писем составила 0,63% от общего объема писем, проанализированных Microsoft по всему миру.

Часто причиной заражения устройства становятся не только несоблюдение базовых правил кибергигиены и недостаточная осведомленность пользователей, но и использование нелицензионного программного обеспечения. Стремление снизить вероятность загрузки потенциально опасного ПО вызвало в 2019 г. рост спроса на операционную систему Windows 10, а также более широкое использование Windows Defender. Тем не менее, злоумышленники тоже не стоят на месте. В мире в 2019 г. в среднем 3,67% компьютеров в месяц сталкивается с вредоносным ПО. Год назад эта цифра составляла 6,37%.

С таким видом атак мир сталкивается все реже, и тем не менее они продолжают представлять угрозу в некоторых регионах, в первую очередь из-за низкой культуры кибербезопасности. В 2019 г. в среднем в месяц такая проблема возникала на 0,03% компьютеров. Год назад цифра составила 0,08%.» ***(По меньшей мере 44 млн пользователей используют один пароль для всех личных аккаунтов // Компьютерное Обозрение (https://ko.com.ua/po_menshej_mere_44_mln_polzovatelej_ispolzuyut_odin_parol_dlya_vseh_lichnyh_akkauntov_131260). 16.12.2019).***

***

**«Правительство Китая обвинило техногигантов Xiaomi и Tencent в незаконном сборе персональных данных пользователей.** Министерство промышленности и информатизации КНР опубликовало список из 41 приложений, которые, по мнению властей, нарушают закон о сборе персональных данных в стране.

В данный список попали такие приложения, как Xiaomi Finance и мессенджер Tencent QQ, а также сервисы других китайских компаний, например, спортивная медиаплатформа Sina Sports и новостные агрегаторы 36Kr и Sohu News.

С ноября 2019 года Министерство промышленности и информатизации КНР ведет активную борьбу с сервисами, нарушающими закон о сборе и коммерческом использовании персональной информации пользователей. В ходе данной кампании мобильные программы заносятся в «черный список» и блокируются на территории страны. Уже более 8 тыс. сервисов признали нарушения и объявили об их исправлении.

Однако некоторые приложения все еще вызывает вопросы у властей, поскольку программы часто запрашивают у пользователя различные разрешения, а в некоторых случаях усложняют процесс отказа от продления платной подписки». ***(Китай обвинил Xiaomi и Tencent в незаконном сборе данных // SecurityLab.ru (https://www.securitylab.ru/news/503681.php).***

***

**«Європейські закони із захисту персональних даних за півтора роки у дії майже не мали жодного ефекту.** Такого висновку дійшли західні ЗМІ, проаналізувавши судові позови та рішення в рамках нового законодавства…

Технічні гіганти, такі як Google, Facebook, Twitter, "ВКонтакте", збирають наші персональні дані. І ми можемо легко стати маріонетками у їхніх руках. Як це відбувається і які матиме наслідки - у Євросоюзі усвідомили після референдуму про "брекзит". Тоді соцмережами розійшлися мільйони фейків та страшилок, які схиляли британців голосувати за вихід з ЄС. Займалась цим компанія Cambridge Analitica, яка купувала персональні дані користувачів у технічних гігантів.

"Ця компанія, яка працювала на Трампа і "брекзит", визначала політичний профіль людини, щоб зрозуміти її персональні страхи і на їх основі краще таргетувати Facebook-рекламу. Вона досягла цього, незаконно проаналізувавши профілі 87 мільйонів користувачів Facebook", - говорить Керол Кадваллард, британська журналістка-розслідувачка і письменниця.

Як усе працювало, британські журналісти дізналися від колишніх співробітників Cambridge Analitica. Стало зрозуміло - сучасні правила виборчих компаній у демократичних країнах в умовах цифрового світу більше не працюють. Притягти партії до відповідальності за перевищення бюджетів на рекламу абощо неможливо.

"Все, що трапляється на Facebook, там і залишається. І лише ви бачите свою стрічку. Та потім вона зникає. Тож ми не уявляємо, ні хто яку рекламу бачив, ні як вона вплинула, ні які дані використали для таргетування", - говорить Керол Кадваллард, британська журналістка-розслідувачка і письменниця.

Євросоюз взявся писати нові закони, аби покласти край таким маніпуляціям. І вже півтора року тому було ухвалено пакет законів під назвою GDPR. Збирати персональні дані користувачів без їхнього відома і вагомої на те причини стало заборонено. Західні ЗМІ взялися активно пояснювати користувачам, як все працює.

Це будь-які дані, які можуть вас ідентифікувати - ім'я, номер телефону, чи нікнейм. Закон також включає такі речі як IP-адреса чи дані про розташування. І навіть таку чутливу інформацію, як сексуальна орієнтація, стан здоров'я та політичні погляди

Користувачі мають право попросити приватні компанії видалити будь-яку зібрану про них інформацію. За порушення закону передбачені багатомільйонні штрафи. Проте на практиці все значно складніше. Австрійський юрист Макс Шремс, наприклад, подав кілька позовів, потім навіть об'єднався із колегами з інших країн, проте марно.

"Усі справи застрягли в Ірландців. Деякі без відповіді уже понад півтора року", - говорить Цитата: Макс Шремс, австрійський юрист.

Справи вивчає Ірландія, бо саме цю маленьку країну, де розташовані головні офіси Google, Facebook, Microsoft та Twitter, призначили відповідальною за розгляд таких справ. Проте країна, пишуть західні ЗМІ, економічно залежна від цих компаній. Таким чином наразі, за новим законодавством є лише один вирок. Франція наклала штраф у розмірі 50 мільйонів євро на Google в січні. Й експерти вже наполягають - нові закони не діють. І їх варто посилити.» ***(Єврозакони про кібербезпеку провалилися - ЗМІ // ООО "Национальные информационные***

***системы" (https://podrobnosti.ua/2332879-vrozakoni-pro-kberbezpeku-provalilisja-zm.html). 27.12.2019).***

***

## Кіберзлочинність та кібертероризм

**«Первые следы «чужих» в немецком автоконцерне обнаружили весной 2019 года…** Группа злоумышленников называет себя «OceanLotus», и вполне возможно, что она может действовать от имени государства Вьетнам. Эксперты по безопасности автопроизводителя наблюдали за хакерами в течение нескольких месяцев, но в прошлые выходные они соответствующим образом обезопасили свои компьютеры. Известно, что хакерская группа незаконно внедрила троянскую программу Cobal Strike на компьютеры производителя. Это позволило шпионить и удаленно контролировать компьютеры. Благодаря поддельному сайту злоумышленники притворились, что принадлежат к тайскому отделению BMW. В офисе самого автопроизводителя инцидент не комментируют, поэтому неясно, успели ли хакеры получить доступ к секретной информации штаб-квартиры в Мюнхене. Не объясняется каким образом, но компьютерные специалисты связали атаку с запуском вьетнамской марки автомобилей Vinfast. Эксперт Dror-John Röcher из немецкой организации по кибербезопасности объясняет, что атаки на автопроизводителя начались, когда Вьетнам организовал собственное производство автомобилей. Первые две модели вьетнамской марки Vinfast созданы по лицензии BMW при участии концерна Magna. Разработчик транспортного средства и контрактный производитель также производит автокомплектующие для баварского производителя премиум-класса. Для Vinfast Magna взяла на себя полную разработку внедорожника и седана. Для седана по лицензии используется платформа «пятерки» BMW прежнего поколения (F10), а базой для кроссовера послужил BMW X5 в кузове F15.» ***(Вьетнамские хакеры залезли в BMW // AvtoBlog.ua – Автомобильный портал (https://avtoblog.ua/technologies/vetnamskie-hakery-zalezli-v-bmw). 09.12.2019).***

***

**«Крупнейший специалист по обеспечению кибербезопасности в мире компания Check Point раскрыла миллионную аферу, организованную предприимчевым хакером.** Он смог вывести на личный счет средства, перечисленные китайской венчурной компанией израильскому стартапу…

Согласно данным, предоставленным сотрудниками Check Point, хакер прибег к весьма креативному способу обмана, контролируя переписку между компаниями, участвовавшими в переговорах. О махинации стало известно после того, как сторона, представлявшая израильский стартап, не получила обещаной инвестиции с Китая в сумме 1 миллион долларов. Работники Check Point сразу провели расследование, изучив электронные письма и компьютеры, которые участвовали в переписке между компаниями, а также проанализировав журнал сервера. Как выяснилось, все это время в двухсторонних переговорах участвовало третье лицо.

Этот неизвестный смог создать домены, которые практически не отличались от настоящих. Их различие состояло лишь в некоторых символах, которые остались незамеченными израильской и китайской компаниями. Хакер создал два электронных письма, повторив заголовок темы первого письма и отправил их получателю от имен генерального директора стартапа и менеджера китайской компании. При этом и в Китае и в Израиле не заметили подвоха и продолжили общение. Хакер умело корректировал электронные письма отправителей согласно своим потребностям, пока дело не дошло до банковских реквизитов, которые махинатор изменил на поддельные. Именно на указанный счет китайская сторона и перевела 1 миллион долларов США. За все время переписки стартап получил 14 писем от мошенника, а китайская компания - 18. При этом представитель и получатель средств планировали провести встречу, но хакер отослал письма с вымышленными причинами отказа.» ***(Мошенничество на миллион: креативный хакер поразил весь мир необычным преступлением // Ukrainianwall.com (https://ukrainianwall.com/world/20514-moshennichestvo-na-million-kreativnyy-haker-porazil-ves-mir-neobychnym-prestupleniem). 08.12.2019).***

***

**«Команда экспертов FortiGuard Labs компании Fortinet представили прогноз ландшафта угроз на 2020 и последующие годы.** Исследование раскрывает направления, по которым с высокой вероятностью будут действовать киберпреступники в ближайшем будущем. Кроме этого, были обозначены приемы, которые помогут организациям защититься от будущих атак.

***Ключевые выводы исследования:***

*Смена направления кибератак*

За последние годы методики проведения кибератак становились все более изощренными, что привело к росту их эффективности и скорости. Этот тренд, вероятнее всего, сохранится, пока на рынке не появится достаточно организаций, которые изменят свой подход к стратегиям защиты. Учитывая масштабы нынешнего ландшафта глобальных угроз, скорость и сложность кибератак, организациям придется реагировать на возникающие угрозы в реальном времени, не отставая от работы машин, чтобы эффективно противостоять агрессивным действиям. В этой борьбе станет жизненно необходимым применять последние достижения в области искусственного интеллекта (ИИ) и исследования угроз.

*Эволюция ИИ для обеспечения безопасности*

Одной из долгосрочных целей в разработке ИИ для обеспечения безопасности является создание адаптивной системы невосприимчивости к угрозам, работающей аналогично иммунной системе человека. Разработка такого ИИ первого поколения была направлена на использование различных моделей машинного обучения. Они обучались, корректировались и предлагали определенный план действий для отражения атаки. В системах ИИ второго поколения акцент был сделан на создание механизма интеллектуального анализа. Его уровень значительно вырос к этому времени и позволял выявлять паттерны, существенно улучшавшие работу различных функций, таких как управление доступом, путем размещения обучающихся узлов по всем направлениям защиты. Развитие систем ИИ третьего поколения идет по пути отказа от использования

монолитного центра обработки в пользу создания системы региональных обучающихся узлов. Данные накапливаются локально и используются для распределенного сравнения, коррекции и анализа. Это будет иметь крайне важное значение для компаний, которые ищут пути защиты своих разрастающихся периферийных сегментов.

*Распределенное машинное обучение*

Помимо применения традиционных форм анализа угроз с использованием данных из открытых источников или после изучения внутреннего трафика и накопленной информации, будущие системы машинного обучения начнут со временем активно применять данные, собираемые с периферийных устройств нового поколения и передаваемые на локальные обучающиеся узлы. Отслеживая и сопоставляя информацию в реальном времени, ИИ-система сможет иметь более полное представление о текущем состоянии угроз. Она также сможет корректировать работу локальных устройств, задавая им правила для ответной реакции на инциденты. Это позволит будущим ИИ-системам безопасности распознавать угрозы, корректировать свои действий, отслеживать и быть готовыми к ответным мерам, обмениваясь информацией в пределах сети. В конечном итоге, распределенная система обучения позволит объединить наборы данных, чтобы адаптироваться к изменяющимся условиям, тенденциям и событиям. Таким образом, каждое событие будет улучшать качество всем системы. В результате, информация об инциденте, полученная в одном месте, будет повышать осведомленность о текущих угрозах для всей системы.

*Применение ИИ и сценариев реагирования для предсказания кибератак*

Внедрение ИИ позволяет компаниям не только автоматизировать выполнение задач, но и открывает возможность создания автоматизированной системы поиска и выявления кибератак – как после появления признаков, так и до реализации сценария. Благодаря совместному использованию машинного обучения и статистического анализа, организации могут разработать индивидуальный план действий с опорой на ИИ для улучшения раскрываемости угроз и реагирования. Подготовленные сценарии реагирования (playbooks) должны научиться выявлять закономерности (паттерны), с помощью которых ИИ будет прогнозировать действия атакующей стороны, подсказать время вероятного начала следующей атаки и даже выявлять подозреваемых, стоящих за угрозой. Если эти данные можно предоставить системе обучения ИИ, то удаленные обучаемые ноды смогут поддержать эффективную и упреждающую защиту, не ограниченную только обнаружением угроз, но позволяющую также предсказывать последующие действия, проактивно вмешиваться в процесс и координировать действия с другими нодами для одновременного противодействия на пути распространения атаки.

*Возможности контрразведки и уловки*

Одним из наиболее важных факторов борьбы против шпионажа является эффективная контрразведка. Это же справедливо и для кибератак или защиты, где все действия тщательно отслеживаются. Обороняющаяся сторона имеет явное преимущество в доступе к различного рода информации об угрозах. Киберпреступники обычно не обладают такими возможностями, к которым теперь

добавились средства машинного обучения и ИИ. Однако применение хитроумных уловок может привести к ответным мерам со стороны злоумышленников. Они учатся отличать легитимный трафик от уловок и стараются делать это незаметно, чтобы не раскрыть себя во время атаки. Чтобы эффективно противостоять такой стратегии, организациям потребуется добавить в свой арсенал сценарии реагирования и улучшенные алгоритмы ИИ. Это поможет не только обнаруживать нарушителей, занятых разбором легитимного трафика, но и улучшит технологию уловок, что сделает невозможным их отличие от легитимных сообщений. В будущем организации должны научиться реагировать на любые шпионские приемы до начала активных действий, сохраняя за собой превосходство в контроле.

*Усиление связей между правоохранительными органами*

Деятельность организаций, связанная с кибербезопасностью, предоставляет им ряд уникальных привилегий, касающихся доступа к персональной информации; представители преступного мира не обладают таким правом. Это позволяет правоохранительным органам создавать собственные командные центры с глобальным охватом и распространять свои действия на частных лиц, имея возможность наблюдать за киберпреступниками в реальном времени и реагировать на их действия. Существующая система законных действий, а также связи с общественными и частными службами также может быть полезна для выявления нарушителей и ответной реакции. Можно ожидать появления инициатив по формированию единого подхода для связей между правоохранительными органами международного и местного уровней, правительственными организациями, корпоративным сектором и экспертами в области безопасности. Это будет способствовать развитию системы своевременного и безопасного обмена информацией для выстраивания защиты критически важной инфраструктуры и усиления борьбы с киберпреступлениями.

*Изобретательность киберпреступников остается на прежнем уровне*

Новые возможности, вносимые организациями в свою стратегию защиты, вряд ли останутся без внимания со стороны противника и будут иметь ответную реакцию. Внедрение улучшенных методов обнаружения и противодействия кибератакам приведет к попыткам киберпреступников сделать что-то другое, еще более серьезное. На фоне появления более совершенных методов атаки, расширения направлений потенциальных атак, внедрения более умных ИИ-систем, изобретательность представителей киберпреступного мира также не снижается.

*Усовершенствованные методы уклонения*

В недавнем отчете Fortinet Threat Landscape отмечался рост популярности различных усовершенствованных методик уклонения. Их разработка направлена специально на то, чтобы избегать обнаружения, отключать функции защиты и устройства контроля, наносить урон, работая «под прицелом» систем защиты и применяя тактику LoTL – использование легитимного установленного ПО и маскировка вредоносного трафика под законный. Многие современные вредоносы уже содержат внутри себя функции, позволяющие уклоняться от обнаружения антивирусными программами или другими средствами противодействия угрозам. Но злоумышленники продолжают применять все более изощренные способы запутывания и противодействия анализу. При использовании таких стратегий роста

значительно повышается значение «слабых мест», которые могут оставаться в средствах безопасности и появляться в результате ошибок персонала.

*Swarm-технология*

Последние несколько лет на рынке наблюдался рост популярности swarm technology, связанного с выполнением поставленной задачи за счет массированных, скоординированных, однотипных действий. Применение средств машинного обучения и ИИ в атаках против легитимных сетей и устройств привело к появлению еще одного способа применения этой технологии. С одной стороны, ее достижения имеют важное значение для решения прикладных задач в области медицины, транспорта, машиностроения, автоматизации. Однако при злонамеренном использовании в условиях, когда организации не вносят изменений в свою стратегию защиты, паритет может нарушиться в пользу злоумышленников. Киберпреступники могут применять Swarm-технологию в бот-атаках для проникновения в сеть, подавления внутренних средств обороны, повышения эффективности поиска и кражи данных. Ожидается, что со временем появятся специализированные боты, наделенные определенными функциями, которые будут обмениваться данными в реальном времени и сопоставлять их. В результате возрастет скорость отбора целей, а тактика проведения атаки станет более разнообразной. Киберпреступники смогут атаковать уже не только одну, а и сразу множество целей одновременно.

*Использование 5G и Edge-вычислений в качестве оружия*

Проникновение сетей 5G может со временем стать катализатором для развития функциональных Swarm-атак. В их основе будет лежать возможность выстраивания локальных специальных сетей, которые способны быстро обмениваться и обрабатывать данные, а также запускать в работу приложения. При этом ненадлежащем использовании 5G и периферийных Edge-вычислений каналом для распространения вредоносного кода могут стать взломанные устройства. Если собрать их в группу, то станет возможным проведение скоординированных атак на скоростях 5G. Принимая во внимание быстродействие, степень интеллектуальности, а также локальный характер проведения таких атак, под угрозой могут оказаться устаревшие технологии защиты, что заставит задуматься о поиске путей для эффективного противостояния таким угрозам.

*Ожидается резкий рост атак нулевого дня*

До сих пор на поиски уязвимости нулевого дня и разработку эксплойта уходило традиционно много сил и времени. Поэтому киберпреступники не торопились с их применением, придерживая в своем арсенале, пока оставались другие варианты для атаки. Нынешняя ситуация характерна ростом возможных направлений для угроз, а также упрощением задачи выявления уязвимостей. Это привело к угрозе потенциального роста числа уязвимостей нулевого дня. Применение технологий фаззинга и планомерный поиск («майнинг») уязвимостей нулевого дня с использованием ИИ также способствуют экспоненциальному росту числа подобных кибератак. Поэтому необходимо заблаговременно принимать меры для защиты, чтобы противостоять этому тренду.» ***(Рост атак нулевого дня, враждебный ИИ и другие тренды ИБ // Компьютерное Обозрение***

***(https://ko.com.ua/rost_atak_nulevogo_dnya_vrazhdebnyj_ii_i_drugie_trendy_ib_131141). 05.12.2019).***

***

**«Мэр Нового Орлеана (американский штат Луизиана) Латоя Кантрелл объявила о введении в городе режима чрезвычайной ситуации из-за массированной кибератаки.**

Кантрелл заявила, что компьютерные системы, которые используют власти города, подверглись атаке с применением вирусов-вымогателей…

В целях предосторожности многие серверы городских служб были отключены. Для защиты компьютеров привлечены специалисты ФБР, Секретной службы США и Национальной гвардии США.

Мэр не уточнила, какие городские службы столкнулись с наиболее серьезными затруднениями из-за кибератаки. Местные телеканалы отмечают, что полиция и пожарные продолжают работать.

Режим ЧС в американских городах и штатах обычно объявляют только в случае стихийных бедствий, что позволяет запрашивать у федеральных властей дополнительные средства и ресурсы…» ***(Ольга Никитина. В американском городе ввели режим ЧС из-за кибератаки // Деловая газета «Взгляд» (https://vz.ru/news/2019/12/14/1013646.html). 14.12.2019).***

***

**«Команда специалистов из Section 52 компании CyberX предупредила о продолжающейся кампании по кибершпионажу против промышленных и инженерных компаний. По словам экспертов, от атак киберпреступников пострадало более 200 компаний.**

Хотя большинство жертв находятся в Южной Корее, пострадали фирмы из разных стран, включая Японию, Индонезию, Турцию, Германию, Эквадор и Великобританию. Одну из неназванных жертв исследователи описывают как «многомиллиардный корейский конгломерат, который производит критически важное инфраструктурное оборудование».

