НКЦК

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

ОГЛЯД ПОДІЙ У СУЧАСНОМУ КІБЕРПРОСТОРІ

за І І квартал 2021 року

Нормативно-правовий та організаційний аспекти забезпечення міжнародної кібербезпеки

Продовження дії надзвичайного стану в США через кібератаки

29.03.2021 президент США подовжив дію раніше накладених санкцій для захисту США від кібератак, а також був пролонгований надзвичайний стан.

У зв'язку зі шкідливими діями в кіберпросторі, які здійснюються або контролюються, в основному, особами за межами США і становлять серйозну загрозу національній безпеці, зовнішній політиці й економіці США, Президент країни Джо Байден продовжив дію Указу Executive Order 13694 від 01.04.2015.

Президент США переконаний, що надзвичайний стан у країні через кібератаки повинен тривати і після 01.04.2021. Продовження дії Указу означає, що введені обмеження проти низки країн, що становлять загрозу для США в кіберпросторі, триватимуть ще мінімум рік. Таким чином, за Міністерством фінансів США зберігається право вводити персональні санкції проти осіб, які здійснюють кібератаки проти США, блокувати рахунки і будь-які активи на території країни та відключати їх від національної банківської системи.

Перший Указ про введення в США надзвичайного стану було підписано 01.04.2015 президентом Бараком Обамою. Термін дії режиму санкцій протягом останніх років неодноразово продовжувався владою США. Зокрема, в 2019 році Дональд Трамп підписав Указ про введення в країні режиму надзвичайної ситуації для розширення повноважень влади щодо захисту інформаційно-комунікаційних мереж. Указ забороняв американським компаніям отримувати обладнання іноземних виробників, що становлять загрозу національній безпеці США.

Системна політика США в сфері безпеки у мережі Інтернет

15.04.2021 Президент США підписав Адміністративний Указ “Про протидію шкідливій іноземній діяльності Уряду Росії”, який передбачає “посилення повноважень для демонстрації рішучості Адміністрації США реагувати на шкідливу іноземну діяльність Росії та стримувати її в повному обсязі”. Проте, окремої уваги в документі заслуговують так звані кібернавчання Cyber Flag, які планується проводити на постійній основі. Фактично відбувається поділ всього простору Інтернету на три базові домени безпеки: учасники Cyber Flag, його партнери і супротивники.

В межах базового домена безпеки учасники отримують доступ до безперешкодної маршрутизації і максимальних швидкостей з мінімальним набором перевірок і сертифікування. Мається на увазі як обмін даними, так і здійснення електронних угод і транзакцій.

Для партнерів і союзників буде введено додаткові протоколи безпеки і перелік обмежень. За попередньою інформацією, існуватиме перелік умов, за яких можна буде змінити статус партнера на статус учасника.

Для супротивників буде введено особливий лімітований режим користування глобальними сервісами, встановлено особливі протоколи безпеки і обмеження.

В майбутньому систему буде доповнено рейтингами і рангами. Право присвоєння цих рейтингів, а також контроль за переходами учасників з однієї доменної зони в іншу, США залишають за собою. Наразі Cyber Flag проводиться під егідою Міністерства оборони США, але в подальшому передбачено створення спеціального органу управління (можливо, міжнародний і недержавний), якому передадуть функції контролю над зонами безпеки.

До ініціативи США вже приєднались Великобританія, Німеччина, Данія та Естонія. Україна планує приєднатися до цієї ініціативи у поточному році. У подальшому навчання можуть стати повноцінною організацією – аналогом НАТО в кіберпросторі – зі штаб-квартирою в Німеччині (наразі до ініціативи долучився Європейський Центр дослідження проблем безпеки Джорджа Маршала, що дислокується в м. Гарміш-Партенкірхен, ФРН).

Метою запровадження так званих кібернавчань є створення цифрової нерівності, забезпечення розвитку на випередження одних за рахунок створення бар'єрів та труднощів для всіх інших. Кіберпростір стає зоною економічного розвитку на даному етапі, і США, не відволікаючись на сторонні речі, встановлюють в ньому свою гегемонію.

Щорічна оцінка загроз від американської розвідки

13.04.2021 Офіс директора Національної розвідки США Авріл Гейнс (Avril Haines) оприлюднив доповідь “Щорічна оцінка загроз” (2021 Annual Threat Assessment). Це щорічний документ Національної розвідувальної спільноти щодо загроз національній безпеці США в усьому світі, який складається з 27 сторінок і відображає колективну думку 18 спецслужб країни. Документ містить тільки нетаємну інформацію та приділяє особливу увагу чотирьом країнам: Китаю, Росії, Ірану та Північній Кореї, а також пандемії коронавірусу, тероризму, міграції, кліматичним змінам та кіберзагрозам. Дії Китаю в доповіді названо “претензіями на світове панування”, а трьох інших країн – “провокаційними діями”.

У документі зазначено, що Росія є однією з головних кіберзагроз для США, оскільки вона вдосконалює та використовує можливості кібершпигунства, впливу за допомогою соціальних мереж та здійснення кібератак. Цілями російських злочинних дій в кіберпросторі стають підводні кабелі і промислові системи контролю США та їх союзників і партнерів. Компрометація такої інфраструктури демонструє здатність Росії наносити шкоду об’єктам критичної інфраструктури країни під час кризи.

На думку американських спецслужб, Москва має можливість та намір атакувати державні та приватні організації в США. В доповіді йдеться про те, що Росія використовує кібероперації для захисту від того, що вона вважає загрозами стабільності для свого уряду.

У 2019 році РФ здійснила хакерські атаки на інформаційні ресурси журналістів та організації, які вели розслідування щодо російського уряду, і в одному випадку вона таки змогла отримати інформацію. В американській розвідці також вважають, що Москва використовує свої розвідувальні служби та інструменти впливу, щоб розділити західні союзи, зберегти свій вплив на пострадянському просторі та посилити свій вплив по всьому світу, підриваючи глобальний статус США, сіючи розбрат всередині них та здійснюючи вплив на вибори й прийняття рішень в країнах. Американські спецслужби припускають, що Росія може поділитись своїми технологіями та досвідом з противником США, зокрема постачати своє шкідливе програмне забезпечення. Окрім того, зазначається, що РФ стане ключовим конкурентом країни в сфері космосу та інтегруватиме цю сферу з воєнною.

НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

100-денний план кіберзахисту енергетичної інфраструктури США

20.04.2021 Білий дім оголосив про початок пілотної програми забезпечення кібербезпеки національної енергетичної інфраструктури, що стане першою більш широкою програмою захисту промислових систем управління.

План захисту енергосистем розраховано на 100 днів і включає “агресивні, але досяжні” результати для підвищення можливостей виявлення, пом'якшення наслідків і судової експертизи кібервторгнень.

За виконання програми відповідає Міністерство енергетики та створене в 2018 році Агентство з кібербезпеки і охорони інфраструктури (US Cybersecurity and Infrastructure Security Agency, CISA).

Причиною прийняття 100-денного плану підвищення безпеки систем управління енергетикою стали кіберінциденти на системах водопостачання. Зокрема, ключовою стала подія у Флориді, де хакер мало не отруїв водопровідну воду на об'єкті її очищення, викликавши передозування одного з хімічних компонентів, що використовуються для знезараження води. У березні поточного року Міністерство юстиції США висунуло звинувачення хакеру з Канзасу також через факт втручання в суспільну систему водопостачання. Обвинувачений свідомо зламав сервер цієї системи, зупинивши очистку і дезінфекцію води.

Атаки здирницького програмного забезпечення – загроза національній безпеці США

Адміністрація президента США Джо Байдена має намір розцінювати атаки здирницького програмного забезпечення як загрозу національній безпеці. У зв’язку з цим американські спецслужби стежитимуть за іноземними кіберзлочинцями і розроблятимуть наступальні кібероперації проти хакерів, які перебувають за межами США.

З огляду на такі наміри, Міністерство юстиції США направило до органів прокуратури по всій країні внутрішню інструкцію, у якій зазначено, що інформація про розслідування атак з використанням здирницького програмного забезпечення на місцях повинна централізовано координуватися з нещодавно створеною робочою групою у Вашингтоні.

Такий порядок забезпечить фіксацію всіх випадків використання програм-вимагачів, незалежно від частини країни, з метою встановлення зв’язків між зловмисниками і ліквідації всього злочинного ланцюга.

НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

На практиці це означає, що слідчі прокуратури США, які займаються розслідуванням атак з використанням здирницького програмного забезпечення, повинні будуть ділитися подробицями своїх розслідувань і активною технічною інформацією з керівництвом у Вашингтоні.

Управління прокуратури повинні розглядати й інші справи, зосереджені на екосистемі кіберзлочинності. Перелік розслідувань, які тепер вимагають централізованого інформування, включає кримінальні справи, пов'язані з антивірусними сервісами, незаконними online-форумами, торговими майданчиками, криптовалютними біржами, ботнетами і online-сервісами з відмивання грошей.

Крім того, офіційний Вашингтон планує створити міжнародну коаліцію щодо боротьби з державами, які, на думку США, не вживають належних заходів для подолання кіберзлочинності. Зокрема, розглядається вжиття заходів на чотирьох великих напрямках:

- руйнування інфраструктури зловмисників, які застосовують віруси-здирники;
- активізація взаємодії влади США з приватним сектором з метою зміцнення кібербезпеки;
- створення міжнародної коаліції з метою притягнення до відповідальності країн, що покривають осіб, які вчинили кіберзлочини;
- розширення аналізу криптовалют з метою припинення злочинних транзакцій.

Технологічні компанії проти прийняття антимонопольних законопроєктів в США

Великі технологічні компанії, зокрема Apple, Amazon, Facebook і Google, виступили проти прийняття антимонопольних законопроєктів, запропонованих Палатою представників США, які обмежують владу технологічних компаній.

У разі прийняття, закони стануть найбільш значущими змінами в антимонопольному законодавстві за останні десятиліття. Вони також можуть мати серйозні наслідки для технологічних гігантів, включно з примусовими змінами в способах ведення бізнесу, з вимогами змін в роботі їх продуктів і навіть з поділом компаній. Один закон, зокрема, забороняє технологічним компаніям робити придбання, спрямовані на придушення конкурентів або розширення впливу на ринок.

Другий закон забороняє збирати дані від розробників та інших фірм, що використовують їх платформи. Третій закон зобов'язує компанії дозволяти користувачам легко перемикатися з продуктів однієї технологічної компанії на іншу.

Зазначені технологічні компанії опублікували прес-релізи, в яких пояснили, чим загрожує прийняття таких законів. У заяві, адресованій Конгресу США, компанія Apple, яка жорстко контролює магазин App Store з моменту його запуску в 2008 році, виступила проти положення в одному із законопроєктів, що зобов'язує компанію відкрити свій магазин додатків для сторонніх розробників.

Дозвіл завантаження сторонніх додатків знизить безпеку платформи iOS і піддасть користувачів серйозним ризикам безпеки не тільки в сторонніх магазинах додатків, але і в App Store.

Раніше глава Apple Тім Кук виступив проти законопроєкту ЄС щодо регулювання цифрових ринків, спрямованого на зниження влади технологічних компаній. За його словами, прийняття закону підірве безпеку iPhone.

Кібератаки на членів НАТО як збройний напад

14.06.2021 у штаб-квартирі НАТО в Брюсселі відбувся саміт, під час якого лідери країн НАТО ухвалили рішення, відповідно до якого особливо масштабні кібератаки на членів Альянсу можуть розцінюватися як збройний напад з подальшим застосуванням статті 5 Вашингтонського договору про колективний захист.

Стаття 5 передбачає принцип колективної оборони НАТО – напад на одного учасника Альянсу вважається нападом на всіх країн-членів НАТО і передбачає атаку у відповідь з боку всіх країн Альянсу, в тому числі, із застосуванням збройних сил. Аналогічним чином реагуватимуть і на окремі кіберзлочини.

В Альянсі схвалили Комплексну політику кіберзахисту НАТО, яка підтримуватиме основні завдання НАТО, зокрема в частині загального стримування та захисту, а також посилюватиме стійкість країн. Підтверджуючи оборонний мандат НАТО, країни вирішили у будь-який час використовувати весь спектр можливостей для активного стримування, захисту та протидії кіберзагрозам, включно з тими, що здійснюються в рамках гібридних кампаній, відповідно до міжнародного права

Надалі учасники саміту запланували ширше використовувати НАТО як платформу для політичних консультацій між членами Альянсу щодо зловмисної кібердіяльності, обмінюючись національними підходами та методами реагування, а також розглядаючи можливі колективні відповіді.

Рекомендації щодо забезпечення безпеки підключень IT-OT

Агентство національної безпеки США (АНБ) опублікувало рекомендації з кібербезпеки операційних технологій стосовно підключення до IT-систем.

Рекомендація АНБ Stop Malicious Cyber Activity Against Connected Operational Technology (“Зупинити зловмисну кіберактивність проти підключених операційних технологій”) адресована Міністерству оборони США, системам національної безпеки (National Security Systems, NSS) і основним організаціям оборонної промисловості.

