НКЦК

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

CYBER DIGEST

Огляд ключових подій у світі кібербезпеки за 12 – 26 вересня 2022 року

Підготовлено за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»

Створення цієї публікації стало можливим завдяки підтримці американського народу, наданій через Агентство США з міжнародного розвитку (USAID). Погляди авторів, висловлені у цій публікації, не обов'язково відображають погляди USAID або Уряду США.

ЗМІСТ

ОСНОВНІ ТЕНДЕНЦІЇ

- США продовжують процес практичного впровадження своїх стратегічних документів, зосереджуючись на питання поліпшення кібербезпеки ланцюжків постачання, протидії вірусам вимагачам та впровадженню політики «нульової довіри» (Zero Trust). З цією метою оприлюднено новий Меморандум щодо кібербезпеки програмних ланцюжків поставок, запущено програму грантової підтримки локальних урядів щодо їх кібербезпеки, додатково активізувала свою діяльність (в т.ч. – міжвідомчу) CISA: розпочала роботу група з протидії вірусам-вимагачам, оперативно оприлюднюються нові Оповіщення про загрози критичній інфраструктурі та новини щодо технік дій ворожих хакерських груп.
- ЄС зосереджений на прийнятті нового закону «Про кіберстійкість» (Cyber Resilience Act). Закон впровадить низку важливих змін, в т.ч. щодо розробки програмного забезпечення (запровадження принципу безпека-як-дизайн) та сертифікації послуг з точки зору їх безпеки. Нові норми (а також норми Директиви NIS2) викликають дискусії між країнами-членами. Зокрема, щодо можливості закриття європейського ринку перед неєвропейськими хмарними сервісами в частині послуг для критичної інфраструктури.
- Китай активізує свою внутрішню діяльність в сфері регулювання кіберпростору – оприлюднено нові ініціативи щодо посилення штрафних санкцій за порушення відповідного законодавства, в т.ч. як китайські хакери активно атакують сусідні країни (зокрема, Індію).
- Зловмисна активність хакерських груп не зменшується. Найбільш помітними інцидентами звітного періоду були кібератаки на: американську та португальську авіакомпанії, кібератака на Uber, систему управління освіти Лос-Анджелесу, одного з основних телекомоператорів Австралії. Крім того, хакери продовжують кібератаки проти Албанії, Боснії та Герцеговини.
- Віруси-вимагачі залишаються найбільшою загрозою для державних та приватних установ. Дослідницькі компанії у своїх звітах вказують на обмежену готовність організацій протидіяти таким атакам (особливо якщо вони здійснюються через ланцюжки поставок) та недостатні темпи впровадження політики Zero Trust. Важливим фактором є і нестача кібербезпекових навичок у співробітників організацій – як державних, так і приватних. Приватні компанії розпочали масштабні навчальні програми з цього питання. США намагається вирішити цю проблему в державному секторі через спеціальну грантову програму. ЄС шукає комплексне рішення через впровадження Європейської настанови з навичок кібербезпеки.
- Критична інфраструктура та її ОТ системи можуть стати наступними цілями хакерів. Дослідники виявляють нові загрози автоматизованим системам управління, CISA публікує рекомендації для ОКІ як їм захистити OT/ICS, а ФБР дає рекомендації щодо ліпшої кібербезпеки медичних пристроїв.

- Міжнародні фахівці продовжують досліджувати російсько-українську кібервійну. Хоча дискусії про те, чи є російська кіберактивність в Україні свідченням кіберійни триває, російські хакерські групи нарощують свою активність в європейських країнах, атакуючи як державні установи, так і окремі компанії в тих країнах, які підтримують Україну.

1. ІНІЦІАТИВИ НАЦІОНАЛЬНИХ СУБ'ЄКТІВ: СТРАТЕГІЇ, ЗАКОНОДАВСТВО, КАДРОВІ ЗМІНИ

Білий Дім оприлюднив нові настанови щодо посилення безпеки програмних ланцюжків постачання

На виконання Указу Президента США з кібербезпеки виданого у травні 2021 року, 14 вересня 2022 року був оприлюднений Меморандум щодо посилення безпеки програмних ланцюжків постачання (*Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*).