Вредоносная кампания начинается с отправки специально сформированных фишинговых писем для внедрения в корпоративные сети. Преступники отправляют сообщения, содержащие вложения на «промышленную тематику», в том числе официальные документы, схемы электростанций и запросы на проектирование объектов, таких как газоперерабатывающие и промышленные предприятия. Злоумышленники выдают себя за легитимные компании, например, в одном из случаев они маскировались под дочернюю компанию Siemens.

По словам экспертов, в кампании применяется новая версия вредоносного ПО Separ для кражи учетных данных. После установки в целях сохранения присутствия на системе вредонос добавляет ключи в реестр Windows, а затем приступает к сбору учетных данных. Separ использует бесплатные инструменты для расшифровки с целью получить пароли от браузеров, включая Mozilla Firefox, Google Chrome и Apple Safari, а также учетные данные для аккаунтов в Gmail, Yahoo, Windows Live и Hotmail.

Обновленная версия Separ также проверяет файлы с различными расширениями, включая изображения и документы Microsoft Office, а затем отправляет полученную информацию по FTP на контролируемый злоумышленниками домен.

Кроме того, вредоносная программа с помощью команды ipconfig проверяет подключенные к скомпрометированной системе сетевые адаптеры и пытается отключить Windows Firewall. По словам экспертов, организатором кампании, скорее всего, является одна из APT-группировок (о какой группе идет речь, не уточняется).» ***(Более 200 промышленных компаний стали жертвами кампании по кибершпионажу // SecurityLab.ru (https://www.securitylab.ru/news/503524.php). 18.12.2019).***

***

**«Исследователь безопасности Клаудио Гуарнери (Claudio Guarnieri) из международной правозащитной организации Amnesty International опубликовал в Сети 25 ГБ данных о 100 тыс. фишинговых атак.**

Согласно результатам ежегодного отчета «Data breach and incident response» (DBIR) компании Verizon, фишинг являлся основным вектором атак в 32% случаях всех утечек данных.

Гуарнери в течение почти десяти лет отслеживал мошеннические атаки. По словам специалиста, архив содержит базу данных фишинговых URL-адресов, информацию об HMTL-страницах и скриншоты мошеннических web-сайтов…» ***(Эксперт опубликовал 25 ГБ данных о 100 000 фишинговых атаках // SecurityLab.ru (https://www.securitylab.ru/news/503478.php). 17.12.2019).***

***

**«Не прошло и недели с предыдущей кибератаки на Иран, как преступники попытали свои силы снова. Об этом в воскресенье, 15 декабря, сообщил министр информационных и телекоммуникационных технологий Ирана Мохаммад Джавад Азари Джахроми**…

По словам министра, целью атаки был «шпионаж за правительственной разведкой», однако она была «выявлена и отражена щитом кибербезопасности». Джахроми также добавил, что властям удалось выявить использовавшиеся в атаке серверы и отследить атакующих, но не вдавался в подробности. Кто стоит за атакой, каковы ее масштабы и есть ли пострадавшие, министр не сообщил.

В прошлую среду Джахроми сообщил информационному агентству IRNA о масштабной «правительственной» кибератаке на электронную инфраструктуру Ирана. Никаких подробностей об инциденте министр не представил, но отметил, что атака была отражена, и вскоре будет опубликован соответствующий отчет. В то же время стало известно о крупнейшей за всю историю Ирана утечке данных клиентов банков. По словам Джахроми, утечка произошла по вине недобросовестного подрядчика, а не в результате взлома банковских систем». ***(Иран отразил вторую кибератаку за неделю // SecurityLab.ru (https://www.securitylab.ru/news/503437.php). 16.12.2019).***

***

**«Злоумышленники атаковали компьютерную сеть больницы в чешском городе Бенешов. Киберпреступники заразили сеть медучреждения вымогательским ПО, зашифровав данные в системе больницы, сообщает информагентство ЧТК.**

Как сообщил директор больницы Роман Мрва, атака произошла около 2 часов ночи. В хирургическом отделении компьютеры стали медленно работать, а примерно через час вся внутренняя система больницы вышла из строя. Вредонос преодолел межсетевой экран и обошел две антивирусные программы, в результате чего прекратили работу около 300 серверов и рабочих устройств.

Больница работала в ограниченном режиме, из-за чего невозможно было проводить обследования и лабораторные исследования. Из Праги прибыли эксперты Национального управления по кибернетической и информационной безопасности, которые займутся восстановлением системы.

Полиция расследует дело о несанкционированном доступе к компьютерной системе и носителю информации. Как сообщает информагентство, результате происшествия не было утечки каких-либо данных». ***(Киберпреступники заразили сеть одной из больниц в Чехии вымогательским ПО // SecurityLab.ru (https://www.securitylab.ru/news/503412.php). 13.12.2019).***

***

**«Компания Microsoft опубликовала отчет о тенденциях вредоносного ПО и кибербезопасности в 2019 году, в котором также рассказала о росте активности фишинговых атак.**

По словам Microsoft, количество обнаруженных фишинговых писем выросло с 0,2% в январе 2018 года до 0,6% в октябре 2019 года. В то время как количество фишинговых атак увеличилось, общее число вымогательского ПО, криптомайнеров и других вредоносных программ сократилось.

В своем блоге компания рассказала о трех наиболее сложных фишинговых атак, выявленных в нынешнем году.

Первой является многоуровневая вредоносная кампания, в результате которой киберпреступники отравили результаты поиска Google. Мошенники сначала направляли перехваченный с законных сайтов web-трафик на собственные ресурсы. Попав в топ результатов поиска Google по ключевым словам, преступники отправляли жертвам электронные письма со ссылками на данные результаты поиска. Если пользователь нажимал на подобную ссылку, а затем на популярный результат поиска, он попадал на сайт, где его перенаправляли на фишинговую страницу.

Другая вредоносная кампания была выявлена в августе. Мошенники использовали вредоносные пользовательские страницы с ошибкой 404 для осуществления мошеннических атак. Тогда как большинство фишинговых писем содержат ссылку на мошеннический URL-адрес, в рамках данной кампании злоумышленники использовали ссылки на несуществующие страницы. Системы безопасности Microsoft во время сканирования ссылки обнаруживали ошибку 404 и считали ссылку безопасной, тогда как в действительности пользователь перенаправлялся на вредоносный сайт. Использование алгоритмов генерации

поддоменов и постоянная смена домена позволяли злоумышленникам создавать большое количество фишинговых URL-адресов.

Третья фишинговая кампания заключалась в осуществлении MitM-атак. Злоумышленники собирали связанную с целевой компанией информацию (логотипы, баннеры, текст и фоновые изображения) с сайта Microsoft, и с помощью данных элементов создавали свой фишинговый сайт, который практически никак не отличался от настоящего. Далее фишеры рассылали письма с URL-адресами, имитирующими страницы авторизации. У жертв складывалось впечатление, что они находятся на легитимной странице, однако выдать подвох мог URL-адрес, отображающийся в адресной строке браузера». ***(Microsoft рассказала о самых сложных фишинговых атаках 2019 года // SecurityLab.ru (https://www.securitylab.ru/news/503372.php). 12.12.2019).***

***

**«В результате утечки данных в Сеть попала информация компании Dronesense, предоставляющая платформу для управления беспилотниками правительственным, правоохранительным и частным клиентам. База данных содержала маршруты и траектории полетов дронов.**

Таким образом стало известно, какие полицейские отделения, службы безопасности и предприятия используют беспилотники в США. Как сообщает Motherboard, один из дронов тщательно следил за жилым комплексом и парковкой возле Атланты, штат Джорджия. На другом маршруте с пометкой «оценка бедствий» указан беспилотник, наблюдающий за детской площадкой. Третий маршрут, обозначенный как «Миссия картирования», насчитывает почти два десятка так называемых «точек захвата», предположительно необходимых для фотографирования по всему жилому району Вашингтона, округ Колумбия.

База данных также включала более 200 различных записей, информацию о марке беспилотника, имя оператора, адрес электронной почты и пр.

Утечку данных выявил исследователь безопасности Ноам Ротем (Noam Rotem) и сразу сообщил о своей находке Dronesense. По словам компании, конфиденциальные данные пользователей не были затронуты, а проблема сразу была устранена после обнаружения». ***(Американская компания случайно раскрыла маршруты полицейских дронов // SecurityLab.ru (https://www.securitylab.ru/news/503344.php). 12.12.2019).***

***

**«Неизвестные киберпреступники могли похитить конфиденциальную информацию у двух подрядчиков Министерства обороны и Вооруженных сил Сингапура.** Как сообщается на сайте минобороны, сети медицинского института HMI Institute и компании ST Logistics подверглись атакам вредоносного ПО, в результате чего могла произойти утечка персональных данных служащих министерства и ВС.

С 2016 года HMI Institute проводит для служащих Минобороны и ВС учения по сердечно-легочной реанимации и использованию автоматического дефибриллятора. ST Logistics является подрядчиком Минобороны и ВС с 1999 года и оказывает услуги логистики. В связи с этим в распоряжении у обеих организаций

имеются персональные данные военных и сотрудников министерства, необходимые для оказания вышеуказанных услуг.

Затронутые инцидентом системы HMI Institute содержали персональные данные 120 тыс. человек, в том числе полные имена и номера регистрационных карт (NRIC) 98 тыс. военнослужащих и сотрудников Минобороны, а также полные имена, номера регистрационных карт, номера телефонов, электронные адреса, даты рождения и адреса проживания остальных клиентов института.

В случае с ST Logistics затронутые инцидентом системы содержали полные имена, номера регистрационных карт, электронные адреса, номера телефонов и адреса проживания 2,4 тыс. военнослужащих и сотрудников Минобороны.

Масштабы инцидента и причиненный им ущерб пока устанавливаются, однако, как показало предварительное расследование, утечка персональных данных могла иметь место. В настоящее время ведется следствие». ***(Подрядчики Минобороны и ВС Сингапура подверглись кибератакам // SecurityLab.ru (https://www.securitylab.ru/news/503657.php). 23.12.2019).***

***

**«Специалисты компании PhishLabs рассказали о необычной кампании, нацеленной на угон аккаунтов пользователей Office 365.** Как сообщили ИБ-аналитики, злоумышленники не стремятся украсть логин и пароль пользователя, но пытаются установить на его устройство вредоносный плагин с широким набором разрешений. Атаки носят целевой характер — киберпреступники применяют методы социальной инженерии, чтобы обманом заставить жертву загрузить зловреда.

Злоумышленники используют поддельное уведомление OneDrive

Точкой входа для нападающих является электронное письмо, маскирующееся под сообщение службы Microsoft OneDrive со ссылкой на файл в хранилище. В тексте письма, а также названии документа используются сведения, знакомые получателю. Реальный адрес отправителя скрыт при помощи спуфинга — вместо него отображаются данные одного из сотрудников целевой организации. Письмо не содержит прикрепленных объектов и способно успешно миновать антивирусные фильтры почтового сервера.

Ссылка на файл, содержащаяся в тексте, на самом деле является запросом на установку дополнительной утилиты для Office 365. Такие надстройки используются для расширения функций почтового клиента Outlook и других приложений, входящих в набор. Они могут быть созданы сторонними разработчиками и загружаются с принадлежащих им ресурсов.

Если получатель письма не был аутентифицирован в Office 365, то при переходе по ссылке откроется легитимный диалог ввода логина и пароля аккаунта Microsoft. После входа происходит запуск процесса установки, при этом вспомогательное приложение запрашивает широкий набор разрешений. Согласившись с ними, пользователь предоставляет надстройке возможность:

читать, изменять и удалять доступные файлы, а также создавать новые документы;

читать электронные письма;

изменять настройки электронной почты, в том числе создавать правила переадресации;

просматривать записные книжки OneNote, доступные в рамках аккаунта;

копировать список контактов.

Как выяснили исследователи, вредоносное расширение было создано 25 ноября 2019 года под учетной записью легитимной организации. По мнению специалистов, аккаунт разработчика был умышленно скомпрометирован для использования в криминальной кампании.

ИБ-аналитики не зафиксировали массового использования этого метода взлома, поскольку подготовка такой атаки требует значительных усилий от нападающих. Гораздо более распространенный способ угона аккаунтов Office 365 — получение доступа через незащищенный протокол IMAP. По данным компании Proofpoint, в период с сентября 2018 года по февраль 2019-го количество подобных инцидентов исчислялось десятками тысяч». ***(Maxim Zaitsev. Вредоносный плагин атакует пользователей Office 365 // Threatpost (https://threatpost.ru/malicious-add-in-aims-to-hijack-office-365-user-account/35007/). 11.12.2019).***

***

**«Исследовательская компания IntSights опубликовала перечень наиболее значимых киберугроз наступающего года.** Эксперты считают, что в преддверии президентских выборов в США интернет ждет новый всплеск фейков и дипфейков, а хакерские атаки и кража личных данных станут более изощренными. И произойдет это благодаря массовому применению злоумышленниками искусственного интеллекта (ИИ).

…IntSights считает, что в числе главных киберугроз 2020 года не только распространение фейковых новостей, но и более сложные для разоблачения дипфейки (deepfake) — поддельные изображения и видео, созданные ИИ на основе изучения алгоритма реальных людей.

Первые дипфейки появились еще в 2016-2017 годах. В последние месяцы все больше экспертов заговорили об их опасности на фоне массового распространения таких видео. Об этом недавно заявила и компания Trend Micro, представившая собственный прогноз главных киберугроз на ближайший год. В отличие от IntSights, эксперты Trend Micro упомянули в числе потенциальных опасностей рост популярности среди компаний облачных сервисов и стороннего открытого кода, удаленно работающих сотрудников и распространение 5G.

В свою очередь, IntSights отмечает, что, помимо дипфейков, в 2020 году киберпространство может ожидать новое нашествие обычных фейков — на фоне активизации политических пиар-кампаний в преддверии президентских выборов в США. Однако в следующем году ситуация будет отличаться не в лучшую сторону.

Бороться со всем этим будет сложно, потому что развитие технологий и инфраструктуры будут более доступными для злоумышленников»,— считает господин Маор.

Главной причиной эксперты IntSights считают растущую доступность ИИ, которая позволит фабриковать фейки, распространяя их адресно для конкретной аудитории. Компания считает, что еще в недавнем прошлом атаки злоумышленников были более затратными как с точки зрения сил, так и времени.

Однако с ростом популярности ИИ-технологий такие способы станут проще и дешевле. А при помощи ИИ злоумышленники могут осуществлять многочисленные и повторяющиеся атаки в сетях, написав программу из нескольких строк кода и позволив ИИ выполнять большую часть работы по рассылке и таргетированию…» ***(Исследователи IntSights включили ИИ в число киберугроз 2020 года // IKSMEDIA.RU: (http://www.iksmedia.ru/news/5631911-Issledovateli-IntSights-vklyuchili.html). 19.12.2019).***

***

**«Киберпреступник отключал от интернета целые страны.**

В 2016 году масштабная DDoS-атака обвалила серверы крупнейшего провайдера Либерии и на несколько дней оставила полстраны без интернета. Затем вирус перекинулся на Европу, атаковав серверы компаний в Германии, Франции и Великобритании. Спецслужбы выяснили, что за атакой стоял 29-летний британец Дэниел Кайе, работавший под ником Spiderman. После ареста он признался, что атаковал либерийского провайдера по заказу его конкурента. Кайе использовал открытый код вируса Mirai и превратил его в крупнейший в мире ботнет. Затем вирус «вышел из-под контроля» и атаковал европейские серверы. Дэниела судили в Германии, где он отделался условным сроком, и в Великобритании, где вместо 10 лет он получил 32 месяца тюрьмы. TheБабель пересказывает большой материал Bloomberg о том, как Дэниел Кайе стал самым разыскиваемым хакером в мире, но его причастность к большинству преступлений не смогли доказать.

В октябре 2016 года на Либерию, одну из беднейших стран мира, началась хакерская атака. Более полумиллиона камер наблюдения по всему миру пытались подключиться к горстке серверов местного оператора мобильной связи Lonestar Cell MTN. Сеть Lonestar рухнула от перегрузки — почти половина страны осталась без интернета, включая банки и больницы…». ***(Поймать Спайдермена. Как упекли за решетку самого разыскиваемого хакера в мире // CRiME (https://crime-ua.com/node/26657). 26.12.2019).***

***

**«В наступному році все більше кіберзлочинців будуть використовувати штучний інтелект для масштабування своїх атак. При цьому традиційні антивірусні рішення не зможуть захистити цифрові системи від загроз.**

Про відповідні прогнози експертів розповів заступник голови Комітету з питань цифрової трансформації ВР Олександр Федієнко під час слухань на тему «Національна кібербезпека та кіберзахист України, у тому числі у сфері критичної інфраструктури», передає «Закон і Бізнес» з посиланням на прес-службу Верховної Ради.

За його словам, наступного року очікуються нові спроби злочинців атакувати об’єкти з відкритим кодом. Буде зростати потреба в таких процесах як фонові перевірки розробників та відкриті джерела розробників. На даний час середовище з відкритим кодом повністю базується на довірі. Організації, як правило, не верифікують попередні проекти й репутацію розробників.

О. Федієнко висловився за необхідність проведення комплексного перегляду всього законодавства щодо питань інформаційної безпеки з метою створення

системи узгодження та гармонізації у законах питань, які не суперечили б один одному та не залишили б білих плям. «В державі необхідно побудувати всеосяжну систему регулярної оцінки стану кібербезпеки, постійного моніторингу та спостереження кіберінцидентів на основі надійних даних», — наголосив він». ***(У 2020 році антивіруси вже не захищатимуть комп'ютери // Закон і Бізнес (https://zib.com.ua/ua/140657-u_2020_roci_antivirusi_vzhe_ne_zahischatimut_kompyuteri_.html). 24.12.2019).***

***

**«Киберпреступники намерены всерьёз взяться за продажу медицинских данных пользователей в даркнете. Таким прогнозом на 2020 год поделилась «Лаборатория Касперского»…**

Как считают эксперты, в даркнете будет появляться всё больше объявлений о продаже информации из медицинских карт или страховых полисов. Некоторые из них уже сейчас оцениваются дороже, чем банковские данные жертв.

Купленная информация станет полезным инструментом в руках злоумышленников, которые хотят войти доверие к пользователям, обманывать их самих или их родственников. Более того, доступ к данным электронных медицинских карт позволит вносить в них изменения для совершения целевых атак и намеренного затруднения постановки диагнозов…

По словам специалистов, медицинские компании недобросовестно относятся к защите информации, в том числе не уделяя должного внимания вопросам обучения сотрудников базовым навыкам кибербезопасности. Именно поэтому подобные фирмы всё чаще становятся жертвами программ-шифровальщиков.

В 2019 году в медицинских организациях по всему миру было атаковано каждое пятое устройство (19%), и число подобных хакерских манипуляций в будущем будет расти, особенно в развивающихся странах, где только начинается процесс цифровизации таких услуг.

Целями киберпреступников, по прогнозам компании, также станут научно-исследовательские медицинские институты и фармацевтические компании. В уходящем году на них было совершено немалое количество атак (49% устройств в фармацевтических компаниях), что объясняется большими денежными затратами на исследования и их ценностью для всей сферы.

Потенциальной опасностью для пациентов в будущем также могут стать имплантируемые медицинские устройства. О подобных атаках эксперты пока не слышали, однако девайсы содержат многочисленные уязвимости, чем рано или поздно воспользуются злоумышленники». ***(Ольга Калинина. Киберзлоумышленники в 2020 году переключатся на медицинские карты // Зоряный (https://zoryanyy.tv/articles/technology/kiberzloumyshlenniki_v_2020_godu_pereklyuchatsya_na_meditsinskie_karty_/). 22.12.2019).***

***

**«Согласно исследованию компании Lenovo, каждый второй хотя бы раз становился жертвой киберпреступников.** Причем 61% пользователей интернета уверены, что с легкостью справятся с кибератаками. Те, кто беспокоятся о

безопасности в сети, прежде всего озадачены защищенностью личных данных (73%) и возможными финансовыми потерями (69%). В свою очередь пользователи меньше боятся репутационных потерь (26%) и снижения производительности работы устройств (28%).

"По данным исследований Lenovo, лишь 3% интернет-пользователей не боятся стать жертвами киберпреступлений. Остальные 97% – ищут способы защитить себя, но в то же время недооценивают реальные угрозы. 23% опрошенных считают, что обычной осторожности в интернете достаточно, чтобы не потерять свои данные. Думаете, только реальный мир может быть жестоким и опасным? Сегодня дети и взрослые все чаще подвергаются угрозам в цифровом пространстве. Создавая устройства Lenovo, мы заботимся о безопасности наших пользователей. Например, для этого разработана уникальная система защиты ThinkShield. Доказано, что данные на наших устройствах на 99% меньше подвержены поражению, чем на других. Однако очень часто решающую роль в потере данных играет банальный человеческий фактор", – отмечает Тарас Джамалов, генеральный директор Lenovo в Украине.