У документі наводяться рекомендації з оцінки ризиків і підвищення безпеки підключень між IT-системами, які часто можуть бути точкою входу в промислові мережі, і системами операційних технологій

Для забезпечення максимальної кібербезпеки не повинно бути з'єднань між корпоративними мережами і мережами операційних технологій, але Агентство визнає, що в деяких випадках такі з'єднання є необхідними. Таким чином, організаціям рекомендовано перевірити підключення та видалити ті, які не потрібні.

Заходи, наведені в рекомендаціях, передбачають повне управління всіма підключеннями операційних технологій до IT-систем, обмеження доступу, активний моніторинг і реєстрацію всіх спроб доступу, а також криптографічний захист векторів віддаленого доступу.

Окрім того, розвідувальні служби Великобританії та США підготували низку рекомендацій для захисту від хакерів, афілійованих зі Службою зовнішньої розвідки (СЗР) РФ. Доповідь було оприлюднено 07.05.2021 урядовим Національним центром кібербезпеки Великобританії (National Cyber Security Center) у співпраці з Агентством національної безпеки (National Security Agency) США, американськими міністерством юстиції та Агентством з кібербезпеки та забезпечення захисту інфраструктури (Cybersecurity and Infrastructure Security Agency).

НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

В доповіді йдеться про те, що СЗР РФ використовує різноманітні інструменти та методи для отримання розвідувальної інформації за допомогою кібератак на закордонні урядові, дипломатичні, аналітичні центри, а також медичні та енергетичні установи. В розвідках Великобританії та США вважають, що цих потужностей достатньо, щоб здійснювати кібератаки на цілі не тільки в цих двох країнах, а й в континентальній Європі, державах-членах НАТО, а також на території країн-сусідів Росії.

Для захисту від атак рекомендується оперативно встановлювати оновлення, що виправляє вразливість в програмному забезпеченні, яке використовується; відстежувати підозрілі електронні листи; застосовувати двоетапну перевірку. Також автори доповіді радять обмежити кількість конфіденційної інформації, яку можуть викрасти зловмисники, обмежити права користувачів і роз'яснити їм принципи мережевої безпеки.

Крім того, експерти, зокрема, звертають увагу на те, що кіберагенти намагаються використовувати інструмент з відкритим вихідним кодом Silver для забезпечення доступу до скомпрометованих мереж та вразливості програмного продукту Microsoft Exchange.

Створення головного центру інформаційних технологій Військ нацгвардії РФ

23.04.2021 голова уряду Михайло Мішустін підписав розпорядження № 1039-р “Про створення федеральної державної урядової установи Головний центр інформаційних технологій Військ національної гвардії Російської Федерації”.

Основними цілями діяльності установи є створення, розвиток і експлуатація інформаційних систем, програмного забезпечення та інформаційно-комунікаційної інфраструктури, використання інформаційно-комунікаційних технологій, а також забезпечення інформаційної безпеки та технічного захисту інформації у Військах національної гвардії.

Повноваження засновника головного центру інформаційних технологій і його фінансування покладається на Федеральну службу військ національної гвардії РФ, яка повинна у тримісячний термін затвердити статут, забезпечити державну реєстрацію установи і організувати роботу центру.

Федеральна служба військ національної гвардії РФ (Росгвардія) є центральним органом управління військами національної гвардії РФ (ВНГ Росії), створеними на основі Внутрішніх військ МВС Росії. Відноситься до державних воєнізованих організацій.

Крім того, Міністерство оборони Російської Федерації найближчим часом планує створити спеціалізоване управління, яке займатиметься питаннями розвитку штучного інтелекту, елементи якого використовуються в комплексах БПЛА і наземної техніки. Про це представники відомства заявили в рамках засідання робочої групи з проблем розвитку комплексів з безпілотними літальними апаратами військового призначення. Захід відбувся на базі конструкторського бюро компанії “Сухой”.

В ході цього заходу на обговорення було винесено питання, що стосуються напрямків інтелектуалізації безпілотних літальних апаратів під час групової експлуатації.

Представники найбільших підприємств-виробників БПЛА, в свою чергу, поінформували про останні розробки, що дають змогу впроваджувати технології штучного інтелекту в військову техніку і техніку подвійного використання.

Створення центру з дослідження безпеки операційних систем на базі Linux

Федеральна служба з технічного та експортного контролю (ФСТЕК) уклала контракт з Інститутом системного програмування ім. В.П. Іваннікова РАН на створення центру з дослідження безпеки операційних систем на базі ядра Linux (ціна контракту – 300 мільйонів рублів). Технологічний центр повинен бути готовий до кінця 2023 року.

Як вказано в технічному завданні, у новому центрі російські програмісти працюватимуть над підвищенням якості та безпеки ядра Linux. Це допоможе знизити “можливі соціально-економічні наслідки від реалізації комп'ютерних атак на критичну інформаційну інфраструктуру Російської Федерації”.

Крім того, новий технологічний центр буде вдосконалювати російські засоби розробки та тестування програмного забезпечення, підвищувати кваліфікацію фахівців і розвивати нормативне та методичне забезпечення процесів безпечної розробки в РФ.

Згідно з планом-графіком, у 2021 році мають бути розроблені та експериментально обґрунтовані вимоги до організаційних, методичних та науково-методичних основ функціонування технологічного центру дослідження безпеки операційних систем на базі ядра Linux, а у 2022 році заплановано його безпосереднє створення, у тому числі за участю розробників операційних систем.

У 2023 році центр повинен бути введений в експлуатацію; організовано наповнення банку даних загроз безпеці інформації ФСТЕК відомостями про вразливості в операційних системах, створених на базі ядра Linux.

Створення центру фінансується з федерального бюджету в рамках федерального проекту “Інформаційна безпека” національної програми “Цифрова економіка”.

Регулювання роботи соціальних мереж з персональними даними в РФ

Міністерство цифрового розвитку, зв’язку і масових комунікацій РФ (Мінцифри) має намір запропонувати поправки до Федерального Закону № 152-ФЗ від 27.07.2006 “Про персональні дані”, які введуть окремий режим регулювання персональних даних для соціальних мереж.

Про це зазначив Міністр цифрового розвитку РФ Максут Шадаєв 7 квітня поточного року на Російському форумі з управління мережею Інтернет. На його думку, це питання надання згоди на обробку персональних даних в соціальних мережах і, як наслідок, необхідність підтвердження такої згоди.

Поправки передбачають спрощення процедури ідентифікації користувачів, а також вирішення проблеми накопичення соціальними мережами великої кількості персональних даних користувачів, які надходять до них відповідно до вищезазначеного закону про персональні дані. Поправки повинні створити умови, які забезпечуватимуть захист даних користувачів, зокрема:

- з’явиться спеціальна форма згоди, яку встановлюватиме Роскомнагляд;
- користувач може попросити видалити його персональні дані в будь-який час (раніше потрібно було обов’язково вказати причину);
- вдвічі збільшаться штрафи за порушення закону.

Окрім цього, обговорюється можливість авторизації в соціальних мережах через портал державних послуг. Проте, обов’язковою умовою такої авторизації є недоступність даних користувача для самих сервісів. В цьому випадку соціальна мережа не має доступу до інформації облікового запису на порталі державних послуг.

Варто також зазначити, що власникам Google, Twitter, Facebook і WhatsApp надано час до кінця травня поточного року, щоб локалізувати на території РФ бази даних своїх російських користувачів.

У разі відмови або відсутності відповідей з боку соціальних мереж буде вирішуватися питання про притягнення їх до відповідальності за порушення російського законодавства. Компанії можуть бути зобов'язані виплатити штрафи в розмірі від 1 до 6 мільйонів рублів. За повторне порушення розмір штрафу збільшиться до 18 мільйонів рублів.

Відповідну норму ввели в Кодекс про адміністративні правопорушення РФ в грудні 2019 року. Компанії Twitter і Facebook відмовляються локалізувати дані російських користувачів на території РФ, за що неодноразово були оштрафовані відповідно до рішень російських судів. Проте, є й такі іноземні компанії (зокрема, Apple, Microsoft, Samsung, PayPal, Booking.com, LG), які вже підтвердили локалізацію даних російських користувачів на території РФ.

Основи державної політики РФ в галузі інформаційної безпеки

12.04.2021 Президент РФ Володимир Путін Указом № 213 затвердив Основи державної політики в галузі міжнародної інформаційної безпеки. Документ стратегічного планування визначає основні загрози в галузі міжнародної інформаційної безпеки, мету, завдання державної політики РФ в цій сфері, а також основні напрямки її реалізації.

До загроз міжнародній інформаційній безпеці віднесено використання інформаційно-комунікаційних технологій у військово-політичній та інших сферах з метою підриву (обмеження) суверенітету, порушення територіальної цілісності держав, здійснення в глобальному інформаційному просторі інших дій, що перешкоджають підтриманню міжнародного миру, безпеки і стабільності; використання IT-технологій з терористичною й екстремістською метою, а також для втручання у внутрішні справи суверенних держав.

Раніше Путін розповів про позицію Росії в галузі інформаційної безпеки. За його словами, країна виступає за універсальні міжнародні домовленості щодо попередження конфліктів в кіберсфері. Глава країни підкреслив, що нова редакція документа повинна зберегти курс РФ на запобігання конфліктів в кіберпросторі.

Введення штрафів за порушення при захисті критичної інфраструктури

26.05.2021 Президент РФ Володимир Путін підписав закон № 141-ФЗ “Щодо внесення змін до Кодексу Російської Федерації про адміністративні правопорушення”, який передбачає штрафи за порушення вимог законодавства у сфері безпеки критичної інформаційної інфраструктури.

У Кодекс РФ про адміністративні правопорушення вносяться зміни, згідно з якими порушення вимог до створення систем безпеки значущих об'єктів критичної інформаційної інфраструктури, забезпечення їх роботи і безпеки в рамках чинних законів і регламентів спричинить накладення штрафу на посадових осіб в розмірі від 10 до 50 тисяч рублів, на юридичних осіб – від 50 до 100 тисяч рублів.

Порушення порядку інформування про комп'ютерні інциденти, реагування на них, вжиття заходів щодо ліквідації наслідків комп'ютерних атак загрожуватиме посадовим особам штрафом в розмірі від 10 до 50 тисяч рублів, а юридичним особам – від 100 тисяч до 500 тисяч рублів

Крім того, законом передбачено відповідальність за порушення порядку обміну інформацією про комп'ютерні інциденти між суб'єктами інфраструктури та уповноваженими органами іноземних держав, міжнародними організаціями, міжнародними неурядовими та іноземними організаціями, що здійснюють діяльність в сфері реагування на комп'ютерні інциденти. Нові норми наберуть чинності 01.09.2021.

Контроль за компаніями, що використовують VPN

14.05.2021 Федеральна служба з нагляду у сфері зв’язку, інформаційних технологій і масових комунікацій РФ (Роскомнагляд) зобов’язала організації повідомляти про використання ними сервісів обходу блокувань (VPN).

В Роскомнагляді повідомили, що направили у відомства запит з проханням інформувати Центр моніторингу та управління мережею зв'язку загального користування про використання підприємствами і організаціями сервісів VyprVPN і Opera VPN. Вжиття таких заходів здійснюється в рамках створення в РФ централізованої системи для боротьби з обходом блокувань.

НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

Запит стосовно інформування про плановане введення централізованого управління щодо засобів обходу обмеження забороненої в рамках закону інформації став наслідком подій 27.03.2019. Тоді Роскомнагляд направив вимоги про необхідність підключення до Федеральної державної інформаційної системи, що містить реєстр забороненої в Росії інформації, власникам 10 VPN-сервісів для фільтрації трафіку. Однак 9 з 10 VPN-сервісів не виконали зазначених вимог.

Стратегія розвитку програмного забезпечення з відкритим кодом в РФ

Міністерство цифрового розвитку, зв'язку і масових комунікацій РФ (Мінцифри) спільно з російськими IT-компаніями планують до вересня 2021 року розробити стратегію розвитку в Росії програмного забезпечення з відкритим кодом.

Документ повинен визначати перелік необхідних заходів з державної підтримки розвитку open source, зокрема: доцільність прямого фінансування; вид регулювання; потреба у підтримці через державне замовлення. Також тривають дискусії щодо доцільності внесення програм на основі open source до реєстру російського програмного забезпечення. Стратегія розвитку складатиметься на основі спільної роботи з учасниками ринку інформаційних технологій.

Наразі у держави є три пріоритети з розвитку відкритого програмного забезпечення: гнучкість в розробці, безпека, а також незалежність від західних компаній і можливих санкцій.

Припускається, що в Росії може бути відкрито власне сховище (репозиторій) проєктів з відкритим кодом – аналог сервісу GitHub, який є найбільшим ресурсом для хостингу IT-проєктів і їх спільної розробки.

Крім того, в Росії планують створити Національну платформу відеоспостереження (в єдиний контур системи об'єднають всі розумні камери, що працюють в російських містах). При створенні зазначеної платформи будуть використані камери, що працюватимуть в єдиному контурі, оснащені обчислювальними модулями, які дозволять самостійно розпізнавати підозрілі ситуації, в тому числі, злочини, і тільки згодом відправлятимуть відеопотік в ЦОД.