Цей документ вимагає від федеральних агентств дотримуватися вказівок NIST – щодо безпечної розробки програмного забезпечення та безпеки ланцюга постачання – під час використання програмного забезпечення сторонніх розробників. Щоб забезпечити відповідність, федеральні агентства повинні отримати форму самоатестації (меморандум встановлює мінімальні дані, які мають бути подані в цій формі) від розробників програмного забезпечення, чиї продукти вони використовують або планують використовувати.

США запустили державну кібербезпекову грантову програму для штатів та місцевих органів влади

16 вересня Уряд США оголосив про запуск державної кібербезпекової грантової програми (State and Local Cybersecurity Grant Program, SLCGP), яка допомагатиме державним і місцевим органам влади та іншим відповідним організаціям зменшити або усунути загрози кібербезпеці для їх IT-мереж і систем.

Обсяг програми – 1 млрд доларів. Операторами програми є CISA (*Cybersecurity and Infrastructure Security Agency*) та FEMA (*Federal Emergency Management Agency*). Програма охоплює декілька сфер поліпшення кібербезпеки, що включає в себе: систематизацію планування заходів з кібербезпеки, поліпшення підготовки фахівців та технічних заходів, що мають сприяти більшій стійкості та поінформованості учасників програми про кіберзагрози (в т.ч. - створення спільних локальних SOC).

Для участі у програмі зацікавлені організації мають подати детальні плани на розгляд CISA, яка має їх затвердити.

США розширили перелік китайських компаній, які можуть становити загрозу національній безпеці

23 вересня Федеральна комісія з комунікацій США (FCC) додала дві китайські компанії до списку організацій, чиє комунікаційне обладнання може становити загрозу національній безпеці: *Pacific Network Corp* та *China Unicom*

(Американське відділення). Відтепер американським компаніям, які використовують кошти федерального уряду, заборонено купувати обладнання цих компаній.

CISA оприлюднила свій перший стратегічний план розвитку на 2023-2025 роки

Вперше з моменту свого заснування CISA оприлюднила своє бачення стратегічних завдань та напрямків розвитку як кібербезпекового агентства. Документ визначає чотири основні цілі Агентства: кіберзахист, зменшення ризиків та розвиток стійкості, операційна взаємодія та внутрішній організаційний розвиток. Кожна з них містить від 4 до 6 завдань, які мають сприяти поліпшенню безпеки та стійкості критичної інфраструктури в інтересах американського народу.

CISA опублікувала запит на інформацію щодо Закону про звітність про кіберінциденти на ОКІ

12 вересня CISA опублікувала запит на інформацію (Request for Information), щоб зібрати пропозиції стосовно імплементації Закону про звітність про кіберінциденти на ОКІ, прийнятого у 2022 році. Закон вимагає від CISA протягом двох років опублікувати проміжне правило з детальним описом вимог щодо звітності про інциденти, які повинні виконувати компанії критичної інфраструктури. Респонденти мають 60 днів для надання своїх пропозицій. CISA також проведе 11 очних зустрічей, щоб отримати додаткові пропозиції від спільноти.

Директор CISA Джен Істерлі заявила, що внесок спільноти допоможе CISA «заповнити критичні інформаційні прогалини, що стане базою для рекомендацій, які ми надаємо всій спільноті, зрештою, допомагаючи нам краще захистити націю від кіберзагроз».

CISA спільно з ФБР провела першу зустріч новоствореної групи реагування на віруси вимагачі

14 вересня відбулось перше засідання групи реагування на віруси вимагачі (спільна група CISA та FBI). Предмет діяльності групи: пріоритизація операцій протидії таким вірусам, ефективна міжвідомча координація, ідентифікація найбільш загрозливих вірусів-вимагачів, обмін досвідом та аналіз тенденцій.

CISA, ФБР, Агентство національної безпеки, Казначейство, Кіберкомандування США та їх закордонні партнери оприлюднили спільну заяву щодо діяльності хакерів, пов'язаних з іранським урядом

Американські кібербезпекові відомства спільно з Австралійським центром кібербезпеки (ACSC), Канадським центром кібербезпеки (CCCS) та Національним центром кібербезпеки Великобританії (NCSC) оприлюднили спільну заяву щодо кіберзагроз, які походять з боку хакерських угрупувань, пов'язаних із Корпусом стражів ісламської революції (Іран). Було описано цілі та завдання їх зловмисної діяльності, основні тактики, методи та процедури, а також вразливості, які вони використовують для атак.