Двухфакторная аутентификация считается одним из самых надежных типов защиты информации. В банковском деле используют 73% пользователей, а вот для социальных сетей – только 35%, чем упрощают доступ киберпреступникам. Не менее надежной считают биометрическую аутентификацию, ее выбирает 54% пользователей. Чаще всего используют отпечаток пальца (43%) или же распознавания лица (21%). Реже – аутентификацию по радужной оболочке глаза (6%) и с помощью подписи (6%)…» ***(Каждый второй становится жертвой киберпреступления – исследование Lenovo // ФОКУС (https://focus.ua/economics/446742-kazhdyi_vtoroi_stanovitsia_zhertvoi_kiberprestupleniia__issledovanie_lenovo). 18.12.2019).***

***

**«Специалисты международной IT-компании – эксперта в области киберзащиты ESET обнаружили новую кибератаку на пользователей платежного сервиса PayPal, сообщается на сайте ESET.** «Компания ESET — лидер в области информационной безопасности — сообщает об обнаружении новой фишинг-атаки, цель которой не только похитить данные входа к платежному сервису PayPal, но и собрать конфиденциальную информацию о жертве», - говорится в сообщении. Согласно сообщению, подобно многим другим схемам фишинга, злоумышленники используют тактику побуждения пользователя к немедленным действиям. В частности, на почту жертве приходит сообщение о «необычной активности» в аккаунте PayPal с рекомендацией защитить его во избежание финансовых потерь. После перехода по ссылке в фишинговом сообщении открывается фейковое окно входа в учетную запись PayPal, где пользователю необходимо ввести имя пользователя и пароль. Однако на этом мошенники не останавливаются, а предлагают жертве якобы «подтвердить свою учетную запись», предоставив дополнительную личную информацию. Таким образом злоумышленники получают не только данные для входа в PayPal, но и информацию о банковской карточке, домашний адрес, данные для доступа к

электронной почте. «Эту информацию киберпреступники могут использовать для различных мошеннических схем, как в интернете, так и за его пределами», - поясняют специалисты ESET. При этом, в компании добавляют, что побуждение к немедленным действиям, как в случае с подтверждением учетной записи в случае с PayPal, — не единственный признак фишинга. Также пользователя должен насторожить странный URL-адрес, ошибки в написании слов, обрезанные буквы. По данным ESET, также наличие зеленого замка слева от URL-адреса свидетельствует о новом тренде — использование фишинговыми сайтами настоящих SSL-сертификатов для убеждения жертв в их легитимности. Например, один из доменов в фишинговой кампании, нацеленной на пользователей PayPal, был зарегистрирован и получил действительный сертификат SSL в начале этого месяца. «В связи с потенциальной опасностью специалисты ESET рекомендуют с максимальной осторожностью относиться к любым нестандартным уведомлениям для ввода вашей конфиденциальной информации и не переходить по подозрительным ссылкам. Также, чтобы не стать жертвой фишинга, при введении любых конфиденциальных данных следует обращать внимание на любые изменения в строке адреса сайта. В случае возникновения сомнений лучше ввести название сайта в браузер вручную или использовать ранее сохраненную закладку», - подытожили специалисты ESET. Как сообщал УНИАН, по данным ESET, в Украине ежедневно фиксируется около 300 тыс. новых киберугроз для информационной безопасности. При этом, найти хакеров-злоумышленников крайне сложно, компаниям остается лишь проводить ежеминутные мониторинги на предмет выявления киберугроз с целью их дальнейшего блокирования…». ***(IT-эксперты обнаружили новую кибератаку на пользователей платежного сервиса PayPal // УНИАН (https://www.unian.net/science/10803983-it-eksperty-obnaruzhili-novuyu-kiberataku-na-polzovateley-platezhnogo-servisa-paypal.html). 20.12.2019).***

***

**«Киберпреступники используют новую тактику для кражи информации о кредитных картах пользователей со всей территории США. Об этом сообщается в пресс-релизе международной платежной системы Visa.**

В то время как большинство ознакомлено со случаями скимминга на автозаправочных станциях, когда преступники устанавливают скиммер на топливораздаточную колонку, новые атаки становятся более сложными и требуют больше знаний.

Visa определила три разных типа атак.

*Злоумышленники скомпрометировали торговую сеть с помощью фишингового электронного письма, отправленного сотруднику. В письме содержалась вредоносная ссылка, при нажатии на которую автоматически устанавливался на компьютер торговой точки троян удаленного доступа (RAT - Remote Access Trojan) и предоставлял мошенникам доступ к данным магазина и его клиентов*

*из сообщения Visa*

В компании отметили, что далее преступники детально изучают корпоративную сеть. Все имеющиеся сведения они используют для того, чтобы

проникнуть в POS-среду. После успешного доступа к POS, вирус начинает собирать с платежного устройства данные банковских карт клиентов.

Второй тип атак предусматривает получение доступа к системе топливной колонки автозаправочной станции. Имея контроль над устройством АЗС, мошенники могут проникнуть в POS-среду. При этом, как они это делают, пока неизвестно…

Третий тип атак тоже касается автозаправочной станции. В Visa считают, что к таким противозаконным действиям могли быть привлечены участники киберпреступной группировки FIN8…» ***(Visa предупредила о новой волне кибератак: на кого нацелены хакеры // PAYSPACE MAGAZINE (https://psm7.com/security/visa-predupredila-o-novoj-volne-kiberatak-na-kogo-naceleny-xakery.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Payspacemagazine+%28Payspacemagazine%29). 16.12.2019).***

***

**«Четырнадцать канадских банков, в том числе CIBC, TD Canada Trust, Scotiabank и Королевский банк Канады (Royal Bank of Canada, RBC), стали жертвой масштабной фишинговой кампании, которая продолжалась на протяжении двух лет.**

Атака начиналась с отправки правдоподобных электронных писем с вложением в формате PDF с использованием официального логотипа банка и кода авторизации. Жертв обманом побуждали как можно быстрее обновить свой цифровой сертификат, чтобы они могли продолжать получать доступ к online-банкингу. Нажав на любой из URL-адресов, жертвы попадали на фишинговую страницу с просьбой ввести свои банковские учетные данные.

Как отметили исследователи из Check Point в своем отчете, в случае с RBC злоумышленники просто сделали снимок экрана официального сайта и добавили невидимые текстовые поля поверх полей ввода, чтобы собрать учетные данные жертвы.

По словам специалистов, существовало несколько вариантов PDF-вложений, с небольшими различиями между ними. Однако некоторые содержащиеся в них текстовые инструкции повторялись, использовали уникальные фразы и появлялись в более чем одном документе.

Фишинговый web-сайт, упоминавшийся во вложениях в формате PDF, был связан с украинским IP-адресом для нескольких доменов, имитирующих страницы банков.» ***(Канадские банки стали жертвами крупной фишинговой кампании // SecurityLab.ru (https://www.securitylab.ru/news/503710.php). 26.12.2019).***

***

**«Во вторник, 24 декабря, Маастрихский университет (Нидерланды) стал жертвой кибератаки. Какого рода кибератака была осуществлена на университет, не уточняется, однако согласно сообщению администрации, она была «серьезной».**

«Маастрихский университет (МУ) подвергся серьезной кибератаке. Затронуты почти все Windows-системы, в частности возникли сложности с

электронной почтой. В настоящее время МУ работает над решением проблемы. Также были приняты дополнительные меры по защите (научных) данных. МУ выясняет, получили ли атакующие доступ к этим данным. Сколько времени понадобится МУ на поиск решения проблемы, пока неизвестно, однако на восстановление работы всех систем определенно уйдет какое-то время», - сообщается на сайте университета.

При попытке открыть электронный ящик или файл появляется пустой экран. Помимо электронной почты также не работают online-библиотека и студенческий портал.

«Проще говоря, если вы хотите что-то сделать, вы не сможете ничем воспользоваться», - сообщил пресс-секретарь университета Герт ван Доорн (Gert van Doorn) порталу Teller Report. По словам ван Доорна, научные данные были «отрезаны» от затронутых атакой систем.» ***(Один из ведущих университетов мира подвергся кибератаке // SecurityLab.ru (https://www.securitylab.ru/news/503699.php). 25.12.2019).***

***

**«Крупная американская радиосеть Entercom подверглась кибератаке, которая могла затронуть функции бэк-офиса. В результате атаки некоторые станции были вынуждены запускать записанные программы.**

Сеть Entercom насчитывает более 235 радиостанций, которые транслируют новости, спорт и музыку, а ее ежемесячная аудитория составляет более 170 млн человек.

Подробности о последнем инциденте на данный момент остаются конфиденциальными, но компания подтвердила факт атаки и вызванный ею сбой в работе.

Злоумышленники атаковали компанию в воскресенье, 23 декабря. Эфирные машины практически не пострадали, но некоторые площадки не могли импортировать музыку и другие типы контента. У компании возникли проблемы с подключением к сети, которые привели к сбою в работе электронной почты, а также потере доступа к файлам и контенту для цифровых платформ. Сотрудникам компании удалось восстановить системы на следующий день.

Это уже вторая по счету атака на компанию Entercom в нынешнем году. Первая произошла в сентябре и была связана с использованием вымогательского ПО, что привело к значительным финансовым потерям компании…». ***(Крупная американская радиосеть Entercom атакована второй раз за год // SecurityLab.ru (https://www.securitylab.ru/news/503693.php). 25.12.2019).***

***

**«Операторы нового однорангового ботнета (P2P), получившего название Mozi, в ходе недавней вредоносной кампании активно проверяли маршрутизаторы Netgear, D-Link и Huawei на наличие ненадежных паролей Telnet.**

По словам исследователей безопасности из компании Qihoo 360 Netlab, киберпреступники используют ботнет для осуществления DDoS-атак. Ботнет использует часть кода Gafgyt, однако не является его производным. В Mozi

реализован DHT-протокол, основанный на стандартном протоколе, обычно используемом торрент-клиентами и другими P2P-платформами для хранения контактной информации узла.

Таким образом злоумышленники могут быстрее заражать новые устройства без необходимости использования серверов, а также «скрывать полезную нагрузку в огромном объеме обычного DHT-трафика». Mozi также использует алгоритмы ECDSA384 и XOR для обеспечения целостности и безопасности компонентов ботнета и сети P2P.

Вредонос использует Telnet-протокол и уязвимости в оборудовании для заражения новых устройств. Операторы авторизуются на целевом маршрутизаторе или видеорегистраторе CCTV с ненадежным паролем, а затем загружают и выполняют полезную нагрузку после успешной эксплуатации уязвимостей в непропатченных хостах. После запуска вредоносного ПО на скомпрометированном устройстве, бот автоматически присоединяется к сети Mozi в качестве нового узла, который в дальнейшем используется для поиска и заражения других уязвимых устройств.

Для обеспечения защиты от перехвата другими преступными группировками, операторы Mozi также настроили автоматическую проверку всех отправляемых на узлы ботнета команд и синхронизированных конфигураций. Таким образом узлами принимаются и выполняются только конфигурации, прошедшие проверку.

Функционал Mozi включает возможность осуществления DDoS-атак, сбора и эксфильтрации информации о зараженных хостах, загрузки и выполнения полезной нагрузки с определенных ресурсов, загрузки обновлений, а также выполнение команд.

В настоящее время список атакуемых ботнетом устройств включает следующие: Eir D1000, Vacron NVR, устройства, использующие Realtek SDK, Netgear R7000 и R6400, DGN1000 Netgear, MVPower DVR, Huawei HG532, D-Link, CCTV DVR и маршрутизаторы GPON». ***(Новый ботнет Mozi заражает маршрутизаторы Netgear, D-Link и Huawei // SecurityLab.ru (https://www.securitylab.ru/news/503685.php). 24.12.2019).***

***

**«Безперервних кібератак зазнають промислові підприємства у всьому світі, навіть ті, які мають розвинену систему кібербезпеки. Завдана шкода від таких атак щоразу зростає в геометричній прогресії, що змушує компанії вживати нових заходів кіберзахисту.**

За перший квартал 2019-го втрати від LockerGoga очікувалися в розмірі $52 млн тільки у Norsk Hydro — одного з найбільших виробників алюмінію у світі. Збитки від Wannacry склали майже $4 млрд, від Petya — $10 млрд. Робочі станції мереж АСК ТП «зачепило» частково, оскільки вразливості стосувалися тільки робочих станцій і панелей оператора під керуванням Windows…

Під час комплексної атаки HatMan (TRITON, TRISIS) на одному з нафтопереробних підприємств на Близькому Сході зловмисники скомпрометували технологічну мережу підприємства й контролювали її кілька місяців. На думку фахівців АСК ТП, причиною стала невдала команда взятого під керування

контролера функціональної безпеки з потрійним резервуванням, що призвело до зупинки критично важливого обладнання.

Необачність багатьох фахівців АСК ТП щодо безпеки власних мереж багато в чому обумовлена рідкістю відомих кіберзагроз у промисловій галузі, сферою відповідальності групи IT-кібербезпеки (що часто пов'язано з організаційними прорахунками керівництва підприємства) й особливостями функціонування підприємства з чітко окресленими ролями.

Інформація про факти вторгнень і їхні наслідки в промисловій сфері досить закрита для широкого загалу й найчастіше невідома багатьом фахівцям. На це впливає імідж великих компаній, вартість їхніх акцій на ринку, біржові спекуляції. До того ж, промислові мережі багато в чому вразливіші за звичайні.

*Про особливості*

Перша особливість промислових мереж — «відкритість». Це пов'язано зі зручністю конфігурації, обслуговування, зміни прикладних програм на мережевих пристроях.

Багато ПЛК мають можливість використання SD-карток для зберігання даних і прикладних програм. Виробники автоматики, поза всяким сумнівом, докладають усіх зусиль для захисту від несанкціонованого доступу до мережевих активів.

Факт наявності великої кількості виробників промислової автоматики викликає питання щодо вразливості вироблених ними пристроїв. Скільки фахівців пройшли через центри розробки цих виробників, чим займаються зараз колишні розробники, до яких даних вони мали доступ? Яку частину робіт виробники довіряють стороннім організаціям, скільки розробників пішли з цих сторонніх організацій? Чи вважають виробники достатньою умовою підписання договорів про нерозголошення з аутсорсерами та співробітниками для впевненості в конфіденційності інформації?

Багато виробників ПЛК і роботів використовують сторонні операційні системи реального часу для свого «заліза». Чи мають вони будь-який контроль за розробниками цих операційних систем? Інші виробники використовують сторонні пристрої на правах ребрендингу. Чи існує взаємодія виробника та його субпідрядників, якщо взяти до уваги плинність кадрів? Цілком зрозуміло, що це питання риторичні, а відносини між виробниками й субпідрядниками регулюються ними самими та бажанням знизити витрати.

Також очевидним є те, що жодних гарантій відсутності витоків інформації не існує за умов сформованих економічних відносин.

Окремо варто відзначити існування в пристроях автоматики «бекдору» виробників для себе, на вимогу спецслужб, і доступу до такої інформації, хоч і обмеженої, але все ж чималої кількості фахівців. У процесі атаки HatMan зловмисник отримав доступ до контролера саме за допомогою привілейованого профілю користувача, що використовувався (ймовірно) техпідтримкою виробника. Зрозуміло, що службова і комерційно важлива інформація разом із її носіями «блукають» на ринку.

Частина підприємств, особливо із безперервним технологічним циклом (process industry), використовують проектні відділи або виділених партнерів-виробників DCS (розподілених систем керування) для впровадження, підтримання

систем автоматики й візуального контролю, для зміни технологічних процесів. Отже, сторонні організації зі своїми співробітниками, плинністю кадрів мають доступ до промислової мережевої структури. Те саме стосується й системних інтеграторів, які впроваджують системи керування і SCADA на виробництві.

Найчастіше використовується машинобудівне обладнання з вмонтованими пристроями автоматики із закритим доступом для захисту алгоритмів керування, що є інтелектуальною власністю. Крім відомих проблем із «непрозорістю» роботи, діагностикою в разі поломок, такі системи обслуговує тільки персонал виробника. Найчастіше, однією з умов гарантії є віддалений контроль за роботою механіки (вібрація й температура підшипників) з боку виробника. Це призводить до виникнення «сліпих зон» у мережі, до яких доступ фахівцям АСК ТП обмежено.

Тож, незважаючи на всі заходи безпеки, що вживаються службою безпеки підприємства, ІБ, фахівцями АСК ТП, промислова мережа підприємства зовсім не є впевнено «закритою знизу». Приклад прибрати STUXNET показує цілком успішну атаку на фізично ізольований від зовнішніх мереж об'єкт.

Цільові кібератаки, як показав HatMan, з боку скомпрометованої IT-мережі підприємства також цілком можливі, незважаючи на використання фахівцями ІБ широких засобів — антивірусів, міжмережевих екранів, засобів керування подіями SIEM, запобігання та виявлення вторгнень IDS/IPS тощо.

Окремо існують бездротові рішення. Поза всяким сумнівом, вони допомагають значно економити завдяки відсутності кабельно-провідникової продукції. Однак, незважаючи на різні заходи щодо шифрування даних, питання залишається відкритим. Крім того, багато сумнівів викликає доступ до вбудованих веб-серверів промислових пристроїв (наприклад, до перетворювачів частоти) по вбудованому комунікаційному модулю Wi-Fi.

Усі ці обставини досить безрадісно характеризують картину безпеки мереж АСК ТП.

Велика кількість різних пристроїв, найчастіше різних виробників, різні комунікаційні протоколи, інтегровані до єдиної системи з величезним числом точок входу для потенційних вразливостей, «сліпі зони», різнорідність типів пристроїв і їхніх виробників роблять промислову мережу потенційно небезпечною. Усе це вимагає найсучасніших підходів і засобів контролю вразливостей.

*Про протидію*

Одним з ефективних методів протидії промисловим кіберзагрозам є спеціалізовані системи контролю вразливостей, розроблені для промислових систем автоматизації.

У портфоліо одного з найбільших дистриб'юторів у галузі IT-безпеки, компанії Softprom by ERC, такі системи представлено рішеннями Indegy і Cyberbit.

Крім традиційних вимог щодо контролю з'єднань, визначення аномалій і вразливостей за базою даних сигнатур, такі системи мають працювати зі спеціалізованими промисловими протоколами.

Відкритість промислових протоколів дає змогу забезпечити доступ до кожного мережевого активу (ПЛК, перетворювача частоти, приладу КВП, операторської панелі тощо). Кращі зразки таких систем можуть повністю контролювати версію FW, оновлення, цілісність прикладної програми і факт її

зміни будь-яким чином (мережевим оновленням, оновлення безпосередньо на ПЛК прямим підключенням програматора, через флеш-картку).

На додачу можна переглядати поточний стан контролера, стан цифрових та аналогових входів/виходів. Усе це дає змогу визначати цілісність внутрішнього середовища пристрою, успішні та безуспішні спроби змінити прикладну програму контролера, мережеві пристрої захисту й керування в енергомережі. Можливість розуміти промислові протоколи, як-от Profinet, Ethernet/IP, Modus за TCP/IP, EtherCAT, IEC61850 тощо, і змога не тільки контролювати програмну цілісність мережевих пристроїв, але й здійснювати інвентаризацію мережевих активів — перший крок до усвідомленої побудови системи кібербезпеки промислової мережі.

Останнім «кордоном» захисту від атак із боку IT-мережі підприємства й нижнього сегмента периметра є спеціалізовані засоби виявлення/запобігання кіберзагроз мереж АСК ТП. Це важливий інструмент, оскільки цільова атака цілком може пройти міжмережеві екрани та досягти критичного об’єкта в нижніх сегментах промислової мережі.

Найбільшу стурбованість також викликає невизначено довга присутність зловмисників у промисловому сегменті мережі. Досвід показує, що невиявлена компрометація мережі впродовж тривалого часу з неактивованими експлойтами — доволі типова ситуація. Тому рішення на базі спеціалізованих засобів виявлення/запобігання кіберзагрозам дають змогу не тільки виявляти потенційні вразливості (неоновлене FW, активи без паролів тощо), але й виявити загрози нульового дня за фактом несанкціонованого помилкового оновлення прикладної програми або мережевого пристрою.

Окремо потрібно сказати про платформу створення помилкових цілей DDP (Distributed Deception Platform), що дає змогу розгорнути мережу підроблених й особливо привабливих для зловмисників пристроїв-приманок, які практично не відрізняються від реальних.

Використання доступної на пастках неправдивої інформації, як-от паролі, мережеве оточення, закладки, файли користувачів і конфігурації систем, практично з 99 % ймовірністю дає змогу виявити зловмисне проникнення. У технологічній мережі розгортають імітації ПЛК, серверів SCADA й інших мережевих активів, а також є можливість виділити реальний пристрій, що є найбільш привабливою пасткою. Пастки фактично є датчиками проникнення.