Джерелом фінансування масштабного проєкту може стати державна корпорація "ВЭБ.РФ" (російська державна корпорація розвитку, державний інвестиційний банк, що фінансує проєкти розвитку економіки).

Німецькі правозахисні організації розкритикували новий закон про стеження

22.06.2021 року влада Німеччини прийняла закон “Про конституційний захист”, який значно розширює можливості стеження для німецьких спецслужб та дозволяє їм встановлювати на пристрої користувачів шпигунське програмне забезпечення.

Правозахисна організація Digitale Gesellschaft опублікувала лист, в якому критикує використання спецслужбами державних троянів для здійснення прослуховування і розширення повноважень Федерального управління із захисту Конституції в частині спостереження. Представники організації стверджують: якщо секретні служби забажають використовувати оновлення безпеки для інсталяції шкідливих програм у майбутньому, це підірве всі зусилля зі встановлення безпечної і свідомої комунікації в мережі Інтернет.

Особливу увагу привернуло надання дозволу на використання державних троянів для моніторингу вихідних телекомунікаційних даних, за допомогою яких, зокрема, збережені зашифровані повідомлення повинні маршрутизуватися і контролюватися безпосередньо на кінцевих пристроях користувачів. При цьому, законом дозволяється не тільки відстежувати поточну комунікацію, але і в деяких випадках використовувати збережені повідомлення ретроспективно. Це не лише є серйозним посяганням на права користувачів, але й підриває безпеку зв’язку в цілому, оскільки влада зламує пристрої і використовує недоліки в безпеці замість того, щоб ліквідувати їх.

Влада Ізраїлю і ОАЕ обмінялися розвідданими про кібератаки

В рамках співробітництва між Ізраїлем і Об'єднаними Арабськими Еміратами, влада обох країн здійснила обмін розвідданими й інформацією щодо кіберактивності угруповання Lebanese Cedar, пов'язаного з ліванською воєнізованою організацією Хезболла.

НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

Директор управління кібербезпеки Об'єднаних Арабських Еміратів Мухаммед аль-Кувейт зазначив, що обміну підлягала інформація щодо механізмів захисту, тактики, методів і процедур, які використовувалися зловмисниками, а також схеми атак та унікальні сигнатури, що дозволяють ідентифікувати злочинців. Варто зазначити, що в січні поточного року стало відомо про злам низки операторів зв'язку й Інтернет-провайдерів в США, Великобританії, Ізраїлі, Єгипті, Саудівській Аравії, Лівані, Йорданії, ОАЕ і Палестинської національної адміністрації. Шкідлива операція стартувала на початку 2020 року і тривала майже рік.

Наразі сторони занепокоєні тим, що через поліпшення відносин ОАЕ з Ізраїлем існує підвищена загроза здійснення кібератак на інфраструктурні об’єкти обох країн.

Нова стратегія кібербезпеки Сінгапуру

На відкритті кіберзаходу Singapore International Cyber Week прем’єр-міністр Сінгапуру Лі Сянь Лун оголосив про розробку нової стратегії щодо забезпечення кібербезпеки, спрямовану на створення стійкого кіберсередовища у країні.

Раніше уряд вже повідомляв, що в країні розроблено новий законопроєкт про кібербезпеку (Cybersecurity Bill), який набере чинності у 2022 році. Відповідно до його норм, більше 100 тисяч комп’ютерів в державних службах не матимуть доступу до мережі Інтернет. У такий спосіб влада країни прагне забезпечити захищеність основних служб Сінгапуру за допомогою реалізації процесів управління кіберризиками і планів з відновлення критично важливих секторів.

З огляду на зазначене, нову стратегію буде сфокусовано на побудові стійкої інфраструктури, створенні безпечного кіберпростору, розвитку екосистеми кібербезпеки і посиленні міжнародного співробітництва.

Як підтвердження своїх намірів, уряд виділить 8% бюджетних коштів для розвитку технологій та на витрати із забезпечення кібербезпеки, що майже вдвічі більше в порівнянні з аналогічними витратами попередніх років. Для підвищення кібербезпеки в регіоні загалом Сінгапур також повідомив про інвестування 10 мільйонів сінгапурських доларів в ASEAN Cyber Capacity Programme. Уряд сподівається забезпечити партнерів в Південно-Східній Азії необхідними ресурсами і навчити готувати кадри для створення власних внутрішніх структур в галузі кібербезпеки.

Крім цього, Сінгапур виступає спонсором проєкту CyberGreen, який допомагає країнам бути більш обізнаними про стан кібербезпеки в їх регіоні. Завдяки спонсорству Сінгапуру всі країни-учасники ASEAN зможуть отримати доступ до CyberGreen безкоштовно.

Загрози глобальній кібербезпеці та заходи з їх запобігання, локалізації і ліквідації

Топ-5 вразливостей з арсеналу російських хакерів

Агентство національної безпеки США, Агентство з кібербезпеки і безпеки інфраструктури і Федеральне бюро розслідувань надали перелік з п'яти вразливостей, що експлуатуються російськими хакерами в атаках на американські організації.

Як повідомляє АНБ, зловмисники використовують ці вразливості в громадських сервісах з метою викрадення облікових даних для подальшої компрометації комп'ютерних мереж американських компаній і урядових установ.

У зв'язку з цим агентство рекомендувало всім організаціям негайно встановити виправлення на вразливі пристрої, щоб уникнути можливих витоків даних, банківського шахрайства і атак програм-вимагачів.

В опублікований американськими спецслужбами перелік включено такі вразливості.

- CVE- 2018-13379 – вразливість в версіях Fortinet FortiOS з 6.0.0 по 6.0.4, з 5.6.3 по 5.6.7 і з 5.4.6 по 5.4.12. Некоректне обмеження шляху до Restricted Directory в web-порталах Fortinet Secure Sockets Layer (SSL) Virtual Private Network (VPN) дозволяє неавторизованому зловмисникові завантажувати системні файли за допомогою сконфігурованих особливим чином HTTP-запитів ресурсів.

Хакери активно експлуатують цю вразливість в атаках на урядові й корпоративні мережі, включно з атаками на електронні системи для голосування, організації, які проводять дослідження COVID-19, а також для встановлення здирницького програмного забезпечення Cring. У листопаді 2020 року облікові дані майже 50 тисяч користувачів Fortinet VPN було виставлено на продаж на хакерському форумі.

- CVE-2019-9670 – вразливість в версіях Synacor Zimbra Collaboration Suite 8.7.x до 8.7.11p10. Ін'єкція зовнішніх сутностей XML (XML External Entity injection, XXE) в компоненті mailboxd. Угруповання APT29 використовує її в атаках на організації, що займаються розробкою вакцин проти COVID-19.

- CVE-2019-19781 – вразливість обходу каталогу в версіях Citrix ADC і Gateway до 13.0.47.24, 12.1.55.18 , 12.0.63.13, 11.1.63.15 і 10.5.70.12, а також в SD-WAN WANOP 4000-WO, 4100-WO, 5000-WO і версіях 5100-WO до 10.2.6b і 11.0.3b.

Вразливість експлуатується для отримання доступу до корпоративних мереж і розгортання в них шкідливих програм. Угруповання APT29 використовує її в атаках на організації, що займаються розробкою вакцин проти COVID-19.

- CVE-2020-4006 – вразливість впровадження команд в версіях VMware One Access 20.01 і 20.10 для Linux, VMware Identity Manager 3.3.1 - 3.3 .3 для Linux, VMware Identity Manager Connector 3.3.1 - 3.3.3 і 19.03, VMware Cloud Foundation 4.0 - 4.1 і VMware Vrealize Suite Lifecycle Manager 8.x.

У грудні 2020 року влада США попереджала про експлуатацію цієї вразливості російськими хакерами для розгортання web-оболонок на вразливих серверах і викрадення даних.

Пошук зламаних серверів Microsoft Exchange

На початку квітня поточного року Агентство з кібербезпеки та безпеки інфраструктури США (Cybersecurity and Infrastructure Security Agency) наказало федеральним агентствам повторно просканувати свої мережі на предмет будь-яких ознак зламу локальних серверів Microsoft Exchange і повідомити про результати у п’ятиденний термін.

Відповідно до директиви CISA Emergency Directive 21-02, федеральні агентства повинні терміново здійснити оновлення або відключити локальні сервери Exchange у зв'язку з виявленням критичних вразливостей ProxyLogon.

Зокрема, федеральним департаментам і агентствам необхідно запустити скрипт Microsoft Test-ProxyLogon.ps1 та інструмент Microsoft Safety Scanner (MSERT) для виявлення факту зламу серверів Microsoft Exchange.

За наявною інформацією, вразливості ProxyLogon розпочало активно використовувати APT-угруповання Hafnium, що працює на китайський уряд. Після Hafnium експлуатувати такі вразливості почали хакерські групи APT27, Bronze Butler/Tick і Calypso, які підтримує Китай, а також угруповання Winnti Group, Tonto Team та Mikroceen

У директиві також зазначено, що державним органам потрібно забезпечити додатковий захист локальних серверів Exchange до 28.06.2021. Обов'язкові заходи щодо посилення захисту включають підготовку міжмережевих екранів, встановлення оновлень протягом 48 годин після їхнього випуску, використання тільки ліцензійних та сумісних версій програмного забезпечення, налаштування ведення логів і встановлення захисту від шкідливих програм на всіх локальних серверах.

Федеральне бюро розслідувань США, в свою чергу, 13.04.2021 отримало дозвіл на доступ до сотень комп'ютерів на території США з вразливими версіями Microsoft Exchange Server з метою видалення встановлених хакерами web-оболонок.

Це наочний приклад того, які проактивні заходи можуть вживатися правоохоронними органами в разі масштабних хакерських операцій.
Таким чином, ФБР має судовий дозвіл на доступ до комп'ютерів для видалення артефактів більш ранньої хакерської активності, чим може заблокувати зловмисникам подальший доступ до цільових систем.

Видалення web-оболонки відбувається шляхом відправки серверу команди, яка змушує його видаляти тільки ту web-оболонку, яка ідентифікована унікальним шляхом до файлу. Web-оболонка – це інтерфейс, відкритий хакерами для зв'язку з вразливою системою в майбутньому. ФБР виправляло лише вразливості, не видаляючи будь-які інші додаткові програми.

Вразливості в WhatsApp дозволяють віддалено зламати телефон

У версії популярного месенджера WhatsApp для Android були виявлено дві небезпечні уразливості. Їх експлуатація дозволяє віддалено виконати шкідливий код на пристрої і викрасти конфіденційну інформацію. Проблеми поширюються на пристрої під керуванням операційної системи всіх версій до Android 9 включно і пов'язані з тим, як програмне забезпечення здійснює обмін конфіденційними даними із зовнішнім сховищем пристрою.
Вразливості в WhatsApp дозволяють віддалено викрадати криптографічні дані TLS-протоколу для сеансів TLS 1.3 і TLS 1.2. Володіючи секретами TLS-протоколу, проведення MitM-атаки може призвести до компрометації комунікацій WhatsApp, віддаленого виконання коду на пристрої жертви і викрадання ключів протоколу Noise для наскрізного шифрування.

Зокрема, одна з вразливостей (CVE-2021-24027) використовує підтримку Chrome для постачальників контенту в Android (через схему URL-адреси “content://”) і вразливість обходу політики в браузері (CVE-2020-6516), дозволяючи зловмисникові відправити жертві спеціально створений HTML-файл через WhatsApp, який при відкритті в браузері виконує код. Шкідливий код може використовуватися для доступу до будь-якого ресурсу в незахищеній зовнішній області зберігання, включно з ресурсами WhatsApp і даними ключа TLS-сеансу в підкаталозі.

НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

Озброївшись ключами, зловмисник може організувати MitM-атаку для віддаленого виконання коду або викрадення пари ключів протоколу Noise, які використовуються для управління зашифрованим каналом зв'язку між клієнтом і сервером на транспортному рівні безпеки.

Коли виникає такий збій в роботі, механізм налагодження WhatsApp завантажує закодовані пари ключів разом з основними тілами додатків, системною інформацією та іншим вмістом пам'яті на виділений сервер логів збоїв (crashlogs.whatsapp.net).

Хоча процес налагодження призначений для перехоплення критичних проблем в додатку, MitM-атака ініціює дане завантаження тільки для того, щоб перехопити з'єднання і розкрити всю конфіденційну інформацію, призначену для відправки у внутрішню інфраструктуру WhatsApp.

Росія – світовий лідер з фейкової активності в соцмережах

Згідно з даними Центру стратегічних комунікацій НАТО, російські компанії домінують на ринку маніпуляцій інформацією у соціальних мережах. Фахівці Центру визначили, що майже всі основні постачальники програмного забезпечення та інфраструктури для аналогічних платформ мають російське походження.

За оцінками аналітиків, загальний відсоток фейкової активності у соціальних мережах може становити 10 – 30% від усіх “лайків”, репостів та переглядів.