Сенат США затвердив призначення першого в історії кіберпосла

15 вересня сенат США одноголосно затвердив призначення Натаніеля Фіка Послом США з особливих доручень з питань кіберпростору та політики у цифровій сфері. Фік очолить створене у квітні бюро Державного департаменту з питань кіберпростору та політики у цифровій сфері *(Bureau of Cyberspace and Digital Policy*).

Бюро відповідає за три напрями державної політики: міжнародна безпека в кіберпросторі, міжнародна політика в галузі інформації та комунікацій та цифрова свобода. Під час слухань у сенаті Фік наголосив, що особливу увагу приділятиме зовнішнім загрозам, включаючи зловмисну діяльність рф у кіберпросторі та конкуренцію з Китаєм у галузі технологій.

Байден підписав виконавчий указ щодо безпеки зовнішніх інвестицій

15 вересня Президент Байден підписав перший з часу створення Комітету з іноземних інвестицій у США (CFIUS) Указ (*Executive order*), згідно з яким перед схваленням інвестиційної угоди, Комітет має розглянути додаткові питання, пов'язані з національною безпекою.

Указ чітко зазначає, що деякі країни використовують іноземні інвестиції для отримання доступу до конфіденційних даних і технологій з метою завдати шкоди національній безпеці США. Під час розгляду потенційних угод Комітет має дати відповіді на такі додаткові питання: чи впливає пропонована інвестиція на стійкість ланцюжків постачання в США, чи впливає вона на технологічне лідерство США, чи підсилює вона тенденцію негативного впливу на національну безпеку США, чи становить загрозу кібербезпеці, та/або чи може скомпрометувати особисті дані американців.

Збільшення уваги до загроз, що їх можуть становити іноземні інвестиції, стало трендом в західних країнах з огляду на тренд щодо вепонізації (*weaponization*) економічних механізмів.

Казначейство США наклало санкції на кіберактрорів з Ірану за причетність до атак з використанням віруса-вимагача

14 вересня Офіс з контролю за іноземними активами (OFAC) Казначейства США наклав санкції на десять фізичних осіб і дві організації, пов'язані з Корпусом вартових ісламської революції (КВІР) Ірану, за їхню роль у здійсненні зловмисних кібердій, включаючи дії програм-вимагачів.

В результаті накладання санкцій, все майно та інтереси у власності цих осіб, які знаходяться в Сполучених Штатах або у володінні чи під контролем осіб США, заблоковано. Також заблоковано можливість здійснювати фінансові транзакції, а фінансові установи, що надаватимуть їм послуги, ризикують також опинитися під санкціями.

ЄС розглядає можливість прийняття нового закону у кіберсфері – Закону про кіберстійкість (*Cyber Resilience Act*)

14 вересня Європейський Союз представив проект нового закону, який має забезпечити захист усіх пристроїв в Інтернеті речей – від «розумних» іграшок до холодильників. Намір розробити такий Закон був проголошений Урсулою фон дер Ляєн у вересні 2021 року під час її звернення про стан Європейського Союзу. Необхідність його прийняття також випливає зі Стратегії кібербезпеки ЄС до 2020 року та Стратегії Союзу безпеки ЄС до 2020 року.

Відповідно до проекту Закону про кіберстійкість (Cyber Resilience Act), щоб отримати маркування CE[1], цифрові продукти, що під'єднуються до мережі, повинні відповідати новим вимогам ЄС, незалежно від того де вони виробляються: в ЄС чи в інших країнах. Виробникам критично важливих продуктів, які порушують правила, загрожує штраф у розмірі до 15 мільйонів євро.

У додатку до закону визначено дві категорії продуктів: перша – критично важливі продукти, які охоплюватимуть близько десяти відсотків ринку, друга категорія – все інше. Виробники критично важливих продуктів, які представляють значний ризик для кібербезпеки, повинні будуть довести, що вони відповідають вимогам національного органу або надати оцінку третьої сторони.

Ця пропозиція ще має пройти обговорення, адже Європейський парламент та Європейська Рада вивчатимуть проект, і, можливо, запропонують внести до нього зміни. Комісія також запропонувала запровадити дворічний термін адаптації до повного запровадження нових правил. Тож правила, ймовірно, наберуть чинності не раніше 2025 року.