У компанії Softprom by ERC подібну систему представлено рішенням TrapX Security.

Усі три згадані рішення (Indegy, Cyberbit, TrapX Security) у поєднанні з іншими заходами значно підвищують рівень безпеки згідно зі стандартами NERC CIP, NIST 800-82, IEC62443.

Популярна концепція

Німецьку ініціативу — концепцію Промисловість 4.0 — активно підтримали виробники та експерти з автоматизації виробництва в усьому світі. Вона передбачає загальні напрями модернізації та розвитку цифрового виробництва. Безсистемна цифровізація економіки поставлена в межі планового розвитку.

Кібербезпека й концепція Промисловості 4.0 тісно пов’язані цифровізацією виробництва. Спроби ізолювати промислові мережі в межах цифровізації, що

постійно прискорюється, і, особливо, з усе більш поширеним упровадженням систем керування виробничими процесами MES (manufacturing execution system) і її інтеграцією з ERP і SCADA є просто наївними ілюзіями.

*Рішення для збільшення рівня кібербезпеки*

Межі розвитку автоматизації виробництв, використання промислового IoT, перехід сервісів у хмари, насичення промислових мереж цифровими пристроями польового рівня створюють додаткові точки входу потенційних промислових кіберзагроз. Велика кількість інформації про існування загроз і брак достовірної інформації про деталі кібератак, приховування багатьма підприємствами фактів збитків від них, розуміння масштабу загроз і відсутність розуміння, що потрібно робити, широкий вибір рішень із суперечливими описами можливостей роблять картину нечіткою й найчастіше не дають змоги ухвалити зважене рішення — у який спосіб можна захистити промислову мережу. Погіршує ситуацію роз'єднаність фактів успішних атак без подробиць про системи кіберзахисту, які застосовували постраждалі, або їхня відсутність. На жаль, 80 % компаній приховують навіть сам факт кібератак, не кажучи вже про те, щоб поділитися подробицями.

Успішно боротися з кіберзагрозами, що постійно ускладнюються й розвиваються, допоможе застосування комплексу передових рішень для безпеки мереж АСК ТП.

Широкі можливості зі збільшення рівня кібербезпеки мереж АСК ТП представлені рішеннями Indegy, Ciberbit, TrapX Security в портфелі одного з найбільших дистриб'юторів у сфері IT-безпеки — Softprom by ERC.» ***(Ксенія Матроскіна. Сучасні рішення кіберзахисту в мережах АСК ТП // ERC™ (https://erc.ua/erc-reviews/21043/suchasni-rishennia-kiberzakhistu-v-merezhakh-ask-tp/). 30.12.2019).***

***

## ***Діяльність хакерів та хакерські угруповування***

---

**«Російські хакери навчились зламувати акаунти в месенджері Telegram, використовуючи для цього СМС-коди, які приходять при вході з нового пристрою**…

Кілька підприємців повідомили про те, що невідомі отримали доступ до їхнього листування в Telegram. При цьому, з проблемою зіткнулися користувачі як iOS, так і Android.

Атака на смартфон починалася з того, що користувачеві приходило повідомлення від сервісного каналу Telegram (офіційного каналу з галочкою верифікації) з кодом підтвердження, який сам користувач не запитував. Після цього користувач отримував СМС-повідомлення з таким же кодом підтвердження і практично відразу ж – повідомлення про те, що в його обліковий запис зроблений вхід з нового пристрою в Самарі.

Щоб зламати чужий обліковий запис, зловмисники самі ініціюють запит на відправку месенджером СМС з кодом активації, потім перехоплюють це СМС і

використовують отриманий код для успішної авторизації в месенджері, пояснюють в Group-IB. Таким чином вони отримують доступ до всіх даних користувача, у тому числі секретних чатів і фотографій, що зберігаються в месенджері.

Для того, щоб отримати доступ до СМС, хакери можуть використовувати спеціальні технічні засоби або інсайди в операторах зв'язку. У Group-IB поки не з'ясували, яким ПО користуються злочинці, але на хакерських форумах в даркнеті з'явилися оголошення про продаж доступу до месенджерів. Наприклад, за 100 тисяч рублів пропонують придбати доступ до всього листування людини в WhatsApp, Telegram або Viber в режимі онлайн протягом двох-чотирьох днів. А за 350 тисяч рублів можна отримати доступ до всієї вилученої із месенджера інформації. У цьому випадку зловмисники будуть користуватися допомогою "співробітників спецслужб"…» ***(Російські хакери знайшли спосіб зламати акаунти в Telegram // Дзеркало тижня. Україна (https://dt.ua/TECHNOLOGIES/rosiyski-hakeri-znayshli-sposib-zlamati-akaunti-v-telegram-331848_.html). 04.12.2019).***

***

**«В России хакеры использовали зараженные ресурсы государственных компаний для майнинга криптовалют, сообщил замдиректора Национального координационного центра по компьютерным инцидентам (НКЦКИ) Николай Мурашов.**

«Выявлены случаи майнинга криптовалюты с помощью зараженных информационных ресурсов государственных организаций. В этом случае злоумышленники заражают веб-страницы, а майнинг осуществляется в момент их просмотра в браузере», – пояснил Мурашов, передает ТАСС.

По его словам, стоимость большинства криптовалют очень большая, поэтому желающих заработать очень много.

«Для генерации виртуальных монет может использоваться до 80% свободной мощности компьютера, причем легальный пользователь может даже об этом не знать», – пояснил он.

Захваченные майнерами серверы крупных компаний могут сильно снизить свою производительность, что приведет к значительному ущербу для бизнеса, добавил Мурашов.

Он пояснил, что в России за последнее время двоих граждан привлекли к ответственности за использование захваченных компьютеров для майнинга криптовалют.

Для обеспечения безопасности пользователям нужно больше уделять внимания защите своих ПК, подчеркнул специалист.

Также он пояснил, насколько выросла опасность от DDoS-атак в России.

«Ежегодно количество DDoS-атак с усилением увеличивается на четверть, а используемых для этого объектов – на треть», – отметил замглавы центра.

Для усиления мощности атак стали использовать ресурсы интернета, это называется методом амплификации, сказал Мурашов.

Вместе с тем он отметил, что НКЦКИ и операторы связи в текущем году не допустили кибератак, которые могли бы негативно повлиять на систему государственного управления и экономику…

Такая работа ведется вместе с российскими операторами связи и компаниями в сфере информационной безопасности.

В 2019 году прекращена работа 12 тыс. зарубежных вредоносных ресурсов, использовавшихся для кибератак против России…» ***(Алексей Дегтярев. Хакеры использовали зараженные ресурсы российских госкомпаний для майнинга // Деловая газета «Взгляд» (https://vz.ru/news/2019/12/16/1013908.html). 16.12.2019).***

***

**«Киберпреступная группировка Lazarus, предположительно спонсируемая государством Северной Кореи, разработала новое троянское ПО, предназначенное для атак на Linux- и Windows-системы…**

По словам исследователей из компании Qihoo 360 Netlab, Lazarus не только приобрела инструменты у других преступников, но также разработала собственный RAT, получивший название Dacls.

Команда специалистов провела анализ образцов вредоносного ПО и пришла к выводу, что оно представляет собой полностью функциональный RAT для ОС Windows и Linux. В то время как образец для Windows динамически загружается через удаленный URL-адрес, версия для Linux компилируется напрямую и включает шесть общих модулей для выполнения команд, управления файлами и процессами, тестирования доступа к сети, сканирования сети и соединения с C&C-сервером.

Как предполагают эксперты, для заражения систем и загрузки Dacls киберпреступники эксплуатируют уязвимость (CVE-2019-3396) удаленного выполнения кода в Widget Connector в сервере Atlassian Confluence (версии 6.6.12 и ниже).

Dacls является модульным вредоносным ПО и использует TLS- и RC4-шифрование при взаимодействии со C&C-сервером, а также AES-шифрование для защиты файлов конфигурации. Как только версия для Linux попадает на целевую систему, вредонос начинает работать в фоновом режиме и проверяет наличие обновлений. Затем Dacls распаковывает и расшифровывает свой файл конфигурации и подключается к C&C-серверу. RAT может выполнять такие действия, как кража, удаление и выполнение файлов, сканирование структур каталогов, загрузка дополнительных полезных нагрузок, отключение системных процессов, создание процессов демона и загрузка данных, в том числе результаты сканирования и выполнения команд». ***(Группировка Lazarus атакует Linux-системы с помощью нового вредоноса Dacls // SecurityLab.ru (https://www.securitylab.ru/news/503518.php). 17.12.2019).***

***

**«Киберпреступная группировка Lazarus Group, предположительно спонсируемая государством Северной Кореи, арендовала вредоносные инструменты и доступ к взломанным сетям у операторов ботнета TrickBot.**

Киберпреступники также вооружились новым набором инструментов, получившим название Anchor. Он представляет собой новую разновидность вредоносного ПО и предоставляется в виде модуля TrickBot.

По словам исследователей из компании SentinelOne, вредонос Anchor создан для преступников, которые хотят оставаться в тени и избегать обнаружения в ходе атак. Данный инструмент может использоваться в атаках, нацеленных на крупные корпорации, где злоумышленникам необходимо оставаться незамеченными в течение нескольких недель или месяцев, пока они похищают данные, и даже на протяжении длительного времени после прекращения атак, отметили эксперты.

Anchor состоит из различных подмодулей, предоставляющих различные функции для целевых атак, включая перемещение в сети, возможность установки бэкдоров для последующего доступа, функции для целевых PoS-систем, извлечение данных платежных карт из оперативной памяти и очистку системы от следов заражения.

Как сообщили эксперты, Lazarus Group арендовала доступ к зараженной системе через ботнет TrickBot, а затем использовала инструмент Anchor для установки бэкдора PowerRatankba в сети взломанной компании. Исследователи не пояснили, какие именно цели преследовали преступники…» ***(APT Lazarus Group арендовала вредоносное ПО у операторов TrickBot // SecurityLab.ru (https://www.securitylab.ru/news/503387.php). 12.12.2019).***

***

**«Команда исследователей из Microsoft Threat Intelligence Center (MSTIC) предупредила о продолжающихся атаках киберпреступной группировки GALLIUM, направленных на телекоммуникационных провайдеров в Юго-Восточной Азии, Европе и Африке.** Злоумышленники эксплуатируют уязвимости в сервере приложений с открытым исходным кодом WildFly (ранее JBoss Application Server).

Проникнув в сеть компании, преступники начинают собирать учетные данные с использованием распространенных инструментов и TTP (тактик, методов и процедур). Они используют скомпрометированные учетные данные и утилиту PsExec для перемещения в сети и выполнения процессов на других системах.

«Операторы полагаются на дешевую и легко заменяемую инфраструктуру, которая состоит из DNS-доменов и повторно используемых точек перехода», — пояснили исследователи.

В числе инструментов GALLIUM, выявленных экспертами во время прошлых кампаний, есть HTRAN (перенаправление пакетов), Mimikatz и Windows Credential Editor (восстановление токенов авторизации), NBTScan (для обнаружения DNS-серверов NETBIOS в локальной или удаленной сети), Netcat (чтение и запись с использованием TCP- или UDP-протоколов), PsExec (удаленное выполнение команд на системе), а также WinRAR.

С помощью web-оболочек преступники обеспечивают персистентность на целевой системе и загружают полезную нагрузку.

В дополнение к бэкдору China Chopper, группировка использует созданный на его основе web-шелл BlackMould для различных целей и задач, включая поиск локальных дисков, выполнение основных файловых операций, настройку атрибутов файла, эксфильтрацию и удаление файлов, а также выполнение вредоносных команд на скомпрометированных устройствах.

В рамках второго этапа группировка загружает модифицированные версии вредоносов Gh0st RAT и Poison Ivy, разработанные для предотвращения обнаружения.

Как отметили специалисты, вместо разработки собственных вредоносных программ, GALLIUM изменяла чужие инструменты для повышения эффективности атак». ***(GALLIUM атаковала крупные телекоммуникационные компании по всему миру // SecurityLab.ru (https://www.securitylab.ru/news/503417.php). 13.12.2019).***

***

**«Исследователи по безопасности обнаружили, что в недавней серии атак хакерская группа, связанная с правительством Китая, сумела обойти двухфакторную аутентификацию (2FA — two-factor authentication).** В нападениях обвиняют группировку, известную как APT20, которая, как полагают специалисты голландской фирмы по кибербезопасности Fox-IT, действует по указу Пекина.

В отчете Fox-IT говорится, что хакерская группа начала свою деятельность в 2011 году, после чего исследователи по безопасности потеряли ее след. Однако в 2018 году они снова обнаружили признаки незаконной деятельности хакеров. Так, в отчете Fox-IT сообщается, чем занималась группа последние два года. Эксперты напрямую не обвиняют хакеров в сотрудничестве с правительством КНР. Это лишь предположения и догадки. Прямых доказательств этого факта нет.

В частности, основное внимание уделялось Jboss, платформе корпоративных приложений, которую обычно используют члены правительства. APT20 использовала уязвимости для проникновения на серверы, взламывая веб-оболочки.

По заявлению Fox-IT, ее специалистам удалось найти доказательства того, что китайская хакерская группировка APT20 получила доступ к учетным записям VPN, защищенных двухфакторной авторизацией. Как им удалось это сделать, остается неясным. В теории, хакеры похитили программный токен RSA SecurID, который впоследствии позволил создавать одноразовые коды для обхода защиты.

Основными целями киберпреступников были поставщики управляемых услуг (MSP) и государственные органы. Не меньший энтузиазм они проявляли в деле похищения интеллектуальной собственности в таких сферах как финансы, авиация, энергетика, здравоохранение и прочие». ***(Китайские хакеры научились обходить двухфакторную аутентификацию // PaySpace Magazine (https://psm7.com/technology/kitajskie-xakery-nauchilis-obxodit-dvuxfaktornuyu-autentifikaciyu.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Payspacemagazine+%28Payspacemagazine%29). 26.12.2019).***

***

**«Операторы вымогательского ПО Maze создали web-сайт, на котором указаны последние компании-жертвы, решившие самостоятельно восстановить свои компьютерные системы без оплаты выкупа.**

«Представленные здесь компании не хотят сотрудничать с нами и пытаются скрыть нашу успешную атаку на их ресурсы. Ждите их базы данных и личные документы здесь. Следите за новостями!», — сообщается на сайте вымогателей.

По данным журналиста Брайана Кребса, по крайней мере одна из перечисленных на сайте компаний действительно недавно пострадала от атаки Maze, о которой еще не сообщалось в СМИ. Преступники уже опубликовали данные о жертвах Maze, включая информацию о дате первого заражения, украденные документы Microsoft Office, текстовые и PDF-файлы и сведения об общем объеме файлов, предположительно похищенных у пострадавших (в гигабайтах), а также IP-адреса и имена инфицированных серверов.

Операторы вымогательского ПО в течение многих лет угрожали жертвам опубликовать в Сети похищенные данные, однако они фактически никогда не осуществляли свои угрозы. Похоже, ситуация изменилась после того, как операторы Maze опубликовали в даркнете 700 МБ данных ИБ-компании Allied Universal, отказавшейся платить выкуп…» ***(Вымогатели угрожают публикацией данных жертв, не заплативших выкуп // SecurityLab.ru (https://www.securitylab.ru/news/503500.php). 17.12.2019).***

***

**«Киберпреступники создали специальное программное обеспечение для взлома камер компании Ring, специализирующейся на разработке устройств для «умного» дома.**

Домашние камеры Ring работают с мобильным приложением, позволяющее наблюдать за происходящим в режиме реального времени и использовать динамик для общения через камеру. Как сообщили местные СМИ, злоумышленник взломал камеру Ring в спальне трех молодых девушек в округе Де-Сото, штат Миссисипи, и общался через динамики устройства с одним из детей. Владельцы камеры не настроили двухфакторную аутентификацию для устройства, что значительно облегчило взлом камеры.

На различных форумах в даркнете преступники обсуждают создание инструментов для взлома учетных записей Ring, подключенные к камерам, сообщает Motherboard. Например, в теме Ring Video Doorbell Config идет речь о файле, используемом для управления ПО для быстрого подбора учетных данных для входа в аккаунты. Подобным образом преступники разработали конфигурации для разных web-сайтов и online-сервисов - от Uber до Facebook.

В другой ветке один пользователь форума предлагает инструмент для подбора учетных данных Ring.com за $6.

Компания Ring начала расследование инцидента и настоятельно рекомендует пользователям включить двухфакторную аутентификацию, а также использовать надежные пароли и регулярно менять их…». ***(Преступники создали***

***инструменты для взлома камер Ring // SecurityLab.ru (https://www.securitylab.ru/news/503398.php). 13.12.2019).***

***

**«От атак NotPetya в 2017 году значительный ущерб понесли ряд компаний, однако не сообщили о заражении.** Об этом заявил директор по информационной безопасности Maersk Эндрю Пауэлл (Andrew Powell) на конференции Black Hat Europe 2019, состоявшейся в Лондоне.

Считается, что вымогательское ПО NotPetya являлось ключевым элементом в масштабной кампании, направленной на правительство Украины. В качестве вектора заражения использовалось финансовое приложение M.E.Doc, которое должны применять компании, ведущие бизнес в стране. Однако, кампания не ограничилась только Украиной, в результате от атак пострадало около 600 предприятий и организаций по всему миру.

Согласно опубликованным отчетам, жертвами NotPetya стали компании почти во всех промышленных отраслях. Например, в США фармацевтическая компания Merck и курьерская компания FedEx в результате атаки потеряли в общей сложности более $300 млн.

По словам Пауэлла, Maersk не была достаточно подготовлена к отражению атаки NotPetya. В начале 2017 года уровень зрелости кибербезопасности компании был относительно низким. Компьютерные сети и серверная инфраструктура не считались критически важными, поэтому цифровые активы были плохо защищены. Таким образом, как только одна из систем Maersk была заражена в одесском офисе, вредонос распространился через глобальную сеть Maersk быстрее, чем кто-либо мог себе представить.

Большая часть ущерба была нанесена за 7 минут, отметил Пауэлл. NotPetya вывел из строя 49 тыс. ноутбуков, более 1 тыс. приложений, привел к отключению всех систем печати и обмена файлами, а также нарушил работу серверов управления облаком VMware vCenter и DHCP и Active Directory. Основная и резервная системы Active Directory также стали бесполезными. В результате Maersk потеряла связь с миллионами морских контейнеров по всему миру и не смогла доставить их по назначению, также были нарушены цепочки поставок по всему миру.

К счастью, во время атаки NotPetya в офисе компании в Лагосе отключилось электричество и его IT-системы, включая копию Active Directory, не пострадали. Узел Lagos AD был извлечен, доставлен в Копенгаген и использован для восстановления остальной части сети». ***(Maersk оказалась не единственной компанией, понесшей значительные убытки от атак NotPetya // SecurityLab.ru (https://www.securitylab.ru/news/503276.php). 10.12.2019).***

***

**«Ранее неизвестный дроппер доставляет на целевые устройства широкий спектр полезной нагрузки.** Зловред, получивший название Legion Loader, не ограничивается установкой коммерческих инфостилеров, а внедряет на Windows-компьютеры собственный скрипт для кражи данных криптокошельков и RDP-бэкдор.

Специалисты компании Deep Instinct зафиксировали атаки с использованием нового загрузчика и подробно описали механизм его работы. Эксперты не сообщили, каким образом дроппер попадает на целевое устройство, однако отметили, что кампания с его участием направлена на пользователей из США и Европы…

По словам исследователей, попав на компьютер, вредоносная программа сначала регистрируется на одном из своих командных серверов. Злоумышленники создали более 30 центров управления и варьируют их от атаки к атаке, чтобы уберечь от блокировки. После установки связи Legion загружает в целевую систему два или три образца полезной нагрузки, среди которых встречаются распространенные инфостилеры Raccoon, Vidar и Predator the Thief, а также другие вредоносные программы.

По мнению ИБ-специалистов, создатели дроппера предоставляют другим злоумышленникам услуги по доставки вредоносного ПО на целевые устройства. Сразу после установки полезной нагрузки Legion запускает PowerShell-скрипт и скачивает собственные вредоносные инструменты. Один из них — бесфайловый инфостилер для сбора учетных данных криптокошельков и сохраненных в браузерах паролей. Похищенные сведения передаются на командный сервер по защищенному каналу, за шифрование которого отвечает отдельная библиотека.