Директор Центру стратегічних комунікацій НАТО Яніс Сартс зазначає, що найбільш захищеною від маніпуляцій є соціальна мережа Twitter. Другою за захищеністю є соціальна мережа Facebook. Мережа Instagram, яка передбачає публікацію фотознімків, та популярний відеохостинг YouTube є недостатньо захищеними від маніпуляцій.

Найменш захищеною мережею від маніпуляцій серед тих, що досліджувались експертами НАТО, є TikTok – базується на публікації коротких відеороликів.

НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

Відслідковування діяльності кіберслужб швидкого реагування США

Протягом декількох місяців, поки офіційні особи США не знали про кібератаку на американські державні установи через програмне забезпечення SolarWinds (злам сотень об'єктів федеральної та регіональної інфраструктури США, включно з Державним департаментом, Міністерством фінансів, Міністерством енергетики), російські хакери визначили кількох ключових аналітиків Міністерства національної безпеки США, які повинні були стати одними з перших, хто відреагує на виявлення факту зламу систем. Після цього хакери намагалися отримати доступ до їхньої електронної пошти.

Вартим уваги є той факт, що зловмисники знали, до яких саме аналітиків в Міністерстві національної безпеки США слід звернутися, тому американські фахівці припускають, що хакери володіють більш глибоким розумінням системи кіберзахисту в США, ніж про це було відомо раніше

Хакери в режимі реального часу могли відстежити, коли офіційні особи в США виявили атаку, і це дозволило їм адаптувати свої дії і залишатися непоміченими якомога довше. Колишній співробітник американського Агентства національної безпеки (АНБ) і військовий аналітик Седрік Лейтон радить співробітникам Міністерства національної безпеки США “повністю оновити систему всіх захисних кібероперацій”.

У свою чергу, Великобританія офіційно повідомила, що відповідальною за кібератаки на IT-компанію Solar Winds є Служба зовнішньої розвідки РФ.

Глава Міністерства закордонних справ Великобританії Домінік Рааб зазначив, що дії Кремля роблять Росію найсерйознішою загрозою національної безпеки Британії. Тому Сполучене Королівство разом з США та іншими партнерами боротиметься з агресивними діями Кремля, включно з кібератаками і втручаннями у вибори.

Китайське угруповання Cycldek вдосконалює свої можливості

У 2020-2021 роках хакерське угруповання Cycldek атакувало урядові та військові організації в країнах Південно-Східної Азії. Угруповання продемонструвало вдосконалені техніки атаки в нещодавній злочинній кампанії проти організацій В’єтнаму.

НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

Cycldek (інші назви Goblin Panda, Conimes), яке активне з 2013 року, у червні 2020 року використовувало спеціально створене шкідливе програмне забезпечення для викрадення даних з фізично ізольованих комп'ютерів. У нещодавній хвилі атак угруповання показало ще більш вдосконалені можливості. Зокрема, шкідлива кампанія, яка тривала з червня 2020 року по січень 2021 року, здійснювалась з використанням завантаження DLL сторонніми каналами для доставки в систему шкідливого коду, який розгортав троян для віддаленого доступу (RAT) та надавав хакерам повний контроль над комп'ютером.

В ході атак на в'єтнамські організації зловмисники використали легітимний компонент Microsoft Outlook для завантаження DLL з метою подальшого впровадження shell-коду, який відігравав роль завантажувача трояна FoundCore RAT.

Після розгортання він запускав чотири процеси: один – для постійної присутності на системі в ролі сервісу, другий – для приховування першого процесу, третій – для попередження доступу до шкідливого файлу та четвертий – для встановлення зв'язку з C&C-сервером.

FoundCore RAT надає злочинцям повний контроль над системою, яку атакують.

Троян підтримує велику кількість різних команд, дозволяючи маніпулювати файловою системою та процесами, виконувати довільні команди, робити знімки екрану. Крім того, в ході атак хакери використовували шкідливе програмне забезпечення DropPhone та CoreLoader.

Зростання кількості атак на вбудоване програмне забезпечення

Протягом двох останніх років більше 80% компаній зазнали хакерських атак на вбудоване програмне забезпечення, але тільки 29% бюджетних коштів корпоративної безпеки спрямовано на усунення даного типу вразливостей.

Такі висновки наведено у дослідженні з інвестицій в безпеку вбудованого програмного забезпечення, проведеного компанією Security Signals в партнерстві з Microsoft. Згідно з дослідженням, існує два види організацій: ті, які зазнали атаки на вбудоване програмне забезпечення, і ті, які зазнали атаки на вбудоване програмне забезпечення, але поки не знають про це.

Переважна більшість (82%) респондентів Security Signals повідомила, що у них немає ресурсів, які можна було б спрямувати на більш ефективну роботу із забезпечення безпеки, оскільки компанії витрачають занадто багато часу на низькорівневу ручну роботу, зокрема: оновлення програмного і апаратного забезпечення, тестування патчів безпеки, а також аудит і усунення внутрішніх і зовнішніх вразливостей. 21% фахівців визнають, що дані їх прошивок залишаються сьогодні без контролю і захисту.

У дослідженні також зазначено, що поточні інвестиції йдуть на оновлення системи безпеки, виявлення вразливостей і вдосконалення рішень для захисту від загроз. Однак багато організацій стурбовані наявністю шкідливих програм, що дозволяють отримувати доступ до корпоративних систем, а також труднощів у виявленні загроз, що говорить про складність моніторингу та контролю вбудованого програмного забезпечення. Проблема також ускладнюється:

- недостатньою обізнаністю про загрози – вбудоване програмне забезпечення стає пріоритетною мішенню для хакерів, адже в ньому зберігається конфіденційна інформація, зокрема облікові дані і ключі шифрування;
- відсутністю автоматизації захисту – фактор, який змушує організації втрачати час і відволікає їх від розробки більш ефективних стратегій превентивної захисту.

Найголовнішим висновком з доповіді Security Signals є те, що прагнуть мати більш проактивні стратегії в галузі безпеки, особливо коли мова йде про боротьбу з атаками на вбудоване програмне забезпечення. Для задоволення цих потреб компанія Microsoft спільно з партнерами створила новий клас пристроїв, спеціально призначених для усунення загроз, спрямованих на вбудоване програмне забезпечення, під назвою Secured-core PC. Вони забезпечують комплексний захист електроживлення з такими можливостями, як Virtualization-Based Security, Credential Guard і Kernel Direct Memory Access (DMA).

Зміна програми обміну інформацією про вразливості через атаки на Microsoft Exchange

Компанія Microsoft розглядає можливість внесення змін до своєї програми обміну даними про загрози і вразливості. Як вважають в компанії, саме ця програма могла стати ключовим фактором у масових атаках на сервери Exchange в березні поточного року.

Microsoft Active Protections Program (MAPP) – програма для постачальників програмного забезпечення і партнерів, що надає їм ранній доступ до даних про вразливість й інші загрози до моменту їх публікації. Мета MAPP, учасниками якої є 81 організація, – забезпечити можливість для компаній розробити стратегії і розгорнути відповідні оновлення до того, як про вразливість стане відомо широкому загалу.

Зокрема, учасникам програми надається пакет документів з усіма відомими компанії Microsoft подробицями про вразливість, що також включають інструкції з відтворення і виявлення вразливостей. У деяких випадках компанія також надає PoC-експлоїти й інші інструменти для кращого розуміння вразливості і розробки виправлення.

Не зважаючи на очевидні переваги MAPP, останнім часом програма потрапила під пильну увагу експертів, оскільки вона могла стати (випадково або навмисно) причиною витоку експлоїта, який в подальшому використовувався в атаках на сервери Exchange.

Microsoft розглядає можливість перегляду програми і, зокрема того, як і коли вона буде надавати партнерам дані про вразливість. За наявною інформацією, компанія підозрює, що учасники MAPP могли "підказати" зловмисникам про наявність вразливостей в Exchange після того, як їм стало відомо про них від Microsoft в лютому 2021 року. Наразі триває розслідування відносно як мінімум двох китайських компаній.

MAPP встановлює для учасників різні рівні доступу, що визначають, яку інформацію буде передано і в який термін. Можливі зміни в програмі можуть включати зміну черговості учасників і їх рівень доступу; переоцінку того, якою інформацією Microsoft ділитиметься в майбутньому; додавання так званих "водяних знаків", що дозволять відслідковувати передачу даних і будь-які подальші факти витоку.

DDoS-атаки на МВС та IT-мережі уряду Бельгії

04.05.2021 велику частину IT-мереж бельгійського уряду було відключено в результаті потужної DDoS-атаки, через що його внутрішні системи і публічні сайти виявилися недоступними.

Атака стосувалася Інтернет-провайдера Belnet, який фінансується державою. Його послугами користуються урядові організації, в тому числі парламент, освітні установи, міністерства і дослідницькі центри. Інцидент позначився на роботі більше 200 організацій, зокрема офіційного порталу для подачі податкових декларацій My Minfin і IT-системи, яку використовують школи та університети для віддаленого навчання. Крім того, портал резервування вакцини проти COVID-19, хостинг якому надає Belnet, був недоступний. Парламентські та інші урядові заходи було скасовано, оскільки їх не можна було транслювати для віддалених учасників.

Кілька бельгійських політиків і політичних спостерігачів зазначили, що атака почалася приблизно в той же час, коли Комітет у закордонних справах парламенту Бельгії повинен був провести засідання і заслухати показання свідків в одній зі справ.

Крім того, масштабної кібератаки зазнали сервери Міністерства внутрішніх справ Бельгії. Хоча хакери атакували цілеспрямовано, вони не отримали доступу до найбільш важливих конфіденційних даних, що зберігаються на надійно захищених серверах. Федеральному прокурору було доручено встановити, звідки велася атака, яку інформацію змогли здобути хакери і чи причетна до атаки конкретна держава

Атака на російського розробника атомних підводних човнів.

Кіберзлочинна група, яка імовірно працює на китайський уряд, атакувала російське оборонне підприємство, що займається розробкою атомних підводних човнів для військово-морського флоту Росії.

Фішинговий лист, відправлений зловмисниками генеральному директору санкт-петербурзького конструкторського бюро “Рубін”, використовував інструмент для створення RTF-експлоїтів Royal Road для доставки на систему, що атакується, раніше невідомого бекдора для Windows під назвою PortDoor.

За словами фахівців команди Nocturnus компанії Cybereason, бекдор PortDoor наділений широкими функціональними можливостями і здатний здійснювати розвідку, доставляти додаткове корисне навантаження, підвищувати привілеї, обходити антивірусне програмне забезпечення, використовувати однобайтове шифрування XOR, отримувати доступ до даних, зашифрованих з використанням стандарту AES.

Протягом багатьох років експлоїти Royal Road є улюбленим інструментом низки китайських хакерських угруповань, зокрема Goblin Panda, Rancor Group, TA428, Tick і Tonto Team, які використовують його в цілеспрямованих фішингових атаках з кінця 2018 року. Зловмисники експлуатують вразливості в Microsoft Equation Editor (CVE-2017-11882, CVE-2018-0798 і CVE-2018-0802) і використовують шкідливі RTF-документи для доставки кастомного шкідливого програмного забезпечення на системи.

НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

Аналогічну тактику хакери використовували під час атаки на генерального директора конструкторського бюро “Рубін” : головним вектором зараження стали фішингові листи. Проте, на відміну від попередніх версій експлоїта Royal Road, що доставляли зашифроване корисне навантаження під назвою “8.t”, нова версія передбачала наявність в листі шкідливого документа, який при відкритті доставив зашифрований файл під назвою “ео” для вилучення імпланта PortDoor.

Таким чином, вектор інфікування, стиль соціальної інженерії, використання експлоїта Royal Road в атаках на аналогічні цілі та схожість між нещодавно виявленим бекдором та іншим відомим шкідливим програмним забезпеченням китайських APT – все це вказує на зловмисників, які діють в державних інтересах Китаю

Хакерська атака на трубопровід Colonial Pipeline

07.05.2021 було здійснено хакерську атаку на оператора трубопроводів в США Colonial Pipeline. Зловмисники викрали масив даних, потім заблокували комп’ютери і вимагали викуп. Вимагачі погрожували “злити” в мережу Інтернет конфіденційну інформацію і залишити комп’ютери заблокованими. З огляду на зазначене, Colonial Pipeline був змушений зупинити роботу паливопроводу. За повідомленням представників компанії, мова йде про вірус, який блокує роботу комп’ютерної системи і шифрує дані до моменту виплати суми, яку вимагають викрадачі.

За наявною інформацією, до хакерської атаки, яка паралізувала роботу найбільшого американського трубопроводу Colonial Pipeline, може бути причетне угруповання, пов’язане з Росією. Федеральне бюро розслідувань США уточнило, що відповідальність за кібератаку покладено на групу хакерів, які називають себе DarkSide. Проте у Кремлі заперечили свою причетність до атаки на трубопроводи в США.

Оскільки атака на Colonial Pipeline привернула увагу експертів, спецслужб та ЗМІ, хакери вирішили опублікувати заяву, в якій зазначили, що вони є аполітичними та діють виключно за власним бажанням.