[1] Знак CE вказує на те, що продукт можна вільно продавати в будь-якій частині Європейської економічної зони, незалежно від країни його походження.

ЄС проводить комунікативну компанію щодо очікуваного прийняття Закону про кіберстійкість (Cyber Resilience Act)

15 вересня Європейська комісія оприлюднила офіційний довідник «Питання та відповіді» щодо майбутнього Закону про кіберстійкість. Це стало наслідком зростаючих дискусій щодо норм цього закону між європейськими країнами та Єврокомісією.

Документ описує основні загрози, з якими зіштовхуються європейські користувачі у сфері використання цифрових систем, та вказує якими шляхами ЄС планує мінімізувати ці загрози в цьому Законі. Зокрема, впровадження принципу «безпека-як-дизайн», сертифікацію (оцінку відповідності) цифрових продуктів, підвищення прозорості програмних рішень (в частині їх елементів, безпекової підтримки з боку розробників тощо). У разі невідповідності цифрових рішень встановленим вимогам, ЄС може вимагати або усунення невідповідностей або заборонити його поширення на європейському ринку.

Німеччина закликає до політичної дискусії щодо європейської схеми сертифікації хмарних систем

19 вересня міністри внутрішніх справ, економіки та цифрового розвитку Німеччини звернулись до керівника Цифрового департаменту Єврокомісії про необхідність проведення політичних дискусій щодо реалізації схем сертифікації, які мають бути запроваджені відповідно до Cybersecurity Act та Network and Information Security 2 (NIS2) Directive.

Занепокоєння викликає норма про те, що найвищі рівні надійності (відповідно до моделі сертифікації) будуть вимагати від постачальників хмарних послуг не лише мати штаб-квартиру в Європі, але і не бути контрольованими неєвропейськими резидентами. Таким чином ринок хмарних послуг ЄС буде обмежено лише європейськими компаніями. Проти цього підходу вже виступають Данія, Естонія, Греція, Ірландія, Нідерланди, Польща, Швеція та Німеччина. Підтримують цей підхід європейські оператори хмарних послуг.

ENISA представила Європейську настанову з навичок кібербезпеки (*European Cybersecurity Skills Framework*)

Під час конференції «*Building a cybersecurity workforce*» ENISA представила свою розробку – Європейську настанову з навичок кібербезпеки. Це документ (частково подібний до NICE від NIST) має створити спільне розуміння ролей, компетенцій, навичок і знань у фахівців з кібербезпеки. Він узагальнює ключові ролі, пов’язані з кібербезпекою у 12 профілях типових фахівців у сфері кібербезпеки, зокрема: головний офіцер з інформаційної безпеки (CISO), архітектор кібербезпеки, розслідувач цифрових злочинів та інші.

Цей документ має створити спільний освітній простір, де запити ринку на фахівців з кібербезпеки будуть більш адресно сформульовані для надавачів освітніх послуг, а майбутні студенти будуть краще розуміти сферу їх майбутньої компетенції.

ЄС намагається повністю заборонити країнам-членам використовувати шпигунське ПЗ проти журналістів та медіа

Європейська Комісія у новому документі *European Media Freedom Act* (EMFA) планує закріпити норми, які мають повністю захистити журналістів та редакції від спроб шпигування за ними з боку безпекових органів держав-членів ЄС за допомогою шпигунського ПЗ. Зокрема, пропонується включити норми, які забороняють використовувати таке ПЗ проти журналістів (та членів їх сімей), співробітників медіа (та членів їх сімей), або проти приватних чи бізнес-приміщень медіа лише на підставі того, що вони відмовляються розкрити джерела інформації. Виключення – лише якщо це не виправдано вимогою захисту суспільних інтересів.

Ця ініціатива стала наслідком серії політичних криз у Польщі, Угорщині, Іспанії та Греції, до яких призвели викриті випадки шпигування за допомогою спеціального ПЗ (такого як *Pegasus* чи *Predator*) за представниками політичної опозиції, громадянами та журналістами. Акти такого кібершпигунства відмічались і проти співробітників Єврокомісії.

Китай планує збільшити штрафи за порушення положень Закону про кібербезпеку

14 вересня Адміністратор кіберпростору Китаю (*the Cyberspace Administration of China, CAC*) оприлюднив свої пропозиції щодо внесення низки змін до Закону про кібербезпеку. Вони стосуються збільшення штрафів за окремі види порушень.