Второй стандартный модуль представляет собой бэкдор, использующий протокол RDP для коммуникации с центром управления. Скрипт упакован как установщик NSIS и закодирован шифром на основе стандарта Base64. Так же как и встроенный инфостилер, он не оставляет следов на диске, работая в рамках PowerShell-оболочки. Исследователи не раскрывают возможностей зловреда, а лишь отмечают, что он регистрируется на инфицированном устройстве как системный процесс…». ***(Maxim Zaitsev. Legion Loader устанавливает инфостилеры и бэкдоры на заказ // Threatpost (https://threatpost.ru/legion-loader-used-in-dropper-for-hire-campaign-to-deliver-infostealers-backdoors/35075/). 20.12.2019).***

***

**«Исследователи из команды nao_sec сообщили о ранее неизвестном эксплойт-паке, получившем название Bottle.** Вредоносный инструмент, ориентированный на японских пользователей, предположительно устанавливает на компьютер жертвы программу для кражи данных. Злоумышленники начали его активно использовать в сентябре этого года, а свежие данные о новой эксплойт-кампании появились у экспертов в начале декабря.

*Как проходит атака Bottle*

Эксплойты Bottle попадают на компьютер жертвы через рекламное объявление, которое ведет на страницу, загружающую два JavaScript-сценария. Первый предназначен только для получения кода установщика с командного сервера. Второй содержит многократно обфусцированную полезную нагрузку. Злоумышленники меняют порядок блоков, а также комбинируют методы Base64, URL Encode и RC4, чтобы обойти антивирусные фильтры.

Далее вредоносный скрипт выполняет ряд проверок, чтобы убедиться в правильности выбранной цели: определяет язык системы, ищет на устройстве браузер Internet Explorer, а также следы предыдущих установок эксплойт-пака.

Если жертва прошла все проверки, Bottle загружает один из трех вариантов полезной нагрузки. Два сценария предназначены для эксплуатации CVE-2018-8174 в 32-разрядной или 64-разрядной версии Internet Explorer. Уязвимость в движке VBScript позволяет атакующему использовать порчу памяти для выполнения стороннего кода в контексте пользователя. Разработчики Microsoft закрыли баг еще в мае 2018 года, однако злоумышленники по-прежнему активно его эксплуатируют.

Третий скрипт использует ошибку use-after-free в медиадвижке Flash Player. Критическая уязвимость CVE-2018-15982 получила заплатку в декабре прошлого года, но еще до этого пополнила арсеналы киберпреступников.

Зловред, загружаемый на машину в результате отработки эксплойта,. является оригинальной разработкой. По мнению ИБ-специалиста Виталия Кремеза (Vitali Kremez), он нацелен на похищение данных у японских пользователей». ***(Egor Nashilov. Эксплойт-пак Bottle атакует японских пользователей // Threatpost (https://threatpost.ru/konnichiwa-bottleek-ek/35036/). 16.12.2019).***

***

**«Независимый ИБ-исследователь Карлос Брендель (Carlos Brendel) обнаружил новую версию IoT-ботнета Echobot. Теперь зловред использует 77 эксплойтов, которые позволяют ему атаковать разнообразные сетевые устройства — от роутеров и IP-телефонов до NAS-хранилищ и аналитических платформ.**

Первые образцы Echobot появились в начале июня и имели на борту 18 различных эксплойтов. Уже через неделю это число выросло до 26, а к концу лета превысило 60. Зловред атакует практически все известные платформы, включая ARM, x86 и PPC.

По словам экспертов, Echobot не представляет серьезной опасности — операторы добавляют в код уже известные эксплойты из публичных репозиториев. О некоторых уязвимостях ИБ-специалисты знают еще с 2003 года, а в других случаях злоумышленники пытаются атаковать малопопулярные платформы, не задумываясь об эффективности ботнета.

По мнению экспертов, злоумышленники копируют весь вредоносный код, который находят онлайн, не пытаясь в нем разобраться. В результате, например, попытки Echobot атаковать MIPSL-хосты заканчиваются неудачей из-за ошибки в пути размещения дроппера.

В то же время эксперты допускают, что Echobot может представлять угрозу для устаревших устройств, которые остаются уязвимыми по недосмотру разработчиков или администраторов.

Как ранее установили исследователи, проблемы могут годами кочевать из одного продукта в другой из-за того, что программисты продолжают использовать одни и те же уязвимые библиотеки. Это особенно актуально для многих промышленных решений, поскольку их создатели нередко пренебрегают рекомендациями по безопасной разработке.

Тем не менее специалисты рекомендуют администраторам обратить внимание на новую волну активности Echobot и удостовериться в защищенности своих устройств. По словам Бренделя, он зафиксировал попытки распространения ботнета с 10 различных устройств». ***(Egor Nashilov. IoT-ботнет Echobot обновил список целей // Threatpost (https://threatpost.ru/echobot-hits-77-exploits/35029/). 16.12.2019).***

***

**«Аналитики «Лаборатории Касперского» опубликовали финальную статистику по киберугрозам 2019 года.** В отчетный период зловредные программы атаковали каждого пятого пользователя под защитой решений Kaspersky, а общее количество отраженных атак превысило 975 млн. Продукты компании также зафиксировали почти 274 млн вредоносных URL.

Данные были собраны анонимно с согласия пользователей «Лаборатории Касперского» в более чем 200 странах мира. Для сбора информации исследователи использовали ресурсы облачной службы Kaspersky Security Network, которая отслеживает и блокирует атаки на частных и корпоративных компьютерах.

*Самые распространенные зловреды*

Попытки установки банковских троянов были обнаружены на компьютерах у 766,7 тыс. пользователей. Как и в прошлом году, первое место по распространенности занял ZeuS — на него пришлось 23% атак. На второй строчке рейтинга с небольшим отставанием оказался зловред RTM (22%), известный частыми атаками на российские организации. В первую пятерку также вошли Emotet (12%), SpyEye (7%) и Nymaim (6%).

Активность шифровальщиков в 2019 году оказалась сравнима с банковскими зловредами. Защитные системы Kaspersky отразили атаки вымогателей на машинах 755,5 тыс. пользователей. Эксперты компании насчитали в отчетный период более 46 тыс. модификаций шифровальщиков и обнаружили 22 новых семейства.

В десятку самых распространенных зловредов этого типа попали пять программ, которые удалось идентифицировать с помощью облачных систем безопасности. Это означает, что преступники успевают создавать новые модификации ПО до того, как они попадают в базы сигнатур. В такой ситуации пользователям необходимо использовать проактивные средства защиты, способные выявлять опасную активность по косвенным признакам.

Первую строчку в рейтинге шифровальщиков продолжает занимать WannaCry. Зловреды этого семейства обеспечили около 24% атак на пользователей Kaspersky. Вымогатель GandCrab, который формально сошел с арены в 2019 году, замыкает топ-3 в своем классе. Шифровальщики Shade, PolyRansom/VirLock и Stop разместились в нижней половине рейтинга.

В то же время эксперты отметили снижение активности, связанной со скрытой добычей криптовалют. «Хотя в топ-20 есть несколько таких вердиктов, количество детектов JavaScript-майнеров и попыток подключения к майнинговым сайтам значительно снизилось по сравнению с 2018 годом», — подчеркнули исследователи.

*Наиболее опасные уязвимости*

Среди ключевых трендов 2019 года аналитики выделили рост количества целевых атак с использованием уязвимостей нулевого дня. Такие баги, как CVE-2018-8611, CVE-2019-0797, CVE-2019-0859, были обнаружены уже после того, как их взяли на вооружение продвинутые кибергруппировки.

Вторая заметная тенденция — это все более активное применение эксплойтов Microsoft Office. Их популярность стала расти еще в 2018 году, и сегодня эти приложения чаще всего подвергаются атакам. Список самых распространенных уязвимостей за год не изменился; все они позволяют удаленно выполнить сторонний код:

CVE-2017-11882, CVE-2018-0802 — содержатся в устаревшем редакторе формул;

CVE-2017-8570 — связана с некорректной обработкой объектов в памяти приложениями Office;

CVE-2017-0199 — обеспечивает полный доступ к системе без каких-либо действий со стороны пользователя, открывшего вредоносный документ.

Уязвимости протокола SMB вроде EternalBlue и EternalRomance также не теряют своей популярности у преступников. Кроме того, сетевые службы постоянно находятся под атаками методом подбора паролей.

Аналитики также отметили несколько уязвимостей, которые были обнаружены в 2019 году. По их словам, наибольшая опасность связана с ошибками подсистемы удаленных рабочих столов, которые получили названия BlueKeep и DejaBlue. Риски несколько снижает тот факт, что для использования этих багов необходима серьезная техническая подготовка, но атаку можно масштабировать, и последствия подобной эксплойт-кампании могут оказаться катастрофическими». ***(Maxim Zaitsev. Эксперты Kaspersky подвели итоги года по киберугрозам // Threatpost (https://threatpost.ru/kaspersky-stats-on-malware-2019/35027/). 13.12.2019).***

***

**«Специалисты IBM X-Force обнаружили ранее неизвестный зловред, используемый в целевых атаках на Ближнем Востоке.** Программа, получившая название ZeroCleare, доставляется на устройство при помощи вредоносного инструмента для обхода механизма проверки подписи драйверов. Вредонос перезаписывает загрузочный сектор диска и делает дальнейшую работу компьютера невозможной. Эксперты предполагают, что за атаками стоит проправительственная иранская группировка OilRig.

Вайпер нацелен на системы под управлением Windows. Поскольку 64-разрядная версия ОС имеет встроенную защиту от установки неподписанных драйверов, злоумышленники применяют утилиту Turla Driver Loader (TDL), которая обходит этот механизм. Загрузчик доставляет на компьютер скомпрометированный драйвер VBoxDrv с легитимной цифровой подписью и инжектом для запуска шелл-кода на уровне ядра.

На заключительном этапе атаки ZeroCleare устанавливает в целевую систему легитимную утилиту EldoS RawDisk, при помощи которой стирает MBR-сектор жесткого диска. Драйвер EldoS не имеет подписи разработчика Windows и устанавливается под прикрытием TDL. Киберпреступники используют тактику

living-off-the-land, применяя системные процессы Windows, а также PowerShell-сценарии, чтобы оставаться незамеченными на инфицированной машине и заражать другие устройства, подключенные к домену.

Анализ также показал некоторое сходство новой вредоносной программы с вайпером Shamoon, ранее тоже замеченным в атаках на арабские страны в Персидском заливе. Как выяснили ИБ-специалисты, IP-адреса, засветившиеся в кампании ZeroCleare, уже использовались OilRig для других нападений. Эксперты также нашли веб-консоль, схожую с утилитой TWOFACE/SEASHARPEE по способу вызова методов сборки, алгоритму шифрования и стилю именования переменных. При этом у аналитиков есть доказательства участия в атаках еще как минимум одной проиранской группы хакеров…». ***(Maxim Zaitsev. Вайпер ZeroCleare атакует цели на Ближнем Востоке // Threatpost (https://threatpost.ru/new-zerocleare-wiper-targets-energy-industrial-organizations-in-the-middle-east/34973/). 05.12.2019).***

***

## *Операції правоохоронних органів та судові справи проти кіберзлочинців*

---

**«Гражданин РФ Антон Б., обвиняемый властями США в кибермошенничестве на $1,5 млрд, готовится дать признательные показания.**

Антон Б., также известный под псевдонимом Kusok, обвиняется во взломе компьютеров, краже личности при отягчающих обстоятельствах и других связанных преступлениях, совершенных с июня 2014-го по ноябрь 2016 года.

Согласно обвинению, опубликованному в апреле нынешнего года, россиянин вместе с группой соучастников «зарабатывал» на незаконных налоговых возвратах. Через уязвимость в бухгалтерском ПО преступники взламывали компьютеры в американских компаниях, занимающихся подачей заявлений на возврат налогов от имени своих клиентов. Мошенники меняли персональную информацию налогоплательщиков, в результате чего переплаченные налоги возвращались не им, а на дебетовые карты мошенников.

Россиянин был арестован в Таиланде в ноябре 2017 года, а затем экстрадирован в США. Согласно письменному обращению адвоката к судье от 15 декабря нынешнего года, в настоящее время защита «улаживает некоторые вопросы» с прокуратурой и готовится к даче ее клиентом признательных показаний 3 февраля 2020 года.

За все предъявленные обвинения россиянину в сумме грозит 27 лет тюрьмы». ***(Обвиняемый в краже $1,5 млрд россиянин признает свою вину // SecurityLab.ru (https://www.securitylab.ru/news/503499.php). 17.12.2019).***

***

**«Сотрудники Федерального бюро расследований США задержали в Лас-Вегасе владельцев крупнейших в стране нелегальных стриминговых сервисов iStreamItAll и Jetflix.** Как сообщило ведомство Министерства юстиции США,

iStreamItAll насчитывал больше подписчиков, чем Netflix, Amazon Prime, Hulu и Vudu вместе взятые.

36-летний Дэррил Поло (Darryl Polo) и 40-летний Луис Вилларино (Luis Villarino) признали себя виновными в обвинениях в нарушении авторских прав за использование iStreamItAll и Jetflix. Контент сайта iStreamItAll содержал примерно 118 тыс. эпизодов телесериалов и 11 тыс. фильмов.

Согласно документам, Поло призывал по электронной почте подписчиков iStreamItAll отменить лицензионные услуги в пользу пиратского сервиса. Обвиняемый также признал, что заработал $1 млн с помощью нелегального стриминга, а также скачивал контент с торрент-сайтов.

Поло также работал в нескольких других пиратских сервисах, в том числе SmackDownOnYou. Он также признал себя виновным по обвинению в отмывании денег. Поло и Вилларино вместе управляли сервисом Jetflix, насчитывающим десятки тысяч платных подписчиков по всей территории США. Оба разработчика признались в использовании «автоматизированных программ и других инструментов для поиска, загрузки, обработки и хранения нелегального контента, чтобы затем данный материал стал доступным на серверах в США и Канаде». ***(ФБР закрыло крупнейшие в США нелегальные стриминговые сервисы // SecurityLab.ru (https://www.securitylab.ru/news/503464.php). 16.12.2019).***

***

**«Участник русскоязычной киберпреступной группировки, занимавшейся распространением вымогательского ПО Reveton, приговорен в Великобритании к шести годам лишения свободы и штрафу в размере $355 тыс.**

Как сообщило Национальное агентство по борьбе с преступностью Великобритании в понедельник, 10 декабря, житель графства Эссекс Зайн Кайсер (Zain Qaiser) признался, что являлся участником киберпреступной группировки, и в апреле нынешнего года был отправлен в исправительное учреждение.

По данным следствия, 25-летний студент в течение шести лет был связан с нашумевшей группировкой Lurk. Его роль заключалась в том, чтобы под видом представителя легитимных компаний покупать на порнографических и эротических ресурсах рекламные площади, использовавшиеся для распространения вредоносного ПО.

Кликнув на рекламу, жертва попадала на мошеннический сайт с вредоносным ПО, в том числе с Reveton. Вредонос блокировал систему и отображал поддельное уведомление от правоохранительных органов о нарушении пользователем закона. Во избежание наказания жертва якобы должна заплатить штраф в размере $300-1000, и тогда ее компьютер будет разблокирован. В период активности группировка заразила вредоносным ПО миллионы компьютеров в 20 странах мира.

Как сообщают британские правоохранительные органы, согласно налоговым декларациям, Кайсер имел нулевой доход, однако при этом вел роскошный образ жизни. Преступник останавливался в дорогих отелях, тратил деньги на наркотики и азартные игры. Он был арестован в 2014 году, но затем отпущен за недостатком доказательств. В 2017 году против Кайсера были выдвинуты обвинения, в итоге приведшие к его заключению под стражу». ***(В Великобритании участник Lurk***

***получил 6 лет тюрьмы // SecurityLab.ru (https://www.securitylab.ru/news/503322.php). 11.12.2019).***

***

**«Европол совместно с правоохранительными органами Колумбии, Австралии и ряда других стран пресек распространение трояна Imminent Monitor.** Киберполицейские добились отключения серверов проекта, который позиционировался как легитимная утилита, однако обладал всеми функциями RAT-трояна.

По информации следователей, вредоносную программу приобрели более 14 тыс. пользователей, распространявших ее в 124 странах, но участники криминальных форумов говорят о вдвое большем тираже приложения…

Зловред Imminent Monitor существует в Сети с 2013 года, однако наибольшую известность приобрел пару лет назад, после ухода с рынка нескольких ключевых игроков. Не последнюю роль в росте популярности трояна сыграла его цена — любой желающий мог приобрести RAT-утилиту за $25. Создатели программы представляли ее как средство удаленного администрирования, однако рекламировали свою разработку на хакерских форумах и других ресурсах в даркнете.

Зловред, установленный на целевое устройство, давал атакующему возможность:

получать изображения с веб-камер;

перехватывать работу с клавиатурой;

удаленно подключаться к рабочему столу жертвы;

похищать логины и пароли из множества приложений;

прослушивать разговоры в реальном времени через микрофон компьютера;

использовать инфицированную машину в качестве прокси-сервера.

Как проходила операция по блокировке RAT-утилиты

В апреле этого года пользователи одного из хакерских форумов заметили, что автор программы, скрывавшийся под псевдонимом Shockwave, долгое время не появляется на ресурсе. Участники криминального сообщества предположили, что деятельностью злоумышленника заинтересовались правоохранительные органы. Эта информация подтвердилась, когда у покупателей Imminent Monitor стали проходить обыски.

Как сообщили представители Европола, активная фаза операции началась летом 2019 года, когда киберполицийские Австралии и Бельгии получили ордеры на арест создателя зловреда и одного из его помощников. В данный момент задержаны 13 наиболее активных пользователей трояна, изъято 430 устройств, проводится экспертиза остального оборудования, полученного в ходе рейдов. Следственные действия прошли в Чехии, Великобритании, Колумбии, Польше, Испании, Швеции и Нидерландах.

Бэкенд-серверы сайта вредоносной программы отключены — теперь по адресу криминального веб-ресурса размещено сообщение о его блокировке. По словам представителей правоохранительных органов, покупатели Imminent Monitor более не смогут использовать приложение…». ***(Maxim Zaitsev. Киберполиция***

***заблокировала троян Imminent Monitor // Threatpost (https://threatpost.ru/europol-international-operation-takes-down-imminent-rat-infrastructure/34946/). 02.12.2019).***

***

**«Уполномоченные по делам кибербезопасности Франции обратились в Генпрокуратуру Украины с просьбой помочь в поимке опасных хакеров, запустивших вирус, терроризирующий весь мир.** Удалось установить, что IP-адреса некоторых замешанных лиц принадлежат Украине…

Согласно данным, речь идет о группе хакеров, запустивших вредоносное ПО-вымогатель LockerGoga, которое атаковало крупные производственные предприятия во Франции, Америке, Норвегии и других странах мира. Вирус блокирует работу компании, зашифровывая файлы на устройствах. Взамен на разблокировку злоумышленники требовали у предприятий крупный денежный выкуп.

В связи с этим французские правоохранители передали в украинскую Генпрокуратуру информацию о почтовых ящиках и IP-адресах, через которые, вероятно, происходило заражение. Сотрудникам Киберполиции Украины удалось установить четырех возможных фигурантов дела.

После этого у суда был запрошен доступ к данным обладателей указанных французами почтовых ящиков, в частности, к использованным услугам и маршрутам передачи. Однако шансы на то, что хакеры при атаке использовали реальные ящики — мизерный…». ***(Французы обвинили украинских хакеров в войне против всего мира // SecureNews (https://securenews.ru/frantsuzi-obvinili-ukrainskih-hakerov/). 18.12.2019).***

***

**«Статистичні показники злочинів, здійснюваних у кіберпросторі, які постійно зростають, демонструють недостатню ефективність механізмів протидії кіберзлочинності, оскільки транскордонний характер високотехнологічних злочинів унеможливлює ефективну боротьбу з ними в рамках лише національних правових систем. Саме тому, починаючи з кінця XX ст. держави розпочали процес кооперації в рамках різних міжнародних організацій для протидії загрозам, що несуть в собі новітні технології.**

Центральне місце у цьому процесі займає Організація Об'єднаних Націй, а також її спеціалізовані установи. Особливі функції щодо боротьби з високотехнологічними злочинами покладені на Управління ООН з наркотиків та злочинності (United Nations Office on Drugsand Crime – UNODC), у рамках якого здійснюється Глобальна програма з кіберзлочинності (Global Program on Cybercrime – GPC), а також функціонує Міжурядова експертна група відкритого складу з кіберзлочинності (Open-ended Intergovernmental Expert Group on Cybercrime). UNODC сприяє довгостроковому і стійкому нарощуванню потенціалу в боротьбі з кіберзлочинністю шляхом підтримки національних структур і дій.

Іншим інституційним механізмом ООН є Комісія з попередження злочинності і кримінального правосуддя (Commission on Crime Prevention and Criminal Justice – CCPCJ), створена на основі Резолюції ЕКОСОР 1992/1. Комісія здійснює координуючі функції, а також готує проведення Конгресів ООН із

попередження злочинності та кримінального правосуддя, проте спеціалізованих функцій у сфері боротьби з кіберзлочинністю не виконує.