14.05.2021 після того, як угруповання Darkside зазнало атаки у відповідь (невідомі хакери відключили його сервери), воно припинило свою діяльність. У своєму веб-повідомленні хакери групи Darkside визнали, що втратили доступ до певних серверів, які використовувались для ведення веб-блогу і здійснення платежів. Крім того, у хакерів було знято криптовалюту, що завдало фінансової шкоди угрупованню, яке позиціонувало себе як “офіційний бізнес із захоплення IT-систем”

Звинувачення Ірану в атаках на німецькі компанії

Служба безпеки Німеччини звинуватила іранських хакерів у здійсненні кібератаки на німецькі компанії, в рамках яких злочинці обманом змушують свої цілі встановлювати шкідливе програмне забезпечення. Хакерські атаки є частиною широкомасштабної кампанії Ірану з отримання доступу до конфіденційної інформації німецьких організацій.

На думку німецьких спецслужб, Іран намагається викрасти у європейських компаній корисні відомості та технології, які можуть використовуватися для створення зброї масового ураження.

В ході нещодавніх кібератак співробітники компаній в Німеччині отримували фішингові листи з пропозиціями роботи. Після того, як жертва переходила за наданим в листі посиланням, на її комп'ютер завантажувалося шкідливе програмне забезпечення. Фішингові листи розсилалися з підроблених адрес і призначалися для отримання доступу до конфіденційних даних організацій, що цікавлять хакерів.

Федеральна служба захисту конституції Німеччини (Bundesamt für Verfassungsschutz, BfV) описала нещодавні кібератаки як найбільш шкідливу кампанію. На думку фахівців, причиною підвищеного інтересу іранців до інформації німецьких організацій є політична напруженість в країнах Перської затоки.

Діяльність іранських хакерів також привернула увагу нідерландських спецслужб, які заявили, що Іран намагається отримати доступ до даних про нідерландські критичні технології.

Атака на авіакомпанії за допомогою нового завантажувача RAT

Фахівці компанії Microsoft попередили про поточну шкідливу кампанію цілеспрямованого фішингу, об’єктом якої є аерокосмічні та туристичні організації. Злочинці використовують низку троянів для віддаленого доступу, встановлених за допомогою нового таємного завантажувача шкідливих програм.

Фішингові електронні листи зловмисників відправляються нібито від імені легітимних організацій і замасковані під документи в форматі PDF, що містять тематичну інформацію. Вбудовані в фішингові повідомлення посилання завантажують файли VB Script і виконують PowerShell-скрипт. Останній виконує корисні дані завантажувача RAT з використанням процесу Process Hollowing.

Після встановлення шкідливе програмне забезпечення може викрадати облікові дані, дані web-камери, браузера і буфера обміну, інформацію про систему і мережі, робити знімки екрану, а також передавати дані через порт 587 протоколу SMTP.

Завантажувач, який отримав назву Snip3, використовується для інсталювання корисних навантажень Revenge RAT, AsyncRAT, Agent Tesla і NetWire RAT на скомпрометованих системах.

Snip3 також має можливість ідентифікувати віртуальні середовища і, таким чином, уникати виявлення з боку антивірусних програмних засобів. Завантажувач шкідливих програм також використовує додаткові методи для уникнення виявлення, включно з:

- виконанням PowerShell-коду з параметром remotesigned;
- використанням веб-сервісів Pastebin і top4top;
- компіляцією завантажувачів RunPE на кінцевій точці під час виконання.

Хакери Fancy Bear використовують нову шкідливу програму в фішингових атаках

Дослідники в галузі кібербезпеки з компанії Cluster25 виявили нове шкідливе програмне забезпечення SkinnyBoy, яке використовувалося в цілеспрямованих фішингових атаках. Шкідливу кампанію пов’язують з російськомовним хакерським угрупованням APT28 (також відомим як Fancy Bear, Sednit, Sofacy, Strontium або PwnStorm).

Злочинці використовували програму SkinnyBoy для здійснення атак на військові та урядові установи на початку поточного року. SkinnyBoy розроблено для проміжного етапу атаки, збору інформації про жертви і отримання корисного навантаження з C&C-сервера.

За даними фахівців, угруповання APT28 організувало кампанію на початку березня 2021 року, зосередивши увагу на міністерствах закордонних справ, посольствах і підприємствах в сфері оборонної промисловості та на військовому секторі. Численні жертви знаходяться в країнах ЄС, проте, шкідлива діяльність імовірно могла поширитись і на організації в США.

Хакери надсилають електронні листи із зараженим документом Microsoft Word. Документ містить макрос для екстракції DLL-файлу і завантаження шкідливого програмного забезпечення SkinnyBoy. Шкідливі листи замасковано під запрошення на міжнародний науковий захід, який відбудеться в Іспанії в кінці липня поточного року.

Потрапивши на цільову систему, завантажувач забезпечує постійну присутність і екстракцію корисного навантаження, зашифрованого в стандарті кодування Base64. Корисне навантаження видаляється після вилучення двох файлів зі скомпрометованої системи.

Метою програмного забезпечення SkinnyBoy є викрадення інформації про заражену систему, завантаження і запуск останнього корисного навантаження атаки, яка на даний момент залишається невідомою. Розкрадання даних здійснюється за допомогою вже наявних в операційній системі Windows інструментів systeminfo.exe і tasklist.exe, які дозволяють отримувати імена файлів.

Китайська шпигунська кампанія, націлена на Південно-Східну Азію

Фахівці з інформаційної безпеки компанії Check Point Research виявили шкідливу кампанію з кібершпигунства, ймовірно пов’язану з Китаєм. Хакери атакують урядові організації в Південно-Східній Азії з метою поширення шпигунського програмного забезпечення на операційних системах Windows. За словами експертів, злочинці залишалися непоміченими більше трьох років.

Атаки починаються з розсилання підроблених документів від імені урядових організацій співробітникам Міністерства закордонних справ. Після відкриття документ запускає корисне навантаження сервера команд і управління (Command and Control server, C&C-сервер). Завантажувач викрадає і передає системну інформацію на віддалений сервер, який згодом відправляє завантажувач shell-коду.

Завантажувач встановлює з’єднання з віддаленим сервером для інсталювання, розшифровки і виконання імплантату VictoryDll_x86.dll, здатного виконувати файлові операції, здійснювати знімки екрану, створювати і завершувати процеси і навіть завершувати роботу зараженої системи.

Фахівці вважають, що шкідлива кампанія може бути пов'язана з китайським кіберзлочинним угрупованням SharpPanda. Такий висновок заснований на тестових версіях бекдора від 2018 року, які було завантажено на сайт служби аналізу підозрілих файлів VirusTotal з Китаю, а також на використанні інструменту для створення RTF-експлоїтів Royal Road

Крім того, C&C-сервер повертав корисні дані тільки в період часу між 1:00 і 8:00 UTC, що, імовірно, є робочим часом в країні зловмисників. Також, з 1 по 5 травня поточного року C&C-сервери не виявляли шкідливої активності навіть у робочий час, що збігається зі святом Дня праці в Китаї.

Китайські кібершпигуни атакували американську транспортну компанію MTA

Хакери зламали комп'ютерну систему американської транспортної компанії Metropolitan Transportation Authority (MTA), що здійснює перевезення в 12 округах на південному заході штату Нью-Йорк і в двох округах на південному заході Коннектикуту. Хакери не отримали доступ до систем управління поїздами, і безпека пасажирів не була під загрозою.

Атака сталася в той же час, коли федеральний уряд США повідомив про злам іноземними хакерами п'яти урядових організацій через VPN-сервіс. Зловмисники експлуатували zero-day в шлюзах Pulse Connect Secure (CVE-2021-22893). За повідомленнями фахівців компанії з інформаційної безпеки FireEye, як мінімум два хакерських угруповання експлуатували вразливість для атак на оборонні, урядові та фінансові організації в США та інших країнах.

Атаку на компанію було здійснено в рамках широкомасштабної кібероперації, що проводиться хакерами, які імовірно працюють на китайський уряд.

Експерти припускають, що хакери могли зацікавитися компанією MTA з двох причин:

- по-перше, їх метою могли бути важливі відомості про роботу транспортних систем, які дозволили б забезпечити Китаю домінантне становище на ринку залізничного транспорту;

- по-друге, хакери могли зламати системи MTA помилково.

Зв’язок між угрупованням RedFoxtrot і китайською армією

Дослідницька команда Insikt Group компанії з інформаційної безпеки Recorded Future виявила зв’язок між хакерським угрупованням RedFoxtrot і Народно-визвольною армією Китаю, зокрема з підрозділом Unit 69010, які оперують з Урумчі – адміністративного центру Сіньцзян-Уйгурського автономного району.

Unit 69010 є частиною Бюро технічної розвідки – структури у складі Сил стратегічного забезпечення при Департаменті мережевих систем Китаю. До складу стратегічного забезпечення входять підрозділи, що відповідають за космічну, кібер і радіоелектронну війну.

Зв’язок між компаніями з кібершпигунства RedFoxtrot, зосереджених на зборі розвідувальних даних про сусідні країни, і Unit 69010 вдалося виявити завдяки припущеним одним з членів угруповання помилкам в операційній безпеці (OpSec), який розкрив фізичну адресу Бюро технічної розвідки.

Атаки угруповання RedFoxtrot сфокусовано на урядовому, телекомунікаційному та оборонному секторах в країнах Центральної Азії, Індії та Пакистані. Протягом останніх шести місяців угруповання атакувало трьох індійських підрядників в аерокосмічній і оборонній сферах, а також телекомунікаційні компанії та урядові відомства в Афганістані, Індії, Казахстані і Пакистані.

Арсенал угруповання включає авторські та відкриті (open source) хакерські інструменти, включно з бекдорами сімейства PlugX, шкідливим програмним забезпеченням Royal Road RTF, QUICKHEAL, PCShare, IceFog і трояном для віддаленого доступу Poison Ivy.

RedFoxtrot також використовує інфраструктуру AXIOMATICASYMPTOTE поряд з модульним бекдором для операційної системи Windows під назвою ShadowPad. Раніше фахівці команди Insikt Group пов’язали цю інфраструктуру з іншим угрупованням – RedEcho, що здійснила атаки на енергетичний сектор і критично важливі об’єкти інфраструктури Індії. В ході атак злочинці також використовували шкідливе програмне забезпечення PlugX і ShadowPad.

Атака на центр ядерних досліджень в Південній Кореї

Хакерське угруповання, пов'язане з Північною Кореєю, проникло в комп'ютерні системи одного з найбільших в Південній Кореї центру ядерних досліджень.

Відповідно до даних південнокорейського політика, 14.05.2021 хакери атакували Корейський дослідний інститут атомної енергії, використовуючи вразливість в VPN-сервері організації. Організація ще проводить розслідування інциденту і намагається з'ясувати, які дані потрапили до рук хакерів.

Під час атаки зловмисники використовували 13 IP-адрес, частина з яких виявилася серверами APT-групи Kimsuky (інші назви – Black Banshee, Velvet Chollima і Thallium), яка, за думкою дослідників, є підрозділом розвідувальної служби КНДР.

Також відомо, що деякі з IP-адрес використовували адресу електронної пошти колишнього радника президента з питань зовнішньої політики Мун Чунг-ина. Поштовий акаунт чиновника був імовірно зламаний в 2018 році, проте тільки в 2020 році експерти встановили причетність Kimsuky до зламу.

Угруповання діє з 2012 року і займається збором розвідувальних даних, в основному, за допомогою цілеспрямованого фішингу. Kimsuky атакує визнаних експертів у різних галузях, аналітичних центрах та державних структурах Південної Кореї.

ReverseRat - новий інструмент в арсеналі пакистанських кібершпигунів

Компанія Black Lotus Labs виявила новий троян для віддаленого доступу ReverseRat, оператори якого націлені на урядові і енергетичні організації в регіонах Південної і Центральної Азії. Імовірно, операційна інфраструктура кіберзлочинного угруповання перебуває в Пакистані.

Крім трояну ReverseRat, злочинці паралельно встановлюють на системах RAT з відкритим вихідним кодом (під назвою AllaKore) для зараження інших систем і забезпечення постійної присутності.

НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

На першому етапі злочинці через електронні листи розсилали жертвам URL-адреси, що перенаправляли на зламані web-сайти. При натисканні на посилання завантажувався архів .zip, який містив ярлик файлу Microsoft (.lnk) і PDF-файл. При запуску ярлика відображався PDF-файл, відволікаючий увагу користувача. Водночас .lnk таємно витягував і запускав HTA-файл (додаток HTML) зі зламаного web-сайту.

У підроблених PDF-документах згадувалися організації і події, що причетні до подій в Індії навесні 2021 року. Деякі з документів або приманок мали більш загальну тематику і були пов'язані з вакцинацією від COVID-19, в той час як інші були пов'язані з тематикою енергетичного сектора.