Так, оператори критичної інфраструктури, які використовують ПЗ чи послуги які не пройшли перевірку безпеки, можуть бути оштрафовані на 5% від їх прибутку за минулий рік або на суму більшу в 10 раз відносно тієї, яку вони заплатили за продукт/послугу. Також для низки чинних порушень буде суттєво збільшено штрафи: зі 100 000 юанів (приблизно 14300$) до 1 млн юанів.

Китай звинувачує NSA у використанні численних інструментів кібернападу проти китайського університету

Китайський Національний центр реагування на надзвичайні ситуації з комп'ютерними вірусами (*National Computer Virus Emergency Response Center*) звинуватив Агенство національної безпеки США у використанні щонайменше «41-го типу кіберзброї» проти Північно-західного політехнічного університету. За свідченнями експертів, більшість описаних у звіті інструментів є відомими і використовуються для шпигунських операцій (наприклад, *Suctionchar*). Китайська сторона звинувачує в атаці *Equation Group* – хакерську групу, яку вважають тісно пов'язаною з АНБ США.

Тайвань збільшує увагу до кіберзахисту

Кібератаки Китаю на Тайвань під час візиту спікерки Палати представників Конгресу США Ненсі Пелосі змусили Тайбей інвестувати більше у свій цифровий захист. «Уряд створює агентство з кібербезпеки в рамках нещодавно створеного Міністерства цифрових справ, яке очолює Одрі Танг – хакер, який став членом кабінету міністрів. Агентство спочатку найме 150 спеціалістів з кібербезпеки, що є різким збільшенням порівняно з 20 співробітниками, які були залучені в центрі кібербезпеки, пов'язаному з Кабінетом міністрів», – повідомив Томпсон Чау з Nikkei Asia.

2. МІЖНАРОДНІ ТА МІЖДЕРЖАВНІ ПОДІЇ В КІБЕРПРОСТОРІ

НАТО підтвердило свою готовність допомогти Албанії з подоланням наслідків кібератаки проти неї

21 вересня заступник помічника Генерального секретаря з нових викликів безпеці Джеймс Аппатурай зустрівся з міністром оборони Албанії Ніко Пелеші аби запевнити його у підтримці Албанії з боку членів НАТО в контексті останньої масштабної кібератаки. Представник НАТО запевнив міністра оборони в тому, що НАТО готово надати допомогу у розвитку кіберпотенціалу Албанії.

Учасники тихоокеанського союзу QUAD домовилися співпрацювати у галузі протидії вірусам-вимагачам

Про це йдеться у заяві, опублікованій на сторінці Білого дому після зустрічі міністрів закордонних справ Австралії, Індії, Японії та Держсекретаря США, яка відбулась 23 вересня. «Ми прагнемо відкритого, безпечного, стабільного, доступного та мирного кіберпростору та підтримуємо регіональні ініціативи з підвищення спроможності країн впроваджувати Рамкову програму ООН щодо відповідальної поведінки держав у кіберпросторі», – йдеться у заяві.

Країни QUAD зобов'язалися боротися з діяльністю вимагачів, що походять з їх території, наголосили на необхідності розбудовувати стійкість та спроможність в Індійсько-тихоокеанському регіоні. Підкреслили важливість дотримування мультистейхолдеристського підходу як базового принципу, що включає укріплення ролі існуючих механізмів, таких як Глобальний форум кіберекспертизи (GFCE). Також вони заявили, що вітають переговори щодо можливої нової конвенції ООН про боротьбу з кіберзлочинністю, яка застосовуватиме підхід, корисний у боротьбі з програмами-вимагачами. «Ми підкреслюємо необхідність розробки нової угоди в технологічно-нейтральній та гнучкій манері, яка не описує конкретних технологій чи кримінальних методів».

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

American Airlines визнало витік даних користувачів внаслідок липневої кібератаки

16 вересня *American Airlines* оприлюднила заяву, в якій визнало, що внаслідок хакерської атаки 5 липня 2022 року злочинці могли отримати доступ до конфіденційної інформації клієнтів. Зловмисники за допомогою фішингової атаки отримали доступ до невизначеної кількості облікованих записів співробітників компанії, а потім розширили свою присутність в мережі.