Міжнародний союз електрозв'язку (International Telecommunication Union – ITU) як спеціалізована установа в системі Організації Об'єднаних Націй відіграє провідну роль у сфері стандартизації та розвитку електрозв'язку, а також у питаннях кібербезпеки. ITU є провідною організацією Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства (World Summit on the Information Society – WSIS), яка проходила в два етапи: у Швейцарії (2003 р.) і в Тунісі (2005 р.). За наслідками цієї зустрічі на ITU було покладено керівництво Напрямом діяльності С5 щодо зміцнення довіри і безпеки у сфері використання ІКТ. В результаті, у 2007 р. було розпочато Глобальну програму кібербезпеки ITU (Global Cyber security Agenda – GCA). Зазначена програма заснована на п'яти «стовпах», що відображають компетенцію цієї організації у сфері протидії кіберзлочинності: юридичні заходи, технічні та процедурні заходи, організаційні структури, нарощування потенціалу та міжнародне співробітництво. Для підготовки плану щодо реалізації GCA було створено Групу експертів на високому рівні (High-Level Experts Group – HLEG), до якої увійшли фахівці різного географічного і предметного спрямування (спеціалісти з кібербезпеки, включаючи представників урядів держав-членів МСЕ, індустрії, регіональних та міжнародних організацій, дослідницьких та академічних установ) з метою якнайбільш повно забезпечити мультистейкходеризм.

У грудні 2008 р. ITU та Європейський Союз (European Union – EU) розпочали три проекти у країнах АКТ (Африки, Карибського і Тихоокеанського регіону), спрямовані на створення і гармонізацію політики та законодавства у сфері інформаційно-комунікаційних технологій шляхом проведення освітніх заходів (HIPCAR, HIPSSA та ICB4PA C). Окрім цього, під егідою ITU розробляються регіональні кібернетичні підрозділи ALERT (Applied Learning for Emergency Response Teams), що слугують центрами обміну інформацією та обговорення поточних питань кібербезпеки, а також забезпечують практичні заходи для національних груп з реагування на комп'ютерні інциденти (CIRT). У 2018 р. було проведено п'ять центрів: AMS (Аргентина, 04-08.06.2018 р.); СНД (Азербайджан, 03-07.09.2018 р.); AFR (Кот-д'Івуар, 01-05.10.2018 р.); EUR (Кіпр, 26-30.11.2018 р.); ARB (Кувейт, 21-25.10.2018 р.). Опосередковано міжнародна співпраця держав щодо протидії кіберзлочинності здійснюється в рамках інших спеціалізованих установ ООН, зокрема: ЮНЕСКО, ІКАО, ЮНІСЕФ, ВОІВ та ін. Так наприклад, ЮНЕСКО була розроблена концепція «Універсальності Інтернету», що відображає позицію організації в межах її мандату стосовно питань, пов'язаних з Інтернетом, на період до 2021 р.

Безпосередній і важливий внесок у налагодження міжнародної співпраці щодо боротьби з високотехнологічною злочинністю здійснює Міжнародна організація кримінальної поліції (International Criminal Police Organization – INTERPOL). Ця організація вживає різноманітних заходів для підтримки держав-учасниць у боротьбі з кіберзлочинністю. INTERPOL реалізує підтримку розслідувань, а також надає технічну допомогу, рекомендації щодо найкращих практик розслідувань та проводить тренування. В рамках INTERPOL функціонує

Глобальна група експертів з кіберзлочинності, до складу якої входять фахівці різноманітних напрямів боротьби з високотехнологічною злочинністю. Відповідно до Глобального комплексу інновацій Інтерполу (Interpol Global Complex for Innovation – IGCI), організація здійснює координацію транснаціональних розслідувань та операції проти кіберзлочинності (наприклад, такі, як: Unmask (2012 р.), Strikeback (2014 р.), Aces (2015 р.), Simbabotnet (2015 р.), Singapore (2017 р.)). Центр КіберФ'южн (CyberFusionCentre – CFC) об'єднує фахівців правоохоронних органів та IT-галузі з метою забезпечення розвідувальної діяльності. Крім цього, в рамках INTERPOL функціонує лабораторія цифрової криміналістики та окремі робочі групи щодо видів кіберзлочинів.

Наступний сегмент у системі міжнародного співробітництва держав у протидії кібернетичним злочинам становлять регіональні організації. Провідну роль у ньому здійснює Рада Європи (Council of Europe – РЄ). Проблематика боротьби з високотехнологічною злочинністю є одним із напрямів діяльності РЄ починаючи з 1976 р. У 1995 р. Європейським комітетом з проблем злочинності (European Committee on Crime Problems – CDPC) було створено Комітет по боротьбі з кіберзлочинністю. А разом із ухваленням Конвенції Ради Європи про кіберзлочинність було утворено Комітет з Конвенції про кіберзлочинність (Cybercrime Convention Committee – T-CY). На виконання зазначеної угоди в рамках РЄ було створено декілька додаткових механізмів сприяння співробітництву, а також нарощуванню потенціалу. Зокрема, у квітні 2014 р. сформовано Офіс з програми кіберзлочинності (C-PROC), у 2013 р. розпочався спільний проект РЄ та ЄС Глобальні дії з кіберзлочинності (GLACY), .

У рамках Європейського Союзу у 2000 р. було прийнято всеохоплюючий «План дій Електронна Європа», а норми матеріального права ЄС гармонізовані за допомогою цілого ряду директив. Стратегія кібербезпеки Європейського Союзу, ухвалена в лютому 2013 р. з метою нарощування потужностей для попередження кіберзагроз, включаючи кіберзлочинність та кібертероризм. Боротьба з високотехнологічними злочинами є одним із основних пріоритетів у діяльності Європейського поліцейського управління (European Police Office – Europol). У 2013 р. Європолом був створений Європейський центр боротьби з кіберзлочинністю (European Cybercrime Centre – EC3) з метою посилення реакції правоохоронних органів на кіберзлочинність в ЄС і захист європейських громадян, бізнесу та урядів.

Щороку EC3 видає Оцінку загрози організованої злочинності в Інтернеті (Internet Organised Crime Threat Assessment – IOCTA), що визначає пріоритети діяльності Оперативного плану дій EMPACT у сфері кіберзлочину, який є основною темою цього року. EC3 також організовує діяльність Об'єднаної робочої групи з боротьби проти кіберзлочинності (Joint Cybercrime Action Task force – J-CAT). Її місія полягає в тому, щоб керувати інтегрованими, узгодженими діями проти основних загроз кіберзлочинності через транскордонні розслідування та операції з боку своїх партнерів.

Крім ЄС, подібні інституції у сфері боротьби з кіберзлочинністю були створені і в інших регіональних організаціях. Наприклад, у 1999 р. у рамках Організації американських держав (міністри юстиції та міністри або генеральні

прокурори держав американського континенту – REMJA) було створено міжурядову групу експертів з кіберзлочинності, Секретаріат міжамериканського комітету з боротьби з кіберзлочинністю (CICTE), Міжамериканську комісію електрозв'язку (CITEL), а також робочу групу з кіберзлочинності та Глобальну міжамериканську стратегію з кібербезпеки.

Таким чином, у результаті діяльності інституційного механізму міжнародної співробітництва держав у боротьбі з кіберзлочинністю здійснюються спільні заходи щодо протидії високотехнологічним злочинам, а також нарощування потужностей у визначеній сфері. Такі дії надають можливості адаптувати національні законодавства окремих держав до міжнародних, а також приєднатись до існуючих нормативних та інституційних механізмів. З іншого боку, основними напрямами нарощування потенціалу щодо протидії кіберзлочинності можуть бути: розроблення політики і стратегій у сфері кіберзлочинності; розроблення ефективного законодавства про боротьбу з кіберзлочинністю; створення спеціальних підрозділів протидії кіберзлочинності; навчання державних органів і персоналу з питань кіберзлочинності; сприяння співробітництву між державами і приватним сектором; розвиток міждержавного співробітництва.

Слід наголосити, що більшість функцій щодо міжнародного співробітництва у протидії кіберзлочинності дублюються у різних інституціях. Їхнє паралельне здійснення, на нашу думку, призводить до значної фрагментації і неоднорідності в відповідної сфери правового регулювання». ***(Яцишин М. Ю Роль міжнародних організацій у протидії кіберзлочинності // Українське право (https://ukrainepravo.com/international_law/public_international_law/rol-mizhnarodnykh-organizatsiy-u-protydiyi-kiberzlochynnosti/). 15.12.2019).***

***

**«В Таиланде правоохранительные органы расследуют недавний взлом системы видеонаблюдения в одной из тюрем на юге страны…** злоумышленники получили несанкционированный доступ к камерам и в течение нескольких часов транслировали видео с них на YouTube-канале BigBrother's Gaze.

Департамент коррекции при Министерстве юстиции Таиланда подтвердил, что несколько камер видеонаблюдения в тюрьме «Ланг Суан» в городе Чумпхон были взломаны неизвестными лицами, находящимися за пределами страны. Властям стало известно об инциденте от журналиста, случайно наткнувшегося на трансляцию.

Генеральный директор департамента коррекции полковник Нарат Саветтанан приказал отключить системы видеонаблюдения и начать расследование инцидента. Начальнику исправительного учреждения также было поручено обратиться в полицию с соответствующим заявлением.

Трансляция велась на YouTube-канале BigBrother's Gaze во вторник, 24 декабря, и была ошибочно подписана как трансляция из тюрьмы Бангкока. В среду видео уже было недоступно… ранее на канале также было опубликовано видео с камер в офисе таиландской компании, на улицах Солт-Лейк-Сити, в австралийской компании и в амстердамском кафе. В настоящее время на канале нет ни одного видео. Число подписчиков BigBrother's Gaze составляет порядка 1,4 тыс. человек.» ***(Хакеры взломали камеры видеонаблюдения в тюрьме и транслировали видео***

***на YouTube // SecurityLab.ru (https://www.securitylab.ru/news/503706.php). 26.12.2019).***

***

**«Бывший сотрудник IT-отдела одной из больниц Нью-Йорка Ричард Лириано признал себя виновным во взломе компьютерных систем медучреждения и учетных записей электронной почты сотрудников, а также в краже личных файлов и фотографий.**

Как сообщило Министерство юстиции США, в период с 2013 по 2018 годы Лириано злоупотреблял своим административным доступом для входа в учетные записи сотрудников и копирования на свой компьютер личных документов коллег, включая налоговые записи и фотографии. Для этого он установил на компьютеры жертв вредоносные программы, в том числе кейлоггер.

За указанный период Лириано украл учетные данные для примерно 70 аккаунтов электронной почты, принадлежащих сотрудникам больницы или связанным с ними лицам. Затем злоумышленник получил несанкционированный доступ к электронной почте, страницам в социальных сетях, фотографиям и аккаунтам в других сервисах, где были зарегистрированы жертвы.

В результате незаконных действий Лириано убытки американской больницы составили более $350 тыс.» ***(Бывший сотрудник больницы Нью-Йорка признался в краже данных коллег // SecurityLab.ru (https://www.securitylab.ru/news/503701.php). 25.12.2019).***

***

## Технічні аспекти кібербезпеки

**«На международной конференции IEEE TPS (Trust, Privacy and Security) в Лос-Анджелесе, штат Калифорния, группа исследователей из Keyfactor представила результаты исследования безопасности цифровых сертификатов.**

RSA-сертификаты используют криптографические алгоритмы для шифрования данных и защиты информации, передаваемой с устройств или служб на серверы. Они используются для защиты интернет-трафика и программного обеспечения, а также данных, генерируемых IoT-устройствами и медицинским оборудованием.

Эксперты рассказали о том, как можно взломать RSA-ключи с «минимальными вычислительными ресурсами», сообщило ZDNet со ссылкой на документ.

Команда использовала базу данных, включающую 75 млн активных RSA-ключей и позже дополненную 100 млн сертификатами, которые стали доступны в системе регистрации и мониторинга выдачи TLS-сертификатов Certificate Transparency (CT). Собранные данные были проанализированы с использованием алгоритма и виртуальной машины Microsoft Azure с целью выявить общие факторы при генерации случайных чисел. Из 175 млн сертификатов более 435 тыс. имеют общий фактор, позволяющий повторно получать закрытые ключи.

Как сообщили эксперты, обнаружение подобных «основных факторов» может быть использовано для компрометации сертификатов, ставя под угрозу безопасность устройств.

В ходе эксперимента атакующий с восстановленным закрытым ключом для SSL/TLS-сертификатов может выдавать себя за данный сервер, когда устройства попытаются подключиться. Подключившийся пользователь или устройство не сможет отличить злоумышленника от легитимного владельца сертификата, позволяя преступнику осуществить атаку или похитить конфиденциальные данные.

По словам специалистов, проблема затрагивает IoT-устройства и устройства с низким уровнем энтропии из-за аппаратных ограничений». ***(Уязвимость в RSA-сертификатах подвергает их риску атак // SecurityLab.ru (https://www.securitylab.ru/news/503462.php). 16.12.2019).***

***

## *Виявлені вразливості технічних засобів та програмного забезпечення*

---

**«Эксперты SafeBreach опубликовали список трёх раскрытых уязвимостей, выявленных в популярных и широко используемых программных продуктах, которые могут привести к захвату злоумышленниками вашего ПК**

Три известных антивирусных продукта содержат опасные уязвимости. Об этом заявила компания SafeBreach, эксперты которой исследовали программы «Лаборатории Касперского», Trend Micro и Autodesk. Экспертами компании были обнаружены уязвимости класса «захват DLL» (Dynamic Link Library, библиотека динамической компоновки для многократного использования программными приложениями), позволяющие запускать произвольные DLL-библиотеки в контексте высокопривилегированных процессов и тем самым компрометировать всю систему.

Команда SafeBreach написала соответствующие коды «доказательства осуществимости» [внешнего вмешательства], чтобы продемонстрировать, как можно будет скомпилировать свой собственный файл DLL, заменив и установив его для загрузки вместо законного. Это приводит к повышению привилегий за счет выполнения кода на самом высоком уровне полномочий, поскольку ни один из трех продуктов не выполняет какую-либо процедуру проверки DLL.

Эксперты отметили, что в этом процессе происходит попытка загрузить библиотеку, используя только имя файла, без учета точного, «абсолютного» месторасположения. Таким образом, злоумышленник получает возможность запускать произвольный код в контексте авторизованного процесса. Информация об уязвимостях была передана в соответствующие компании еще в июле 2019 г., и к настоящему времени они все исправлены…». ***(В ПО Касперского, Trend Micro и Autodesk обнаружены опасные бреши // РосКомСвобода (https://roskomsvoboda.org/53043/). 05.12.2019).***

***

**«Специалисты израильской ИБ-компании Polyrize обнаружили в приложении для общения и совместной работы Slack уязвимость, из-за которой отправленные по приватному каналу файлы могут быть видны всем пользователям в этом рабочем пространстве, даже «гостям».**

По словам специалистов, если пользователь хотя бы один раз открыл доступ к файлу, он становится доступен для всех, даже если потом пользователь закрыл доступ. Сам владелец файла при этом ни о чем не догадывается.

Уязвимость связана с реализацией в Slack механизма обмена файлами. Приложение позволяет делать публикации в рабочем пространстве двумя способами. Первый – через общий канал (беседу), и в таком случае любой участник рабочего пространства может присоединиться к беседе и просматривать сообщения и файлы. Второй способ предполагает обмен сообщениями в закрытой беседе, стать участником которой можно только по приглашению.

Пересылаемые в приватной беседе файлы должны быть видны только ее участникам. Если пользователь покидает беседу, он больше не может просматривать файлы. Однако специалисты Polyrize обнаружили, что если участник закрытой беседы перешлет файл из нее в другую беседу, он сможет обойти эти ограничения.

«Мы понимаем важность безопасности файлов для пользователей Slack. Описанное поведение характерно только для двух типов файлов в Slack – Сниппетов и Постов (опции для обмена и совместной работы над контентом крупных форм). Большинство публикуемых в Slack файлов не относятся к этим типам. Когда вы обмениваетесь Сниппетами и Постами в приватных каналах или сообщениях, они видны только ограниченному кругу людей, которые могут находить их через поиск. Когда вы обмениваетесь Сниппетами и Постами в открытых каналах, найти их через поиск и увидеть может каждый в рабочем пространстве. Это предусмотренный функционал», – сообщили в пресс-службе Slack изданию The Register. Разработчик приложения признал, что копка «Закрыть доступ» в пользовательском интерфейсе может сбить пользователя с толку. «Мы намерены откорректировать интерфейс, но модель безопасности обмена Сниппетами и Постами в Slack будет работать как раньше», – сообщили в пресс-службе Slack.» ***(Уязвимость в Slack позволяет видеть изъятые из открытого доступа файлы // SecurityLab.ru (https://www.securitylab.ru/news/503481.php). 17.12.2019).***

***

**«Компания TP-Link исправила в некоторых моделях маршрутизаторов Archer опасную уязвимость, позволяющую злоумышленникам аннулировать пароль администратора и захватить контроль над устройством по LAN через Telnet.** Проблема затрагивает маршрутизаторы Archer C5 V4, Archer MR200v4, Archer MR6400v4 и Archer MR400v3.

Для эксплуатации уязвимости атакующий должен отправить HTTP-запрос со строкой, содержащей большее число символов, чем разрешенное количество байтов. В результате пароль администратора аннулируется и заменяется пустым значением. Несмотря на наличие встроенного механизма валидации, вышеописанный способ все равно работает. Дело в том, что механизм проверяет

только HTTP-заголовки реферера, и с помощью вшитого значения tplinkwifi.net атакующий может заставить сервис httpd маршрутизатора принять запрос как подлинный.

Поскольку администратор обладает на устройстве правами суперпользователя, обойдя процесс аутентификации, злоумышленник автоматически получит эти права и захватит полный контроль над маршрутизатором. Он сможет не только контролировать все процессы, но также блокировать легитимным пользователям возможность авторизации в web-сервисе через пользовательский интерфейс. В таком случае жертва потеряет доступ к консоли и даже к оболочке и не сможет сменить пароль.

Даже если владельцу маршрутизатора удастся установить новый пароль, злоумышленник снова аннулирует его с помощью запроса LAN/WAN/CGI. И наконец, автоматически перестанут работать ключи RSA, поскольку шифрование не работает с пустыми паролями.

Уязвимость обнаружил исследователь IBM X-Force Red Гжегож Випич (Grzegorz Wypych). Проблеме был присвоен идентификатор CVE-2019-7405.» ***(Уязвимость в TP-Link Archer позволяет захватить контроль над устройством // SecurityLab.ru (https://www.securitylab.ru/news/503474.php). 17.12.2019).***

***

**«В программируемых контроллерах автоматизации (ПКА) Schneider Modicon M580, M340, Quantum и Premium обнаружены три опасные уязвимости. Их эксплуатация позволяет злоумышленникам вызвать отказ в обслуживании устройства.**

Все три проблемы (CVE-2019-6857, CVE-2019-6856, CVE-2018-7794) связаны с «некорректной проверкой на предмет нестандартных условий или исключений» и могут быть вызваны при чтении или записи определенных блоков памяти или при чтении данных с недопустимым индексом. Эксплуатация может быть осуществлена с помощью протокола Modbus TCP злоумышленником, который имеет сетевой доступ к уязвимым контроллерам.

Неизвестно, возможно ли проэксплуатировать уязвимости из интернета, но результаты поискового запроса Shodan выявили в открытом доступе несколько устройств M580 и почти 100 контроллеров M340.

Schneider Electric также проинформировала клиентов об уязвимостях в трех продуктах из линейки EcoStruxure, в том числе в ПО Power SCADA Operation для мониторинга и управления питанием. В продукте содержится опасная уязвимость, связанная с переполнением буфера в стеке. Ее эксплуатация позволяет вызвать сбой в работе на стороне сервера.

Продукт EcoStruxure Geo SCADA Expert (ClearSCADA), предназначенный для мониторинга и управления промышленными процессами, содержит опасную уязвимость незащищенных прав доступа к файлам, позволяющую локальному злоумышленнику с низкими привилегиями удалять или изменять файлы в базе данных, настройки или сертификаты.

Последняя уязвимость содержится в программном обеспечении EcoStruxure Control Expert для ПКА Modicon, эксплуатация которой позволяет обойти процесс аутентификации между программным обеспечением и контроллером.

Компания Schneider Electric выпустила патчи, исправляющие уязвимости в ПКА Schneider Modicon и продуктах EcoStruxure». ***(Уязвимости в продуктах Schneider Electric ставят под угрозу производственный процесс // SecurityLab.ru (https://www.securitylab.ru/news/503473.php). 17.12.2019).***

***

**«Некоторые аппаратные менеджеры паролей не обеспечивают должную защиту хранящихся в них данных и позволяют читать пароли в незашифрованном виде даже после сброса настроек.** По словам Фила Ивели (Phil Eveleigh) из PenTestPartners, получить информацию с проблемных устройств можно, подключившись напрямую к их чипам флеш-памяти на материнской плате.