На наступному етапі атаки HTA-файл, який містив JavaScript-код на базі GitHub-проєкту під назвою CactusTorch, запускав .NET-програму preBotHta.pdb, яку угруповання використовує з 2019 року. У варіанті файлу preBotHta від 2021 року було дві особливості: він повністю виконувався в пам'яті, а також міг змінювати розміщення ReverseRat, якщо на скомпрометованій системі було запущено антивірусне програмне рішення.

Згодом програма preBotHta запускала інструмент ReverseRat, який через Windows Management Instrumentation (WMI) збирав інформацію про MAC-адресу, фізичну пам'ять на пристрої, процесор (максимальну тактову частоту, назву, виробника) тощо. Шкідливе програмне забезпечення шифрувало дані за допомогою RC4-ключа і відправляло їх на C&C-сервер.

Другий файл HTA містив закодовану команду для зміни розділу реєстру, завантажувач і інструмент AllaKore, що надає доступ до скомпрометованої мережі.

Аналізуючи дані про вказану кампанію, фахівці виявили схожість з техніками, тактиками і процедурами, які використовувались в операції Operation SideCopy, організованою пакистанським APT-угрупованням Transparent Tribe в 2020 році.

Зростання кількості атак на VPN-обладнання в 1 кварталі 2021 року

Кількість атак на VPN-обладнання виробництва Fortinet і Pulse Secure суттєво зросло в 1 кварталі 2021 року, що пов'язано зі спробами хакерських угруповань скористатися відомими вразливостями в VPN-обладнанні.

Зокрема, за даними компанії Nuspire, що надає послуги мережевої безпеки, у зазначений період число атак на продукти Fortinet SSL-VPN виросло на 1916%, Pulse Connect Secure VPN – на 1527%. У першому випадку зловмисники експлуатували вразливість CVE-2018-13379, що дозволяє завантажити файли, а в другому – атаки концентрувалися на вразливості CVE-2019-11510, що дозволяє прочитати файли.

Хоча виробники вже давно випустили відповідні оновлення, багато організацій продовжують ігнорувати численні попередження експертів в сфері безпеки й залишають проблеми невиправленими, чим і користуються хакери.
Не зважаючи на різке зростання числа атак на VPN-обладнання, фахівці відзначають спад активності шкідливого програмного забезпечення, ботнетів і інших загроз. Зокрема, активність шкідливого програмного забезпечення в 1 кварталі поточного року знизилася на 54% у порівнянні з останнім кварталом 2020 року, ботнетів – на 11%, а число спроб експлуатації вразливостей (без обліку атак на VPN) впало майже на 22%.

За словами аналітика Nuspire Джоша Сміта (Josh Smith), організаціям слід приділяти увагу безпеці не лише VPN, а і Microsoft Remote Desktop Protocol – ще одній цілі зловмисників. Зокрема, здійснювати моніторинг, оперативно застосовувати оновлення безпеки, а також реалізувати багатофакторну аутентифікацію. У випадку витоку облікових даних для сервісів дистанційного доступу багатофакторна аутентифікація може стати вирішальним фактором у тому, чи буде злам успішним, або доступ зловмисникам буде заблоковано.

Новий метод MitM-атак на протокол HTTPS

Вчені з Рурського університету в Бохумі та Мюнстерського університету прикладних наук (Німеччина) оприлюднили інформацію про нову техніку атак на протокол HTTPS, що дозволяє отримати доступ до cookie-файлів, здійснити XSS-атаки і викрасти важливу інформацію.

Атака, що отримала назву ALPACA (Application Layer Protocol Confusion - Analyzing and mitigating Cracks in TLS Authentication), експлуатує вразливість в протоколі TLS і вражає TLS-сервери.

Відповідно до даних дослідників, принцип атаки полягає в тому, що зловмисник, який має доступ до мережевого шлюзу або бездротової точки доступу, може перенаправити web-трафік на інший мережевий порт і встановити з'єднання з FTP або поштовим сервером, що підтримують TLS-шифрування і використовують спільний з HTTP протокол. При цьому, браузер користувача вважатиме, що встановлено з'єднання з запитуваним HTTP-сервером.

Здійснення атаки ALPACA є можливим тому, що протокол TLS не прив'язує TCP-з'єднання до визначеного протоколу рівня програм, що, у свою чергу, може використовуватися для перенаправлення TLS-трафіку з призначеного TLS-сервера на інший (підставний) TLS-сервер. Метод працює за умови, що у зловмисника є можливість перехоплення трафіку на рівні TCP/IP.

Крім того, вразливість в протоколі TLS може використовуватися для отримання доступу до аутентифікаційних cookie-файлів, інших конфіденційних даних на FTP-сервері, а також для завантаження шкідливого коду JavaScript з FTP-сервера

Для запобігання подібних атак пропонується використовувати розширення ALPN (Application Layer Protocol Negotiation) з метою узгодження TLS-сеансу, з урахуванням прикладного протоколу і розширення SNI (Server Name Indication) для прив’язування до імені хоста.

Технології та інструменти забезпечення кібербезпеки та проведення операцій у кіберпросторі

Невідома фірма отримала від Пентагону контроль над 175 мільйонами IP-адрес

Компанія Global Resource Systems в день вступу Джо Байдена на посаду президента США 20.01.2021 отримала від Пентагону контроль над 56 мільйонами IP-адрес. Згодом кількість IP-адрес зросла до 175 мільйонів, (становить близько 6% всіх IP-адрес в мережі Інтернет і є більшою, ніж у таких великих американських провайдерів, як Comcast або AT&T).

Представники Пентагону пояснили такий крок тим, що компанія реалізує пілотний проект з оцінки простору IP-адрес. Це повинно дозволити унеможливити їх несанкціоноване використання в майбутньому. Таким чином, військові мають намір "взяти під контроль, оцінити і запобігти несанкціонованому використанню IP-адрес Міністерства оборони США".

Однак представник Пентагону не пояснив, чому Міністерство оборони обрало для управління адресним простором компанію Global Resource Systems, яка не має державних контрактів

Компанія Global Resource Systems (не має web-сайту, але є домен grscorp.com) зареєстрована в Делавері юристом з Беверлі-Хіллз і тепер керує величезним обсягом Інтернет-простору.

Аналіз використання біткоїнів в фінансових операціях

Майкл Морелл, колишній виконувач обов'язків директора ЦРУ, опублікував звіт "Аналіз використання біткоїнів в незаконних фінансах", в якому зазначено, що технологія блокчейн є потужним інструментом, який недостатньо використовується судовими експертизами з метою виявлення незаконної діяльності і притягнення злочинців до відповідальності.

НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

У звіті було зроблено висновок про те, що злочинне використання біткоїнів “значно перебільшено”. Більш того, біткоїн можна використовувати для виявлення та затримання фінансових злочинців. Можливість здійснення аналізу ланцюга блоків – це високоефективний інструмент боротьби зі злочинністю та збору розвідувальної інформації. Технологія, на якій працює біткоїн, передбачає реєстрацію всіх транзакцій в публічному, децентралізованому незмінному реєстрі.

Таким чином, відстеження незаконних транзакцій з біткоїнів простіше, ніж відстеження незаконного обігу коштів, що переміщуються через кордон з використанням традиційних банківських транзакцій, і набагато простіше, ніж спроби відстежувати обіг готівкових коштів.

Розслідування колишнього директора ЦРУ також показало, що більш небезпечним є обіг конфіденційних монет, зокрема Monero, які наразі ускладнюють роботу силових структур.

Програма розкриття вразливостей Пентагону

Міністерство оборони США оголосило про розширення своєї програми розкриття вразливостей (Vulnerability Disclosure Program) – тепер вона поширюється і на всі публічно доступні інформаційні системи міністерства.

Програма функціонуватиме на базі розпочатої п'ять років тому ініціативи “Зламай Пентагон” (Hack the Pentagon). У 2016 році Ештон Картер (Ashton Carter), який на той час обіймав посаду міністра оборони США, зустрівся з двома хакерами, щоб висловити їм подяку за повідомлення про небезпечні вразливості на декількох сайтах Пентагона. Ці хакери були найуспішнішими учасниками проєкту “Зламай Пентагон”, що став першою програмою bug bounty Міністерства оборони (програма, за допомогою якої люди можуть отримати винагороду за здайдені помилки, особливо ті, які стосуються експлойтів та вразливостей).

Раніше жодної можливості зв'язатися з Пентагоном і повідомити про вразливість в його системах у дослідників безпеки не було. Директор цифрової служби оборони (Defense Digital Service) Бретт Голдштейн (Brett Goldstein) повідомив, що через це багато вразливостей залишалися невиявленими. Програму з виявлення вразливостей Міністерства оборони США розпочали тоді, коли фахівці продемонстрували ефективність роботи з хакерською спільнотою і найняли хакерів для пошуку і виправлення вразливостей в системах.

Реалізацією програми розкриття вразливостей займається Центр боротьби з кіберзлочинністю Міністерства оборони (Cyber Crime Center). За весь час існування програми Пентагон отримав від дослідників 29 тисяч повідомлень про вразливість, і 70% з них було підтверджено.

Спочатку програма обмежувалася тільки громадськими сайтами і додатками Міністерства оборони, але тепер дослідники безпеки можуть повідомляти про вразливість в усіх суспільно доступних мережах, в тому числі, в системах радіозв'язку, IoT і промислових системах.

Next Generation – інструмент для кібервійн

Представники армії США зазначили, що в оборонному арсеналі країни з’явиться новий пригнічувач сигналів, який може працювати в кіберпросторі. Таким чином, США планують стерти кордони між традиційною радіоелектронною війною та кібероперaціями.

Контр-адмірал Джон Меєр, командувач Військово-морськими силами Атлантики, анонсував вихід пригнічувача Next Generation – головної платформи повітряної радіоелектронної атаки для ВМФ США, яку буде встановлено на літак EA-18G Growlers.

Він поділений на три модулі, які охоплюють три частини електромагнітного спектру: середню, низьку та високу. Кіберпростір з використанням радіочастот стає більш важливим компонентом кібероперацій, оскільки все більше супротивників підключають свої системи до провідних мереж, які захищені брандмауером чи є незалежними від мережі Інтернет.

Зокрема, Росія та Китай протягом останнього часу переміщують багато обладнання в провідні мережі, внаслідок чого виникає інтерес до нових інноваційних способів проникнення в мережі супротивників, таких як радарна система, яка використовується для передачі інформації до бойової системи, пригнічувачі сигналів в рамках радіоелектронної боротьби.

Армія США провела експерименти в цій сфері та створила нові тактичні кіберпідрозділи для проведення наземних операцій з використанням радіочастот. Під час навчань використовували радіочастотні методи для отримання доступу до камер відеоспостереження в містах перед запланованою операцією.

Інтернет-сервіс Starlink стане “повністю мобільним” до кінця року

Як стверджує Ілон Маск, супутниковий Інтернет-провайдер Starlink стане повністю мобільним до кінця цього року. Для цього треба запустити додаткові супутники і оновити програмне забезпечення системи.

“Повністю мобільним” означає, що Інтернет від Starlink зможе бути доступний клієнтам за різними адресами і навіть для тих, хто перебуває в русі. Варто зазначити, що наразі відбувається тестування бета-версії системи. Вона працює тільки за фіксованою адресою і не дозволяє користувачам переміщати приймальне обладнання з місця на місце. На сьогодні на бета-версію Starlink, що стартувала в жовтні 2020 року, підписалося більше 10 000 чоловік.

Подробиці про майбутнє Starlink з’явилися, коли Маск відповів у Twitter підписнику, який поцікавився, коли він зможе встановити тарілку на автофургон. Підприємець повідомив, що Starlink буде повністю мобільним в кінці поточного року, що дозволить переміщати приймальне обладнання куди завгодно або використовувати його в русі. Він також зазначив, що SpaceX необхідно “ще кілька запусків супутників” для досягнення повного покриття, а системі буде потрібно оновлене програмне забезпечення.

Маск також зазначив, що такі показники, як час безвідмовної роботи системи, пропускна здатність і час очікування, “швидко поліпшуються”. Раніше Маск обіцяв, що до кінця 2021 року швидкість Інтернету від Starlink подвоїться.

Новий стандарт Google для посилення безпеки мобільних додатків

Компанія Google активно просуває новий стандарт, призначений для посилення базової безпеки мобільних додатків. Стандарт Mobile Application Profile розроблений консорціумом Internet of Secure Things Alliance (ioXt), що налічує більше трьохсот учасників, включно з Google, Facebook, T-Mobile, Zigbee Alliance, Schneider Electric тощо.

НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

Завдяки участі такої кількості компаній ioXt охоплює широкий спектр пристроїв різних типів, зокрема “розумні” системи освітлення, смарт-колонки і web-камери, і, оскільки більшість смарт-пристроїв керується через додатки, стандарт розширив охоплення, включивши до нього й мобільні додатки.

Розроблений ioXt стандарт Mobile Application Profile забезпечує мінімальний набір кращих галузевих практик для всіх об'єднаних в хмарі додатків, що виконуються на мобільних пристроях. Така базова безпека дозволяє протистояти поширеним загрозам і знижує можливість експлуатації зловмисниками небезпечних вразливостей.