С помощью микрокомпьютера Raspberry Pi Ивели удалось получить доступ и извлечь информацию из флеш-памяти аппаратного менеджера паролей RecZone Password Safe. Исследователь использовал для чтения данных утилиту hexdump и обнаружил, что они не зашифрованы. Более того, информация сохранилась в памяти даже после сброса настроек устройства до заводских. Изменилось лишь одно – PIN-код для разблокировки устройства, извлечь который также можно было из флеш-памяти.

По словам Ивели, проблема не ограничивается только устройствами RecZone Password Safe. Исследуя Royal Password Vault Keeper, он обнаружил чип CMOS. В отличии от RecZone, где данные можно было извлечь с помощью недорогого оборудования, здесь исследователю пришлось потратиться, однако расходы оправдали себя. В устройстве также были реализованы базовые механизмы защиты, но и их удалось обойти.

В Royal Password Vault Keeper данные оказались закодированы, но с помощью криптоанализа Ивели смог их расшифровать. По его мнению, шифрование не уникально для каждого устройства и является одним для всех. То есть, взломав шифрование одного менеджера пароля, можно взломать их все.

Третье исследованное устройство – passwordsFAST, использующее шину I2C. В этом случае данные оказались зашифрованными, и извлечь их было не так легко как в двух предыдущих. Хотя исследователю не удалось их расшифровать, он смог получить доступ к микроконтроллерам. По его мнению, теоретически, в итоге это позволит получить данные.

Компания PenTestPartners уведомила производителей RecZone Password Safe и Royal Password Vault Keeper о проблеме, но не получила никакого ответа». ***(Аппаратные менеджеры паролей не обеспечивают должную защиту данных // SecurityLab.ru (https://www.securitylab.ru/news/503239.php). 09.12.2019).***

***

**«Эксперты из Positive Technologies и Flutter Entertainment обнаружили в двух продуктах Citrix критическую уязвимость, которая потенциально угрожает 80 тыс. компаний в 158 странах.** По их оценкам, CVE-2019-19781,

позволяющая меньше чем за минуту взломать корпоративную сеть, может получить максимальную, 10-балльную оценку по шкале CVSS.

Проблема содержится в системах Citrix Application Delivery Controller (ранее называлась NetScaler ADC) и Citrix Gateway (NetScaler Gateway).

Первый продукт применяется для доставки приложений и балансировки нагрузки в частных и публичных облачных сервисах. Citrix Gateway, в свою очередь, позволяет организовать удаленный доступ к гибридным облакам и SaaS-платформам. По данным аналитиков, эти решения востребованы среди телекоммуникационных и IT-компаний — в 2014 году через Citrix ADC интернет-доступ получили 75% пользователей по всему миру.

Уязвимость небывалого масштаба

Подробности бага пока не раскрываются. Известно лишь, что он открывает злоумышленникам прямой доступ в локальную сеть, при этом авторизация не требуется. Под угрозой оказались все версии двух продуктов и все поддерживаемые платформы. Специалисты подчеркнули, что события такого масштаба происходят в индустрии максимум раз в 5–10 лет.

Уязвимость ставит под угрозу все элементы корпоративной инфраструктуры, к которым подключаются серверы Citrix. Это могут быть пользовательские рабочие компьютеры, финансовые и ERP-решения и прочие критически важные бизнес-системы.

Основная доля жертв — в США и Европе

Все эти факторы позволили экспертам предварительно оценить уровень угрозы CVE-2019-19781 как максимальный. Больше всего потенциальных жертв обнаружено в США — на эту страну приходится 38% пользователей уязвимых продуктов. В первую пятерку также вошли Германия, Великобритания, Нидерланды и Австралия. В России, которая занимает 26-ю строчку, эксперты насчитали более 300 компаний, которые могут пострадать от атак.

На момент публикации патча для уязвимости нет. Эксперты Citrix подготовили пакет временных мер и настоятельно советуют всем администраторам применить рекомендуемые настройки. Аналитики отметили оперативность разработчиков, которые составили список защитных мер за две недели с момента выявления уязвимости…». ***(Egor Nashilov. Уязвимость в Citrix позволяет взломать сеть за минуту // Threatpost (https://threatpost.ru/citrix-vulnerability-is-a-doomsday-button-for-networks/35073/). 20.12.2019).***

***

**«Операторы портала HackerOne выплатили $20 тыс. исследователю, обнаружившему серьезную уязвимость в их собственной платформе для хостинга программ bug bounty.** Выявленный недостаток позволял атакующему получить доступ к отчетам клиентов сервиса и другой конфиденциальной информации. Проблема была связана со случайным раскрытием идентификаторов сеанса в переписке службы поддержки…

Инцидент произошел 24 ноября 2019 года и стал следствием человеческой ошибки. Сотрудник HackerOne попытался воспроизвести некую уязвимость, найденную этичным хакером haxta4ok00, однако потерпел неудачу. Написав об

этом исследователю, он случайно включил в тело письма свой сеансовый файл cookie, который мог быть использован для доступа к порталу.

Как пояснили представители HackerOne, часть команды с URL, скопированная с консоли браузера, не была удалена при ответе клиенту сервиса. В результате этичный хакер получил возможность авторизоваться на портале с привилегиями сотрудника. Обнаружив идентификатор, haxta4ok00 заявил об уязвимости в программе bug bounty HackerOne, указав на серьезность допущенной утечки.

Портал отозвал скомпрометированный файл cookie и проверил остальные сообщения службы техподдержки на наличие конфиденциальных данных. Разработчики сервиса уже реализовали несколько краткосрочных мер, направленных на предотвращение подобных инцидентов в будущем. Теперь на HackerOne действует привязка сеанса пользователя к IP-адресу, используемому при первоначальном входе в систему, а также ограничение доступа сотрудников к ресурсам из определенных стран.

Сервис также обновил политику безопасности своей программы bug bounty, включив в нее случаи, когда хакер может иметь доступ к учетной записи HackerOne, секретным ключам или конфиденциальным данным. Дополнительно разработчики платформы добавили в нее функцию проверки исходящих сообщений на наличие сеансовых куки и токенов аутентификации. Если такой контент будет обнаружен, система запросит подтверждение отправки письма…». ***(Maxim Zaitsev. Этичный хакер выявил уязвимость в процессах HackerOne // Threatpost (https://threatpost.ru/hackerone-rewards-bug-hunter-for-finding-account-takeover-vulnerability/34984/). 06.12.2019).***

***

**«Военное ведомство Соединенных Штатов Америки опубликовало документ, указывающий на уязвимость ПО китайского производителя беспилотников, компанию DJI…**

«Исследования в открытом коде указывают на наличие многочисленных методов, позволяющих пассивно просматривать видео и метаданные с воздушного средства, а также осуществлять контроль над ним», - говорится в предупреждении.

Этот документ был обнародован, поскольку технологии, разработанные китайскими компаниями, которые поддерживают большую часть базовой инфраструктуры Интернета, подвергаются повышенному вниманию со стороны правительства США. Среди беспокойств - китайский закон, который в настоящее время вынуждает предприятия выполнять запросы разведывательных органов страны.

«В целом, система является очень уязвимой и требует соответствующего обращения», - говорится в документе, полученном из архива Национальной безопасности Университета Джорджа Вашингтона. В предупреждении Пентагон указал на проблемы с тем, как беспилотник DJI связывается и отправляет данные на наземную станцию». ***(Пентагон обвинили компанию DJI в работе на китайскую разведку // SecureNews (https://securenews.ru/pentagon-obvinil-dji-v-spionazhe/). 18.12.2019).***

***

**«Із завидною регулярністю експерти розвінчують міф про безпеку Google Play. Фахівці White Ops, що спеціалізуються на кібербезпеці, виявили в магазині додатків Google більше сотні програм, які потенційно небезпечні для пристроїв.**

Всього експертам вдалося знайти 104 шкідливих додатки, які в цілях безпеки не варто встановлювати на свої Android-пристрої. А якщо їх уже встигли завантажити, то користувачам рекомендується негайно їх видалити. Всього за оцінками фахівців, ці утиліти були завантажені понад 4,6 млн разів. Більшість з них з'явилися в каталозі Play Store з вересня нинішнього року.

За даними White Ops, всі шкідливі програми використовують у своїй роботі два різних коди Sogo і Soraka для показу повноекранної реклами на пристроях. Завдання таких програм — показ реклами на дисплеї смартфона. Вона нав'язлива і з'являється навіть тоді, коли пристрій заблоковано або знаходиться в режимі очікування.

Крім того, самі програми стали «розумніші» і далеко не завжди показ рекламних оголошень відбувається відразу після установки програми. Утиліта вичікує певний час і тільки потім атакує пристрій…». ***(Google пропустила в Play Store більше сотні шкідливих додатків // ВСВІТІ (http://vsviti.com.ua/news/108863). 24.12.2019).***

***

**«Компанія Rapid7, що працює в сфері кібербезпеки, виявила уразливість в ряді дитячих розумних годин з підтримкою GPS.** Дослідники придбали на сайті Amazon годинник трьох марок: children's SmartWatch, G36 children's Smartwatch і SmarTurtles kid's Smartwatch. Вивчення пристроїв показало, що вони мають практично однакове апаратне і програмне забезпечення. Точніше кажучи, апаратна частина годин ідентична тій, що використовується в аналогічному пристрої китайської компанії 3G Elec. Всі годинники використовують GPS-трекінг, серверний хмарний сервіс SETracker або SETracker2 і мобільний додаток для iPhone і Android. Судячи з підпису розробника ПЗ, він пов'язаний з 3G Elec.

Одна технічна сторона уразливості пов'язана з тим, що для управління годинами використовуються SMS, але всупереч опису, годинник сприймають повідомлення не тільки з заздалегідь визначеного номера, але і з будь-якого іншого. Відсутність фільтрації дозволяє зловмисникам віддалено змінювати налаштування годин, прив'язувати їх до інших смартфонів і стежити за дітьми.

Інше слабке місце – недокументований пароль за замовчуванням, який використовується для зв'язку з пристроями. За замовчуванням паролем служить рядок «123456». При цьому в документації або взагалі відсутня згадка про це, або не сказано, як можна змінити пароль.

Ситуацію погіршує третій момент, що носить не технічний, а організаційний характер. Всі спроби отримати відомості про постачальників годинників або зв'язатися з ними виявилися безуспішними. Це, зокрема, означає, що можна не розраховувати на усунення зазначених вище технічних проблем». ***(Харитоненко Андрій. У дитячих розумних годинниках виявлена вразливість, що дозволяє зловмисникам стежити за дітьми // TechnoPortal.com.ua (https://technoportal.com.ua/gadgets/38720). 14.12.2019).***

***

## *Технічні та програмні рішення для протидії кібернетичним загрозам*

**«Компания VMware на конференции VMworld 2019 представила обновление существующих и сообщила о доступности новых решений для обеспечения информационной безопасности.**

Отмечается, что новые инициативы воплощают на практике представление VMware об архитектуре встроенной безопасности, в которой обеспечение ИБ на предприятии становится в большей степени автоматизированным, проактивным и повсеместным.

Как подчеркивается, с помощью встроенной безопасности VMware снижает риск для критически важных приложений, пользователей и конфиденциальных данных, уменьшая «поверхность атаки» применительно к облакам, ЦОД, пользователям и инфраструктуры периферийных вычислений предприятия.

Новое решение VMware NSX Distributed Intrusion Detection and Prevention для обнаружения и предотвращения сетевых атак. Анонсирован новый функционал VMware NSX Federation для централизованной и единообразной настройки сетей и политика безопасности в сценарии крупномасштабного развертывания NSX, а также улучшения производительности, гибкости и функциональности филиального межсетевого экрана в составе VMware SD-WAN. Обновления в VMware Secure State позволят снизить уровень риска при работе в среде публичного облака и улучшить статус безопасности; новая архитектура безопасности «с нулевым доверием» для цифрового рабочего пространства.

«Мы в VMware уверены, что должны прекратить всё более усложнять процесс обеспечения кибербезопасности и использовать вместо этого нашу инфраструктуру как часть решения. Если коротко, мы должны сделать безопасность встроенной, — заявил Санджай Пунен, главный операционный директор VMware. — Устранив присущую системам кибербезопасности структурную сложность, VMware смещает баланс сил в извечном противостоянии нападения и защиты в пользу защиты. VMware обеспечивает встроенную безопасность с помощью комплексного портфеля решений, охватывающего критические точки контроля ИБ: сеть, конечные устройства, рабочие нагрузки, учетные записи, облако и аналитику. Встроенная защита находится везде, где находятся приложения, устройства и пользователи. Это позволяет максимально оперативно получать информацию о том, что происходит в среде заказчика. С помощью этого знания мы можем активно укреплять среду наших заказчиков для более эффективного предотвращения угроз».

После заключения сделки по приобретению Carbon Black в октябре 2019 года VMware открыла новое бизнес-подразделение под руководством бывшего генерального директора Carbon Black Патрика Морли. Основная задача, которую ставит перед собой это подразделение — это помощь заказчикам в обеспечении комплексной защиты конечных устройств и рабочих нагрузок, а также

усовершенствование аналитики в сфере кибербезопасности для пресечения технологически сложных кибератак и сокращения времени реагирования.

В качестве первого шага на этом пути VMware предложит заказчикам сразу несколько новых решений Carbon Black Cloud, включая Carbon Black Endpoint Standard: антивирус следующего поколения, комбинированный с системой обнаружения и реагирования на угрозы на уровне конечного устройства; Carbon Black Endpoint Advanced: решение Carbon Black Endpoint Standard, комбинированное с функцией запроса и исправления в режиме реального времени; Carbon Black Endpoint Enterprise: функция запроса и исправления в режиме реального времени в сочетании с усовершенствованной функцией активного поиска угроз и реагирования на инциденты; Carbon Black Workload: новое усовершенствованное облачное дополнение для защиты рабочих нагрузок в VMware vSphere; VMware Workspace Security: сочетает лучшие в своем классе функции обнаружения угроз на основе анализа поведения, антивирус следующего поколения, а также решения для аналитики и исправления нарушений безопасности цифрового рабочего пространства; Carbon Black Endpoint Standard с Secureworks Threat Detection and Response: это лучший в своем классе антивирус следующего поколения с функциями обнаружения и реагирования на угрозы на уровне конечных устройств, а также усовершенствованное приложение для анализа безопасности, расширяющее телеметрию безопасности за пределы конечного устройства, охватывая сеть и облако.

VMware также объявила о расширении сотрудничества с компанией Dell, которая сделает Carbon Black Cloud предпочтительным средством обеспечения безопасности конечных устройств для своих коммерческих клиентов наряду с Dell Trusted Devices and Secureworks. Расширенное партнерство позволит предприятиям любого размера получить усовершенствованную защиту конечных устройств при помощи Carbon Black в качестве встроенной функции.

Программное обеспечение VMware NSX стало первым решением, позволяющим на практике реализовать микросегментацию сети как с финансовой, так и с эксплуатационной точки зрения. С его помощью заказчики могут легко предотвращать «горизонтальное» распространение вредоносного ПО внутри ЦОД. Теперь VMware представляет новый функционал в NSX по обнаружению и предотвращению сетевых атак (IDS/IPS), выводя на принципиально новый уровень возможности платформы NSX по межсетевому экранированию за счёт распознавания контекста (Layer 7). Решение NSX Distributed IDS/IPS уникально тем, что обладает всеми преимуществами глубокого понимания запущенных на платформе VMware сервисов, образующих в совокупности приложение, позволяющего сопоставлять сигнатуры IDS/IPS с конкретными компонентами приложения. Это означает, что сервер Apache или Tomcat будет получать только релевантные сигнатуры, а не все подряд. В результате производительность и точность станут намного выше за счет сокращения количества ложных обнаружений. Сервисно-определяемый сетевой экран VMware в сочетании с NSX Distributed IDS/IPS позволит заказчикам не только производить микросегментирование своих сетей, но и блокировать внутренний трафик от взломанных учетных записей или скомпрометированных машин.

Недавно было представлено решение NSX Intelligence — усовершенствованная система для анализа трафика рабочих нагрузок и автоматического создания политик безопасности. NSX Federation — новая функция, которая позволяет развертывать и последовательно применять политики безопасности, сгенерированные NSX Intelligence, сразу в нескольких ЦОД. NSX Federation поможет предприятиям упростить аварийное восстановления и предотвращение аварий, а также распределить ресурсы приложения по нескольким ЦОД. Совмещение эксплуатационных задач значительно упростит архитектуру безопасности в целом. Это позволит сделать процесс управления политиками безопасности и исполнения нормативно-правовых требований более удобным для заказчиков и сформировать целостный контекст для выявления и решения проблем безопасности. Такого уровня эффективности и гибкости невозможно добиться с помощью традиционных средств, использующих подход “bump in the wire”, что является существенным дифференциатором открытой горизонтально-масштабируемой платформы, такой, как NSX, относительно наследованных и проприетарных аппаратно-определяемых решений.» ***(VMware представила решения для внедрения встроенной безопасности // Компьютерное Обозрение (https://ko.com.ua/vmware_predstavila_resheniya_dlya_vnedreniya_vstroennoj_bezopasnosti_131109). 03.12.2019).***

***

**«Компания Mozilla обязала всех разработчиков расширений для своего браузера Firefox включить в своих учетных записях функцию двухфакторной аутентификации.**

«С начала 2020 года разработчики расширений будут обязаны включать на AMO (портале Mozilla Add-On – ред.) двухфакторную аутентификацию», – сообщила менеджер сообщества разработчиков расширений компании Mozilla Кейтлин Нейман (Caitlin Neiman). По ее словам, благодаря этому злоумышленники не смогут захватывать контроль над легитимными расширениями и, соответственно, системами пользователей.

Получив доступ к учетной записи разработчика, злоумышленник может рассылать с нее пользователям Firefox вредоносные обновления для расширений, пояснила Нейман. Поскольку расширения занимают в браузере привилегированную позицию, их компрометация позволяет злоумышленникам похищать пароли и файлы cookie, следить за активностью пользователей или направлять их на фишинговые или вредоносные страницы. Такой вид кибератаки называется «атака на цепочку поставок».

Портал AMO является официальным ресурсом Mozilla, и пользователи всецело доверяют присланным с него обновлениям. В случае получения с него вредоносных обновлений жертва даже ни о чем не догадается. В связи с этим Mozilla решила улучшить безопасность пользователей, обязав разработчиков расширений обезопасить свои учетные записи AMO с помощью двухфакторной аутентификации». ***(Mozilla обязала разработчиков расширений включить двухфакторную аутентификацию // SecurityLab.ru (https://www.securitylab.ru/news/503430.php). 16.12.2019).***

***

**«В MaxPatrol SIEM загружены 19 новых правил для обнаружения атак, нацеленных на получение учетных данных (Credential Access).** Это четвертый пакет экспертизы из специальной серии для покрытия тактик модели MITRE ATT&CK. С его помощью пользователи MaxPatrol SIEM смогут предотвратить получение злоумышленниками легитимных учетных данных, которое в случае успеха атаки усложнило бы возможность обнаружения атакующих в системе.

Тактика «Получение учетных данных» объединяет техники, нацеленные на кражу учетных имен и паролей. Это возможно, например, с помощью подбора паролей (брутфорс), поиска файлов, содержащих пароли, дампинга учетных записей, эксплуатации уязвимостей.

Использование легитимных учетных записей помогает злоумышленникам получить доступ к системам, создать новые учетные записи для ускорения достижения их целей и усложняет обнаружение их присутствия.

«Credential Access — один из самых эффективных инструментов в арсенале атакующих, — комментирует Антон Тюрин, руководитель отдела экспертных сервисов PT Expert Security Center. — Получив доступ хотя бы к одному сетевому узлу, они применяют отлаженный сценарий для дальнейшего продвижения в инфраструктуре. Злоумышленники получают содержимое памяти процессов или файлов и используют полученные оттуда учетные данные для доступа к другим системам. Остановить такое продвижение может только своевременная реакция команды ИБ, обнаружившей применение техник кражи учетных данных, и сегментация сети».

Новый пакет экспертизы нацелен на выявление трех распространенных техник кражи учетных данных:

Credential Dumping — получение учетных данных из дампа памяти системных служб Windows или стороннего ПО. Пароли могут храниться в открытом виде или в виде контрольной суммы.

Credentials in Files — поиск учетных данных в файловой системе или в общих папках. Например, такие данные могут содержаться в файлах, созданных самими пользователями, или в конфигурационных файлах ПО. Также учетные данные могут сохраняться на контроллерах домена, в файлах предпочтений групповой политики (GPP).

Credentials in Registry — поиск учетных данных в реестре Windows. В разделах реестра могут храниться учетные данные для автоматического ввода в ОС или стороннем ПО.