Mobile Application Profile охоплює паролі, інтерфейси, шифрування, програмні оновлення, повідомлення про вразливості і безпеку за замовчуванням.

Стандарт базується на фреймворку OWASP MASVS і VPN Trust Initiative. Хоча мобільним додаткам достатньо бути сертифікованими за Mobile Application Profile, VPN-додатки повинні також відповідати спеціалізованому розширенню VPN. Таким чином, сертифікація дозволить розробникам продемонструвати безпечність продукту.

Підводні Інтернет-кабелі для Facebook і Google

Facebook вперше прокладе два підводних кабелі, що з'єднають США та Індонезію, оскільки група з Кремнієвої долини орієнтується на ринок смартфонів, що швидко зростає.

Проект, в якому американському пошуковому гігантові Google також буде належати частка, забезпечить швидший Інтернет для найбільшої економіки Південно-Східної Азії, а також з'єднає обидві країни з Сінгапуром. Кабелі збільшать пропускну здатність на 70% між західним узбережжям США й азіатськими країнами.

Близько 400 підводних кабелів, що діють по всьому світу, передають голосовий і Інтернет-трафік між країнами й континентами.

Інфраструктура, яка колись належала телекомунікаційним компаніям, тепер стала об'єктом масштабних інвестицій Facebook та інших технологічних груп, включно з Microsoft і Google.

Facebook відмовився повідомити вартість кабельної інфраструктури, яку планують завершити в 2023-2024 роках.

Будівництво підводних кабелів стало геополітичною точкою кипіння для технологічних компаній, особливо у зв'язку зі зростанням напруженості між США та Китаєм.

Саме з цієї причини, а також з міркувань безпеки у 2020 році було призупинено будівництво мережі Pacific Light Cable, яка фінансувалася Facebook і материнською компанією Google Alphabet. Мережа PLCN з великою пропускною здатністю довжиною 13 000 км повинна була з'єднати Гонконг зі США, Тайванем і Філіппінами, але Вашингтон виступив проти підключення до Гонконгу на тій підставі, що він може передати Китаю глобальні дані.

Раніше Facebook відмовився від свого проєкту Гонконг-Америка: ще одного підводного волоконно-оптичного кабелю, що повинен був з'єднати Каліфорнію з китайською територією, через побоювання уряду США.

Інструмент для запобігання зламу штучного інтелекту від Microsoft

Компанія Microsoft випустила автоматизований інструмент з відкритим вихідним кодом Counterfit, завданням якого є допомогти компаніям оцінити рівень кібербезпеки систем на базі машинного навчання.

Проєкт Counterfit доступний на веб-сервісі GitHub і містить інструмент командного рядка та загальний рівень автоматизації, що дозволяє розробникам моделювати кібератаки на системи штучного інтелекту. Будь-який користувач може завантажити інструмент і встановити його через оболонку Azure Shell, запустити в браузері або локально в середовищі Anaconda Python. Counterfit має можливість оцінювати моделі штучного інтелекту в різних хмарних середовищах, локально або на периферії.

Інструмент не залежить від моделей штучного інтелекту, а також підтримує різні типи даних, включно з текстами, зображеннями або загальним введенням. Фахівці з інформаційної безпеки можуть використовувати Counterfit для тестування на проникнення і об'єднання систем штучного інтелекту, сканування систем штучного інтелекту на наявність вразливостей і реєстрації атак на моделі штучного інтелекту.

Counterfit – набір спеціальних скриптів для симуляції атак на різні моделі штучного інтелекту. На початковому етапі компанія Microsoft застосовувала скрипти для внутрішніх тестів, проте, з часом Counterfit став самостійним автоматизованим інструментом, що дозволяє проводити тестові атаки одночасно на кілька моделей штучного інтелекту.

Також в останні роки стає все більш актуальною гонка за мілітаризацією штучного інтелекту, що підвищує ризики безпеки. З огляду на зазначене, у січні 2021 року Європейський парламент опублікував директиви, згідно з якими військовий штучний інтелект не повинен підміняти людські рішення.

Також експерти вважають, що штучний інтелект не має права приймати рішення про позбавлення життя людини, що відповідає керівним принципам Європейського парламенту і постановами Європейського союзу. У свою чергу, Комісія з національної безпеки і штучного інтелекту США (National Security Commission on Artificial Intelligence, NSCAI) порекомендувала владі США прискорити розвиток технологій штучного інтелекту, щоб зберегти національну безпеку і залишатися конкурентоспроможною країною на рівні з Китаєм і Росією.

Нова ера комп'ютерів

15.06.2021 в дата-центрі американського концерну IBM (комуна Енінген, Німеччина) відбувся запуск системи IBM Quantum System One - найпотужнішого комерційного квантового комп'ютера, розміщеного компанією IBM в Європі.

Через коронавірусні обмеження у церемонії в заочному режимі взяли участь генеральний директор IBM Арвінд Крішна, канцлер Німеччини Ангела Меркель, а також представники Товариства імені Фраунгофера – найбільшого європейського об'єднання інститутів прикладних досліджень.

IBM Quantum System One стала першою в світі інтегрованою квантовою комп'ютерною системою, створеною на стику квантової науки, кріогенної інженерії, системної інженерії та промислового дизайну. Крім того, вказаний комп'ютер є першим, представленим за межами США, з процесором в 27 кубітів. У компанії зазначили, що до 2023 року планують випустити квантовий комп'ютер в чотири рази потужніший.

Інноваційна модульна архітектура MeluXina дозволяє обслуговувати широкий спектр складних обчислювальних робочих навантажень. Передбачається, що суперкомп'ютер використовуватиметься для ресурсоємних завдань моделювання, аналізу великих даних і штучного інтелекту. Система працює на екологічно чистій енергії. Її створення було профінансовано урядом Люксембургу та Європейським спільним підприємством високопродуктивних обчислень (European High Performance Computing Joint Undertaking, EuroHPC)

Встановлення апаратури для контролю за об'єктами в КНР

Міністерство державної безпеки Китаю має на меті скласти перелік ключових китайських організацій для захисту від іноземних розвідок – в цих організаціях контррозвідники зможуть встановлювати необхідну апаратуру, а також, на власний розсуд, демонтувати потенційно небезпечне обладнання.

Після включення до переліку організація повинна провести контррозвідувальну перевірку і навчання всього персоналу, що має доступ до секретів. Цей персонал повинен підписати угоди про нерозголошення інформації. Контррозвідувальний інструктаж є обов'язковим для відряджених за кордон фахівців, що мають доступ до секретної інформації.

Рішення про посилення контррозвідувальної роботи прийнято через напруженість у відносинах між Пекіном і Вашингтоном. Раніше в щорічному розвідувальному звіті для адміністрації Байдена дії Китаю було названо однією з найсерйозніших загроз для США. Зокрема, Китай використовує кіберпростір для економічного шпигунства і крадіжки об'єктів інтелектуальної власності, вартість якої вимірюється трильйонами доларів.

Міністр закордонних справ Китаю Ван І (Wang Yi) закликав Вашингтон припинити дискредитувати політичну систему Китаю як авторитарну. Нові контррозвідувальні правила стали відповіддю КНР на постійне зростання кількості “проникнень” і фактів шпигунства відносно країни.

Варто зазначити, що Китай вже не поступається США в багатьох критично важливих технологічних галузях, зокрема у розвитку штучного інтелекту. Наразі КНР через американські санкції прискорено розвиває власні напівпровідникові фабрики – це рішення є частиною плану, який впроваджується протягом останніх шести років.

Закордонні антивіруси для китайського кіберпідрозділу

Команда дослідників у сфері кібербезпеки Insikt Group з компанії Recorded Future виявила на офіційних військових сайтах Народно-визвольної армії Китаю (НВАК) шість документів про закупівлі, згідно з якими Бюро 61419 Сил стратегічної підтримки НВАК отримало антивірусне програмне забезпечення від декількох великих американських, європейських і російських фірм інформаційної безпеки. Бюро 61419 НВАК мало на меті придбати англомовні версії програмного забезпечення, а не версії китайською мовою.

НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

Як вважають фахівці, купівля іноземного антивірусного програмного забезпечення є високим ризиком для глобального ланцюга постачань антивірусних рішень. Імовірно, кіберпідрозділи НВАК і хакерські угруповання використовуватимуть закордонні антивірусні програми як тестове середовище для шкідливих програм власної розробки, а також запускатимуть шкідливе програмне забезпечення через такі антивірусні продукти, щоб перевірити його здатність уникати виявлення, підвищуючи ймовірність успішного зараження потенційних цілей.

Більш того, існує ймовірність, що кіберпідрозділи НВАК займуться зворотною розробкою програмного коду іноземного захисного рішення з метою знайти раніше нерозкриті вразливості нульового дня. Потім хакери проексплуатують їх в рамках кібератак.

Сили стратегічної підтримки НВАК також опублікували документ про придбання маршрутизаторів Cisco. У документі використовується аналогічна контактна адреса, що і для Бюро 61419. Варто зазначити, що з 2014 року в Китаї діє заборона на використання іноземних антивірусних рішень. У серпні того ж року Департамент закупівель центрального уряду КНР виключив “Лабораторію Касперського” і Symantec зі списку затверджених постачальників програмних продуктів для забезпечення інформаційної безпеки. Китайські офіційні особи ухвалили використання рішень п'яти китайських фірм: Qihoo 360 Technology, Venustech, CAJinchen, Beijing Jiangmin і Rising.

Крім використання антивірусного програмного забезпечення задля власної вигоди, Народно-визвольна армія Китаю також підозрюється в кібератаках на сотні цілей в Японії (в тому числі на космічне агентство і оборонні підприємства). Зокрема, підозрювані злочинці діяли за наказом Бюро 61419 і замовили у кіберзлочинного угруповання Tick низку кібератак на японські організації.

Huawei переходить на виробництво програмного забезпечення

Засновник китайської технологічної компанії Huawei Рен Чженфей (Ren Zhengfei) закликав персонал компанії зосередитись на розробці програмного забезпечення та посісти провідне місце в світі в цій галузі.

НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

Керівництво компанії Huawei вирішило зосередити увагу на програмному забезпеченні, оскільки майбутній розвиток цього ринку послуг перебуває за межами контролю США, і китайська компанія зможе отримати незалежність і автономність.

Huawei має намір розбудувати програмну екосистему, яка включатиме операційну систему HarmonyOS, систему штучного інтелекту Mindspore та інші IT-продукти. Запуск операційної системи HarmonyOS для смартфонів передбачено вже у червні поточного року

Розвиток програмного забезпечення залежатиме від вибору правильної бізнес-моделі. Рен Чженфей наголосив, що з огляду на труднощі роботи в США, слід посилювати позиції на домашньому ринку і зміцнити становище настільки, щоб не залучати до своєї діяльності американських виробників.

Фахівці Huawei вважають, що виробництво програмного забезпечення є ефективним способом зберегти або завоювати технологічне лідерство в сфері традиційних для Huawei технологій бездротового зв'язку 5G.

У Китаї створили гігантську нейромережу

01.06.2021 у Китаї дослідники з Пекінської академії штучного інтелекту (Beijing Academy of Artificial Intelligence, BAAI) оголосили про створення нейромережі Wu Dao 2.0, що вдесятеро перевершує за потужністю найбільш розвинені алгоритми GPT-3.

За словами фахівців, потужність нової нейронної мережі Wu Dao 2.0 перевершує найближчих конкурентів – алгоритми Open AI GPT-3 і Google Switch. Потужність нейромережі вимірюється числом параметрів, які нейромережа може використовувати в своїй роботі. Нейромережа Open AI GPT-3 використовує 175 мільярдів параметрів, поза як Wu Dao 2.0 – 1,75 трильйонів параметрів.

Нова китайська нейромережа мультимодальна – може виконувати безліч різнорідних завдань. Wu Dao 2.0 пише есе та вірші традиційною китайською мовою, розпізнає зображення і генерує їх за словесним описом, імітує мову, створює кулінарні рецепти, а також пророкує тривимірну структуру білків, на кшталт програми штучного інтелекту AlphaFold.

За наявною інформацією, новою нейромережею зацікавилися щонайменше 22 компанії

Передача квантових бітів на 600 км від японських вчених

Японські вчені розробили метод дводіапазонної стабілізації, що надав можливість інженерам Toshiba відправити квантову інформацію оптичним волокном довжиною 600 кілометрів, встановивши новий рекорд.
Інформація, що передається волоконно-оптичними лініями зв'язку, зашифрована за допомогою технології квантового розподілу ключів (QKD). Фахівці зазначили, що для створення ключів шифрування протокол використовує квантові мережі, які несприйнятливі до зламів. Нову технологію можна використовувати й у військових цілях, тому припускають, що цією розробкою зацікавляться оборонні відомства країн.

Завдяки методу дводіапазонної стабілізації захист переданої інформації зростає в рази і практично дані стають не сприйнятливі до зламу. Якщо хакерам вдасться проникнути в таку мережу, то обидві сторони, які обмінюються даними, про це будуть попереджені.

Крім того, новий метод уможливлює подальше збільшення відстані для застосування технології квантового розподілу ключів, а також застосування зазначеного методу до інших протоколів і додатків квантового зв'язку.

Раніше передавати інформацію оптоволоконними мережами вдавалося тільки на невеликі відстані. У компанії Toshiba стверджують, що за допомогою нової технології держави можуть ділитися таємною інформацією, не побоюючись її витоку третім сторонам.

Іншим напрямком розвитку даної сфери є реалізація постквантової криптографії та її впровадження у життя. Хоча квантові обчислення все ще перебувають на початковому етапі розробки, уряди й компанії приватного сектору, зокрема Microsoft і Google, працюють над питанням постквантової криптографії. Фахівці зазначають, що протягом десятиліття квантові комп'ютери можуть стати достатньо потужними, щоб зламати криптографічну безпеку мобільних телефонів, банківських рахунків, адрес електронної пошти й біткоїн-гаманців.

НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

Наразі у світі застосовується так звана асиметрична криптографія, у якій використовується пара закритих і відкритих ключів для доступу до облікових записів і криптогаманців. Кожна фінансова операція, кожна авторизація в системі на телефоні засновані на асиметричній криптографії, яка вразлива до зламу за допомогою квантового комп'ютера.

Експерти з інформаційної безпеки, включно з Національним інститутом науки й технологій (NIST), вже перебувають у процесі створення квантово-безпечної криптографії. Проте, поява першого стандартного квантово-безпечного криптографічного алгоритму очікується до 2024 року. За словами експертів, це відбудеться до того, як світ побачить квантовий комп'ютер.

Криптографічний модуль для роботи з біометричними даними від Ростелеком

На початку квітня поточного року Ростелеком розпочав тестування нового криптографічного модуля "КриптоSDK", розробленого для спрощення реалізації заходів із захисту даних при впровадженні біометричної ідентифікації в бізнес-процеси банків.

Впровадження модуля дозволить проводити ідентифікацію громадян з біометрії і надавати їм послуги безпосередньо в мобільному додатку банку, а також спростить їх взаємодію з Єдиною біометричною системою (ЄБС), оператором якої є Ростелеком.

Наразі, щоб надавати послуги з використанням ЄБС, захищений мобільний додаток "Біометрія" від Ростелеком має бути інтегровано в сервіс банку, або фінансовим організаціям необхідно самостійно розробляти і сертифікувати рішення для забезпечення безпеки біометричних даних. При використанні "Біометрії" користувач перенаправляється в додаток для безпечного підтвердження особи, а після повертається до отримання послуги в сервіс банку.

Завдяки новому рішенню Ростелекому банки зможуть проводити ідентифікацію з біометрії у власному додатку, виконуючи всі вимоги щодо захисту даних. Клієнту, при цьому, буде достатньо встановити тільки додаток банку. Фінансова організація самостійно вирішуватиме: вбудовувати модуль "КриптоSDK", який надійде в продаж наприкінці 2021 року, або провести інтеграцію мобільних додатків банку і доступної з 2018 року "Біометрії".

Ростелеком має намір сертифікувати модуль “КриптоSDK” відповідно до вимог російських регуляторів у сфері інформаційної безпеки, що дасть банкам можливість не сертифікуючи власний додаток реалізувати в ньому захищений сервіс віддаленої ідентифікації.

Готовність взяти участь у тестуванні модуля “КриптоSDK” підтвердили декілька російських банків і найбільші розробники автоматизованих банківських систем – Центр фінансових технологій (ЦФТ) і iDSystems.

Варто зазначити, що згідно з Федеральним Законом від 29 грудня 2020 року № 479-ФЗ до 1 січня 2022 року всі банки з універсальною ліцензією, що мають додатки для роботи з фізичними особами, повинні реалізувати можливість надання послуг для нових клієнтів (відкриття рахунку, вкладу або отримання кредиту) в дистанційному каналі, з використанням ЄСІА і Єдиної біометричної системи.

Смартфони для військовослужбовців від Міністерства оборони РФ

На базі військового технополісу “Эра” Міністерство оборони Росії веде розробку смартфонів власного виробництва для військовослужбовців і членів їх родин. Ці телефони дозволять надавати безпечний зв’язок. Також буде створено спеціальні мобільні додатки для повсякденної діяльності на території військових частин.

За словами заступника керівника Департаменту інформаційних систем Міністерства оборони РФ Олександра Осадчука, наразі у відомстві вжито серйозних заходів із забезпечення високого рівня інформаційної безпеки, в той час як використання стільникових телефонів іноземного виробництва значно підвищує ступінь ризику. Було наголошено на тому, що використання таких пристроїв на території військової частини може стати джерелом витоків різного роду інформації і призведе до виникнення відповідної небезпеки і загрози.

На базі військового технополісу “Эра” вже було розроблено мобільну платформу “Аврора”. У цьому ж напрямку тривають експерименти зі створення захищеного телефона/смартфона, який працюватиме в різних режимах, забезпечуючи безпечний зв’язок.

Крім того, фахівці технополісу вже апробовують проєкт “Кварц”, націлений на створення цифрової екосистеми для повсякденної діяльності військових і їх родин. Зокрема, розгорнуто систему “Паспорт”, яка забезпечує доступ військовослужбовців до даних, необхідних для його повсякденного життя

На базі технополісу “Эра” також розробляється комплекс гібридної реальності “Аватар”. Він буде застосовуватися для навчання й тренування військовослужбовців військ зв’язку і передбачатиме комплексне бойове задіювання підрозділів з використанням реальних зразків військової техніки зв’язку, а також одиночну й групову підготовку військових у навчальному класі з використанням віртуальних тренажерів.

Технологія сповільнення трафіку в РФ

Росія використовує нову технологію для сповільнення Інтернет-трафіку на території країни. Це перший відомий випадок, коли уряд піддає цензурі Інтернет-контент, обмежуючи трафік компанії, а не блокуючи доступ до її послуг.

Зокрема, за невиконання вимог російського законодавства з видалення протиправного контенту Роскомнагляд розпочав сповільнювати трафік Twitter. Для цього регулятор використовує технічні засоби протидії загрозам (ТЗПЗ), які прийшли на заміну системі технічних засобів для забезпечення роботи системи оперативно-розшукових заходів (СОРМ).

СОРМ, яка складається зі спеціальних мережевих пристроїв, встановлених в дата-центрах операторів зв’язку, дозволяє блокувати доступ до визначених доменів, додаючи їх в реєстр заборонених ресурсів. За наявності рішення суду та Роскомнагляду оператори зв’язку повинні змінювати відповідні налаштування міжмережевого екрану та блокувати трафік цих доменів. Проте, за останні роки стало зрозуміло, що таке блокування можна обійти за допомогою проксі- та VPN-сервісів.

Компанії, зокрема Telegram, знайшли спосіб обходу блокування за допомогою домен-фронтингу (використання різних доменних імен на різних рівнях HTTPS-з’єднання для непомітного підключення до другого цільового домена, який є непомітним для третіх сторін, що відслідковують запити та з’єднання).

Нові ТЗПЗ працюють не так, як СОРМ. Вони не знаходяться під контролем операторів зв’язку, а перебувають безпосередньо у віданні Роскомнагляду. ТЗПЗ розгортаються на два кроки ближче до кінцевого користувача, ніж СОРМ. Ці пристрої працюють не як традиційні міжмережеві екрани, а як мережеві DPI-фільтри. Рішення на базі DPI дають змогу бачити вміст мережевих пакетів та реальне місце їх призначення, навіть якщо з’єднання шифрується за допомогою TLS.

Як пояснили експерти Censored Planet, ТЗПЗ працюють шляхом аналізу розширення SNI протоколу TLS, завдяки чому Роскомнагляд може визначити до якого домена підключається користувач до того, як з’єднання буде зашифровано. Інцидент з Twitter є першим випадком використання ТЗПЗ. За словами експертів, це пояснює, чому перший запуск системи пройшов невдало – надто широке правило фільтрації призвело до сповільнення не лише трафіку Twitter, але й інших доменів

Прототип квантового комп'ютера в РФ

Наприкінці квітня поточного року Російський квантовий центр відкрив доступ до хмарної платформи квантових обчислень для дослідників і бізнесу. Платформа дозволяє вирішувати складні обчислювальні задачі на квантовому комп'ютері користувачам, що не мають профільної освіти і експертних навичок в квантовій механіці. Система самостійно перетворює задачу, сформульовану користувачем мовою математики, техніки або економіки, в програму для “бекенд” – квантового комп'ютера, а потім переводить результат обчислення назад в зрозумілу форму.

Платформа буде корисна для вирішення задач дискретної оптимізації, а також для аналізу економічного ефекту від впровадження квантових обчислювальних архітектур. В першу чергу, технологія розрахована на компанії в сфері фінансів, логістики, хімічної і атомної промисловості, біоінформатики і телекомунікацій.

Команда фахівців вже реалізує пілотні проєкти з низкою індустріальних партнерів, включно з автовиробником Nissan.

Платформа має інтуїтивно зрозумілий інтерфейс, що включає:

емулятор квантових обчислень SimCIM, розроблений і запатентований командою проекту.

Для вирішення завдань він використовує класичні алгоритми, які моделюють

- поведінку квантових систем;
- квантові комп'ютери, які створено в рамках реалізації дорожньої карти з квантових обчислень;
- квантові обчислювачі сторонніх міжнародних компаній.

Команда проєкту вже отримала заявки на підключення до хмарної платформи квантових обчислень від наукових установ та представників бізнесу з Росії, Франції, Німеччини, Великобританії, Тайваню та Китаю. Наразі триває процедура надання їм доступу і реалізації спільних проектів.

Крім Російського квантового центру, про відкриття доступу до власної хмарної квантової платформи оголосили і вчені з Центру квантових технологій фізичного факультету МДУ ім. М.В. Ломоносова. Програмна платформа для розробників квантових і гібридних квантово-класичних алгоритмів, представлена дослідниками, дає доступ до емуляторів квантових комп'ютерів на атомах і фотонах, розвиток яких здійснюється в рамках проєкту “Прибой” і Центру квантових технологій НТІ МДУ. У світі хмарний доступ до квантових комп'ютерів надають лідери в галузі квантових обчислень: Google, IBM, Microsoft та Amazon.

Створення міжнародної системи зберігання ключів шифрування

Російська Федерація виступила з пропозицією створити універсальну систему депонування (довіреного зберігання) ключів шифрування від мобільних додатків для оперативного доступу правоохоронних органів до даних. Закордонні партнери в цілому позитивно сприйняли цю пропозицію.

Наразі в соціальних мережах існують серйозні ризики, пов'язані з поширенням інформації, спрямованої на радикалізацію населення, а також такої, що вихваляє насильство, тероризм. Крім того, соціальні мережі неодноразово використовувались для цільового впливу на окремі соціальні групи населення, дестабілізації обстановки в різних країнах і регіонах світу.

У 2017 році, глава Федеральної служби безпеки Олександр Бортніков запропонував створити довірену і прозору для контролю систему депонування ключів шифрування, що генеруються мобільними додатками, для припинення їх безконтрольного використання терористами. За його словами, розробити єдині законні правила поводження з ключами шифрування і доступу до них можливо тільки за тісної співпраці між спецслужбами, операторами зв'язку і телекомунікаційними компаніями. Разом з тим, важливо повністю дотримуватись прав і свобод громадян в частині збереження конфіденційності даних.

TLS 1.0 та TLS 1.1 офіційно визнані застарілими

Інженерна рада Інтернету (Internet Engineering Task Force, IETF) офіційно визнала криптографічні протоколи TLS 1.0 і TLS 1.1 застарілими у зв'язку із загрозами безпеці, які вони становлять. IETF рекомендує всім компаніям, урядовим організаціям і розробникам програмного забезпечення використовувати актуальні версії TLS, зокрема TLS 1.2 і TLS 1.3, які вважаються безпечними.

Процес офіційного визнання обох протоколів застарілими розпочався в червні 2018 року. Його ініціаторами виступили IETF і вендори програмного забезпечення, включно з виробниками найбільших браузерів. Таке рішення було прийнято через виявлення протягом останніх кількох років низки атак на SSL, TLS 1.0 і TLS 1.1, таких як BEAST, POODLE, ROBOT, SWEET 32, LUCKY 13, що дозволяють скомпрометувати зашифроване з'єднання.

Хоча процес офіційного визнання TLS 1.0 і TLS 1.1 застарілими почався в червні 2018 року, свого піку він досяг у жовтні того ж року, коли великі виробники браузерів Apple, Google, Microsoft і Mozilla оголосили про намір відмовитися від їхнього використання у своїх продуктах. Завершення процесу було призначено на початок 2020 року, але через пандемію COVID-19 було перенесено на пізніший термін.

На сьогодні протоколи TLS 1.0 і TLS 1.1 офіційно визнано застарілими, і жоден сучасний браузер не завантажує сайти по HTTPS, налаштованому через ці протоколи. Але, не зважаючи на це, багато організацій як і раніше використовують їх: більше 32 мільйонів серверів і пристроїв все ще відкривають доступ до точок підключення TLS 1.0 і TLS 1.1.

НКЦК

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