К техникам получения учетных данных относится также брутфорс. Правила для его выявления были загружены в MaxPatrol SIEM отдельным пакетом экспертизы в начале года…» ***(MaxPatrol SIEM выявляет попытки атакующих получить учетные данные // SecurityLab.ru (https://www.securitylab.ru/news/503389.php). 12.12.2019).***

***

**«Во вторник, 10 декабря, компания Microsoft выпустила последние в нынешнем году плановые обновления безопасности для своих продуктов. В общей сложности они исправляют 36 уязвимостей в Windows, Internet Explorer, SQL Server, Visual Studio, Hyper-V Server и Office. 7 уязвимостей**

**являются критическими, 28 отмечены как опасные и 1 – как средней опасности.**

Одна из исправленных уязвимостей в Windows (CVE-2019-1458) активно эксплуатируется киберпреступниками. Проблема возникает, когда компонент Win32k не может должным образом обработать объекты в памяти. Благодаря этому атакующий может повысить свои привилегии на системе и запустить произвольный код в режиме ядра, что позволит ему устанавливать программы, читать, изменять и удалять данные, а также создавать новые учетные записи пользователей со всеми правами.

Для эксплуатации уязвимости атакующему сначала нужно авторизоваться в системе. Затем с помощью особым образом сконфигурированного приложения он сможет проэксплуатировать уязвимость и получить полный контроль над атакуемой системой.

По словам Дастина Чайлдса (Dustin Childs) из Trend Micro Zero Day Initiative, уязвимость такого типа может эксплуатироваться в паре с уязвимостью использования памяти после высвобождения в Chrome ( CVE-2019-13720 ) для обхода песочницы. Данная проблема затрагивает библиотеку PDFium и была исправлена Google в конце октября.

CVE-2019-1458 была выявлена специалистами «Лаборатории Касперского» Антоном Ивановым и Алексеем Кулаевым. Никаких других способов обойти или исправить ее, кроме как установить обновление, Microsoft не обнаружила». ***(Microsoft исправила уязвимость нулевого дня в Windows // SecurityLab.ru (https://www.securitylab.ru/news/503314.php). 11.12.2019).***

***

**«ФБР вважає, що у компаній є можливість обмежити збиток від злому даних, а саме надати хакерам неправильні дані. Ars Technica дізналася про програму ФБР IDLE (Illicit Data Loss Exploitation), в рамках якої компанії впроваджують «помилкові дані», щоб збити з пантелику зловмисників, охочих вкрасти цінну інформацію.**

Хоча ФБР не ділиться більш тонкими деталями того, як працює IDLE, відомо, що неправдиві дані додаються в існуючі бази, щоб вони виглядали достовірними. Хакер не може просто збирати дані у великій кількості і очікувати, що вони всі будуть корисні. Тому, просте завантаження помилкових може попередити IT-персонал про те, що відбувається. ФБР допомагає створювати фіктивні дані, використовуючи реальну інформацію, але бюро не зберігає інформацію і отримує її виключно за згодою.

Немає жодних гарантій, що це буде ефективно. Однак, мова йде не стільки про забезпечення «герметичного» захисту, скільки про оригінальний підхід. Він допомагає компаніям «підготувати свій захист» замість того, щоб просто реагувати на порушення, коли вони відбуваються. Тож, цей варіант може бути корисною частиною кібербезпеки компаній». ***(Грицина Вікторія. Програма ФБР допоможе компаніям в боротьбі з хакерами // Pingvin.pro (https://pingvin.pro/gadgets/news-gadgets/programa-fbr-dopomozhe-kompaniyam-v-borotbi-z-hakeramy.html). 23.12.2019).***

***

**«Інтернет-сервіси з оцінки надійності паролів покликані допомогти користувачам захистити свої особисті дані від загроз кіберзлочинців.**

Однак «непослідовні та оманливі» поради, які надають деякі з найпопулярніших веб-сайтів, насправді можуть принести більше шкоди, ніж користі. Про це свідчать результати дослідження вчених з Університету Плімута (Велика Британія), повідомляє прес-служба вишу.

Дослідники оцінили ефективність 16 популярних сервісів із оцінки паролів. Також учені оцінили аналогічні сервіси, вбудовані в деякі поширені онлайн-сервіси (зокрема Dropbox та Reddit) та стандартні для деяких пристроїв.

В межах дослідження були протестовані 16 паролів на різних сервісах, причому 10 з них відносилися до найбільш часто використовуваних паролів в світі (включаючи «password» і «123456»).

З 10 явно слабких паролів тільки п'ять були послідовно негативно оцінені усіма цими сервісами.

Особливо характерною була ситуація з очевидно слабким паролем «Password1!», у котрому, однак, застосовані поширені рекомендації щодо підбору надійних паролів — наявні великі і малі літери, цифра та небуквенний символ. Цей пароль був сприйнятий набагато краще, ніж варто було б, і навіть отримав високу оцінку у трьох з відповідних сервісів.

Водночас пароль, згенерований браузером, постійно отримував високу оцінку. Це означає, що користувачі, схоже, можуть довіряти цим функціям, оскільки вони добре справлялися зі своїм завданням, — зазначають дослідники… ». ***(Кібербезпека: популярні сервіси з оцінки паролів збільшують ризик хакерських атак — учені // Ракурс (https://racurs.ua/ua/n131072-kiberbezpeka-populyarni-servisy-z-ocinky-paroliv-zbilshuut-ryzyk-hakerskyh-atak-ucheni.html). 19.12.2019).***

***

**«Международная платежная система Mastercard объявила о покупке компании RiskRecon, поставщика искусственного интеллекта и решений для анализа данных, чтобы помочь клиентам расширить возможности кибербезопасности.**

Технологии сканирования и оценки рисков от RiskRecon помогут компаниям лучше защищать платежные данные и интеллектуальную собственность. Отмечается, что помимо сотрудничества с Mastercard, предприятие продолжит предоставлять решения и для компаний в других сферах, включая здравоохранение и производство…

Условия сделки пока не разглашаются». ***(Mastercard пополнит набор решений по киберзащите: компания заключила новую сделку // PaySpace Magazine (https://psm7.com/technology/mastercard-popolnit-nabor-reshenij-po-kiberzashhite-kompaniya-zaklyuchila-novuyu-sdelku.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Payspacemagazine+%28Payspacemagazine%29). 26.12.2019).***

***

**«Командование Военно-воздушных сил США заключило контракт с калифорнийской компанией Xage Security на внедрение блокчейн-системы для обеспечения кибербезопасности систем Министерства обороны США.**

Как отмечается, Xage Security фокусируется на промышленном интернете вещей, обеспечивая безопасность IoT- и других устройств с сетевым подключением. Военные IoT-системы могут включать в себя несколько тысяч устройств, в том числе различные датчики, каждый из которых может служить входом в систему, угрожая ее безопасности. Из-за огромного количества удаленных устройств, вероятность успешной кибератаки возрастает во много раз.

Для защиты необходимо запретить подключение неавторизованных устройств к сети, а также предоставить средства для выявления поддельных устройств. Именно это может обеспечить блокчейн, который хранит точную и неизменяемую информацию обо всех подключениях и привилегиях отдельных устройств с контрольным журналом действий. Зачастую хакеры меняют пароль и пытаются скрыть следы своего присутствия меняя журналы аудита. Однако если контрольные журналы ведутся на блокчейне, злоумышленнику придется менять не одну запись, а огромное подмножество на нескольких узлах. Такой подход обеспечивает высокий уровень кибербезопасности.

«В условиях диджитализации, преобразующей промышленные и военные операции, мы должны гарантировать, что подключенные устройства и сети не откажутся работать в самый неподходящий момент даже при кибератаке или системном сбое», - пояснил генеральный директор Xage Security Дункан Грейтвуд.

Он также добавил, что блокчейн-система Xage обеспечивает необходимый уровень безопасности распределенных военных сетей…». ***(ВВС США усилят кибербезопасность блокчейном // LetKnow OÜ (https://letknow.news/news/universitet-v-santa-barbare-nachal-prepodavat-blokcheyn-34802.html). 25.12.2019).***

***

**«Корпоративные клиенты облачной платформы Google получат больше способов защиты от хакеров благодаря анонсированной компанией интеграции своего облачного продукта с многими популярными средствами кибербезопасности и нескольким новым предложениям от её партнёров.**

В категории защиты конечных точек, свой сервис MVISION Cloud for Containers перенесла на Google Cloud фирма McAfee. Помимо защиты своих контейнеризованных рабочих нагрузок, клиенты в результате такой интеграции получают доступ к инструментам пакета McAfee Endpoint Protection, которые будут обеспечивать в облаке Google безопасность виртуальных машин, работающих с Windows и Linux. Все эти решения можно будет получить на ресурсе Google Cloud Marketplace.

В категории аналитики угроз, добавилась интеграция с двумя различными провайдерами. Google Cloud теперь сможет использовать информацию о деятельности хакеров, собранную Palo Alto Networks и стартапом Tanium, чтобы предоставить корпоративным клиентам максимально достоверную картину онлайновых рисков. Аналитика сервиса AutoFocus компании Palo Alto Networks

будет поступать через службу Event Threat Detection, а телеметрия от Tanium будет сохраняться в Backstory.

В области управления идентификацией, Google делает доступным на своей платформе набор инструментов от ForgeRock, предназначенных для контроля доступа пользователей к приложениям. Те клиенты, которые используют Active Directory, могут теперь применять для защиты этого сервиса от сбоев и инсайдерских угроз инструменты от Semperis и STEALTHbits Technologies.

Список доступных для Google Cloud продуктов, разработанных партнёрами компании, пополнился платформой виртуальных Windows-десктопов Workplace от Citrix Systems, а также брандмауэром веб-приложений FortiWeb Cloud от Fortinet.

Углубляется и сотрудничество Google с консалтинговыми партнёрами. Компания сообщила о расширении ассортимента сервисов безопасности — от оценки рисков до изоляции инцидентов — предоставляемых клиентам Google Cloud корпорацией IBM, компаниями Deloitte и Wipro, филиалом KKR & Co. — Optiv Security, австрийским предприятием Comm-IT и CYDERES — «дочкой» Fishtech Group». ***(Google Cloud расширяет интеграцию с ведущими решениями безопасности // Компьютерное Обозрение (https://ko.com.ua/google_cloud_rasshiryaet_integraciyu_s_vedushhimi_resheniyami_bezopasnosti_131277). 17.12.20190.***

***

**«Американская компания-разработчик стандартов безопасности в промышленности и электроники Underwriters Laboratories представила концепцию стандартов безопасности для интернета вещей…**

Также в компании уточнили, что большая часть продуктов, находящихся сейчас на рынке, эту сертификацию не пройдет.

Обладая постоянными представительствами в 46 странах мира и обслуживая более сотни, UL — одна из самых авторитетных структур в своей области. Ею разработаны стандарты безопасности для множества разных отраслей промышленности, включая экологию, строительство, промышленное оборудование, электрические и электронные продукты и т. д.

UL недавно опубликовала свой «Рейтинг безопасности интернета вещей», в рамках которого производится оценка «критических факторов безопасности smart-продуктов», где фиксируется наличие или отсутствие известных уязвимостей и устойчивость устройств перед наиболее типичными методами кибератак.

«Большинство взломов являются следствием слабых мест и известных уязвимостей, — говорится в публикации UL. — Как производитель вы должны стремиться избавиться от них и придерживаться проверенных методов обеспечения безопасности. Лишь недавно государства взялись за регулирование безопасности IoT-устройств, но они все еще полагают, что инициатива должна исходить от индустрии безопасности».

«Подобные меры следовало бы принять уже давно: количество подключенных устройств во всем мире вплотную подбирается к 50 миллиардам, а положение с их защищенностью никакого оптимизма не внушает, — говорит Олег Галушкин, генеральный директор компании SEC Consult Services. — Из-за этого интернет вещей становится источником постоянной угрозы для частных и

корпоративных пользователей. В 2016 году ботнет, состоявший из IoT-устройств, был использован для организации одной из мощнейших DDoS-атак в истории, но это лишь один, самый известный случай. Подобные атаки, пусть и меньших масштабов, происходят постоянно. Необходима и сертификация, и законодательные меры для того, чтобы заблокировать попадание небезопасных устройств на рынок; но также необходимо, чтобы инициативу проявляли и коммерческие структуры, и конечные пользователи».

Компания SEC Consult разработала специальное решение для анализа безопасности устройств интернета вещей — IoT Inspector, которое позволяет анализировать программные оболочки таких устройств на предмет наиболее распространенных проблем – уязвимостей, вшитых паролей, ключей SSH/SSL и других факторов, сказывающихся на безопасности этих систем. В большинстве случае, указывает Галушкин, устройства оказываются уязвимыми именно в силу таких ошибок, а также небрежного отношения пользователей к своей безопасности.

На сегодняшний день никаких общепринятых стандартов качества и безопасности интернета вещей нет. Обилие уязвимостей превращают их в самый буквальный риск для кибербезопасности на макроуровне…

Сертифицировать устройства предлагается по семи категориям: обновление программных компонентов, данные и криптография, логическая безопасность, управление системой, пользовательские личные данные, протоколы безопасности и процесс, документирование.

Каждому из этих факторов соответствует набор практических рекомендаций по обеспечению защищенности.

Например, самым минимальным требованием в категории «данные и криптография» является отсутствие пароля по умолчанию. Для получения максимального сертификата, Diamond в той же категории устройство должно выстоять против брутфорса.

По мнению директора по безопасности и технологиям UL Эндрю Джеймисона (Andrew Jamieson), лишь небольшой процент устройств, доступных сегодня на рынке, отвечает максимальным требованиям, предъявляемым сертификацией UL, в то время как большая часть таких устройств не пройдет сертификацию даже по нижнему порогу.

Еще в июне 2019 г. UL опубликовала черновой вариант своих стандартов и требований, но Джеймисон признал, что фактически разработка этих нормативов находится на ранней стадии. Сейчас компания активно сотрудничает с производителями устройств интернета вещей в надежде на улучшение качества их разработок. В начале 2020 г. ожидается публикация новой редакции стандартов…» ***(Николай Загорский. В США разработали стандарты безопасности для интернета вещей // Голос UA (https://golos.ua/i/723448). 17.12.2019).***

***

**Васильковський І. І. Взаємодія правоохоронних органів при розслідуванні кіберзлочинів : автореф. дис. ... канд. юрид. наук : 12.00.09 / Васильковський Ігор Ігорович ; ПВНЗ «Європ. ун-т». - Київ, 2019. - 18 с.**

На основі комплексного аналізу фундаментальних положень криміналістики обґрунтовано взаємодію правоохоронних органів при розслідуванні кіберзлочинів. Досліджено теоретичні основи та нормативне забезпечення взаємодії та обґрунтовано необхідність координації та взаємодії в діяльності правоохоронних та інших державних органів при розслідуваннікіберзлочинів. Проаналізовано міжнародний досвід при розслідуванні кіберзлочинів. Розглянуто особливості в діяльності ООН, ЄС з проблем міжнародного співробітництва при їх розслідуванні.

Шифр зберігання НБУВ: РА442844

***

**Васильковский І. І. Поняття, класифікація та характеристика окремих видів кіберзлочинів / І. І. Васильковский // Прикарпатський юридичний вісник. - 2017. - Вип. 1(2). - С. 196-201.**

Визначено основні поняття кіберзлочинності та класифікації кіберзлочнів, їх характеристики, які виникають у результаті здійснення даного виду діяльності.

Шифр зберігання НБУВ: Ж74200

***

**Гибридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства : аналіт. док.- Київ, 2018. - 105 с.**

Проаналізовано гібридні загрози безпеки України, можливості і слабкі місця держави з протидії їм, досвід окремих країн Європейського Союзу і Східного партнерства (Польща, Грузія, Молдова, Білорусь, Росія). Подано висновки і рекомендації щодо розбудови можливостей України гарантувати безпеку суспільства в умовах гібридних загроз.

Шифр зберігання НБУВ: ВА837724

***

**Захарко А. В. Аналіз стану законотворчої діяльності щодо імплементації процедурних положень конвенції про кіберзлочинність / Захарко А. В. // Науковий вісник Дніпротетровського державного університету внутрішніх справ. - 2019. - № 2. - С. 134-142.**

Розглянуто процедурні положення Конвенції про кіберзлочинність. Проаналізовано актуальний стан кримінального процесуального законодавства на наявність норм, що кореспондують процедурним положенням Конвенції про кіберзлочинність. Вивчено порядок денний десятої сесії Верховної Ради України восьмого скликання на предмет наявності законопроектів щодо імплементації процедурних положень Конвенції про кіберзлочинність до Кримінального процесуального кодексу України.

Шифр зберігання НБУВ: Ж70666

***

**Князєв О. А. Метод адаптивної комплексної фільтрації контенту в мережі Інтернет : автореф. дис. ... канд. техн. наук : 05.13.21 / Князєв Олександр Андрійович ; Одес. нац. акад. зв'язку ім. О. С. Попова. - Одеса, 2019. - 20 с.**

Розроблено спосіб адаптивної фільтрації унікальних ідентифікаторів ресурсів (URI) Інтернет, що дозволяє зменшити середній час обробки запиту. Розроблено алгоритм адаптивної комплексної системи фільтрації небажаного контенту в мережі Інтернет та імітаційну модель, яка спроможна кількісно оцінити ефект від впровадження адаптивної комплексної фільтрації в реальних системах. Сформовано математичні моделі визначення загального часу обробки вхідного запиту та обчислення часу середньої затримки. Удосконалено метод оцінки та забезпечення структурної живучості мережі на основі показника, а також метод розрахунку оптимальної структури резерву.

Шифр зберігання НБУВ: РА442739

***

**Кримінальні загрози в секторі безпеки: практики ефективного реагування : матеріали панел. дискусії III Харків. міжнар. юрид. форуму, м. Харків, 26 верес. 2019 р. - Харків : Право, 2019. - 170 с.**

Зі змісту:

- Бусол О.М. Кібернетична війна та кібертероризм як загрози міжнародній безпеці: диференціація злочинів від традиційної війни;
- Воронов І. Захист персональних даних в мережі Інтернет;
- Колб О.Г., Дучимінська Л.М. Про деякі прояви кіберзлочинності у місцях позбавлення волі;
- Копотун І.М., Довбань І.М. Види кіберзлочинів відповідно до міжнародних нормативних актів;
- Кудінов С.С., Марущак А.І., Петров С.Г. Актуальні кіберзагрози національним інтересам України: протидія і міжнародне співробітництво;
- Левченко Ю.О. Сучасний стан протидії кіберзлочинності в Україні;
- Миронюк Т.В. Сучасний стан та тенденції кіберзлочинності в Україні;
- Настюк В.Я., Бєлєнцева В.В. Особливості правових режимів забезпечення кібербезпеки в Україні;
- Радутний О.Е. Злочини майбутнього та інші загрози кібербезпеці, пов’язані зі штучним інтелектом;
- Ткачова О.В. Міжнародний досвід у сфері інформаційної та кібернетичної безпеки;
- Шаблистий В.В. Способи мінімізації кримінальних загроз безпеці критичної інфраструктури та кібернетичній безпеці людини в Україні;
- Шевчук В.М. Використання інформації із соціальних інтернет-мереж при розслідуванні кіберзлочинів: криміналістичні проблеми;
- Шкута О.О. Кіберзлочинність у місцях несвободи;

- Шило О.Г., Шило А.В. Проблема забезпечення кібербезпеки: чинне законодавство України та сучасні виклики;
- Таволжанський О.В. Деякі аспекти регламентації приватності у кіберпросторі.

Шифр зберігання НБУВ: ВА838033

***

**Сторчак А. С. Метод оцінювання рівня захищеності мережевої частини комунікаційної системи спеціального призначення від кіберзагроз / А. С. Сторчак, С. В. Сальник // Системи обробки інформації. - 2019. - Вип. 3. - С. 98-109.**

Представлено удосконалений метод оцінки рівня захищеності мережевої частини комунікаційної системи спеціального призначення від кіберзагроз на основі алгоритму розподільчої ідентифікації та динамічного програмування. Розролено методу оцінки захищеності інформації, яка обробляється в комунікаційній системі, на основі керованих багатокрокових процесів прийняття рішень, для підвищення ефективності управління захистом інформації, з огляду на характеристики процесу захисту. Визначено величину ризику на кожному етапі процесу захисту і правило вибору засобів захисту, які мінімізують значення ризиків на всіх етапах.

Шифр зберігання НБУВ: Ж70474

***

**Шостак Н. В. Аналіз стійкості стеганографічних методів вбудовування даних в відеофайли до атак / Н. В. Шостак, А. А. Астраханцев // Системи обробки інформації. - 2019. - Вип. 3. - С. 110-116.**

Зроблено порівняльний аналіз сучасних методів вбудовування цифрових водяних знаків (ЦВЗ) у відеофайли з метою виявлення методів з найкращими показниками по стійкості до атак та скритності вбудовування ЦВЗ. Досліджено методи підвищення завадостійкості та стійкості до основних атак.

Шифр зберігання НБУВ: Ж70474