Хоча American Airlines наполягає, що дуже невелика кількість клієнтів компанії могла постраждати, однак превентивно готово оплатити доступ клієнтам до системи *Experian's IdentityWorks* – механізму моніторингу кредитів чи спроб використати вкрадені особисті дані з фінансовою метою.

Угрупування Vice Society атакувало вірусом-вимагачем управління освіти Лос-Анджелесу

Хакерська група *Vice Society* на День праці (5 вересня) атакувала системи управління освіти Лос-Анджелесу вірусом вимагачем, наслідки дії якого досі не подолані. 22 вересня влада підтвердила, що хакери висунули вимогу щодо викупу, але сума викупу не розголошується.

Хакерам вдалось отримати доступ до частини персональних даних студентів. Угрупування *Vice Society* орієнтоване на атаки вірусами-вимагачами закладів освіти.

Іран продовжує атакувати Албанію

Вже після того, як Тірана розірвала дипломатичні стосунки з Тегераном через попередні кібератаки, спонсоровані державою хакери від'єднали від Інтернету Загальну систему управління інформацією (TIMS), яка використовуються для прикордонного контролю. У відповідь на попередні атаки, OFAC США наклав санкції на Міністерство розвідки та безпеки Ірану (MOIS) і Міністра розвідки Ірану. Згідно з розслідуванням, проведеним ФБР, хакери отримали доступ до системи за 14 місяців до атаки.

Події відбуваються на тлі запрошення Ірану до ШОС, яку західні аналітики називають антизахідним клубом. Кібератака проти Албанії є важливим кейсом з точки зору масштабної кібератаки проти країни-члена НАТО.

Хакери успішно атакували португальські національні авіалінії

У вересні стало відомо, що португальські національні авіалінії TAP були атаковані хакерами (попередньо хакерською групою *Ragnar Locker*). Зловмисникам вдалось заволодіти деякими персональними даними клієнтів (орієнтовно – 1,5 млн облікових записів), а пізніше опублікувати цю інформацію в даркнеті. Вимоги щодо викупу не висувались.

Кібератака проти Optus – одного з ключових телекомунікаційних операторів Австралії

23 вересня стало відомо, що невстановлене хакерське угрупування провело масовану кібератаку проти одного з найбільших (9 млн користувачів) телекомунікаційних операторів Австралії – *Optus*. Зловмисникам стали доступні персональні дані споживачів, в окремих випадках їх фізичні адреси.

До розслідування долучені Австралійський центр кібербезпеки, Федеральна поліція та Австралійський Комісар з інформації (відповідає за безпеку персональних даних). Крім розслідування самого злочину Комісар з інформації намагається оцінити чи не порушила компанія національне законодавство щодо персональних даних (зокрема, вимогу негайно інформувати тих клієнтів, чиї персональні дані могли стати доступні зловмисникам).

Іранські хакери прицільно атакують визнаних експертів в галузі ядерної безпеки та геномних досліджень

Мета атак – збір чутливої інформації. Ці атаки відрізняються від інших фішингових атак використанням тактики Proofpoint під назвою Multi-Persona Impersonation (MPI). Таким чином зловмисник використовує не одну, а кілька керованих актором персон в одному обміні електронними поштовими повідомленнями, щоб збільшити шанси на успіх.

Боснія і Герцеговина розслідує можливу атаку вірусу-вимагача на парламент країни

19 вересня ЗМІ повідомили, що вебсайт парламенту Боснії та Герцеговини не працює протягом двох тижнів. Депутати повідомили місцевому виданню «Незавісне», що їм наказали навіть не вмикати свої комп’ютери, заборонивши користуватися своїми обліковими записами електронної пошти та відкривати офіційні документи.

Офіційно не повідомляється, про який тип атаки йдеться, але зі своїх джерел видання дізнались, що йдеться про програму-вимагач. Sarajevo Times повідомила, що головний сервер парламенту був вимкнений одразу після нападу. Країна перебуває в розпалі політичних потрясінь, оскільки зростає занепокоєння щодо спроб відокремлення Республіки Сербської. Якщо чутки про атаку програм-вимагачів підтвердяться, це буде ще один інцидент цього року, коли групи кібервимагачів використовують політичні суперечки у своїх інтересах.

Хакери використовують оголошення у Facebook, щоб надсилати посилання для збору облікових даних

13 вересня фірма Avanan повідомила, що хакери використовують емейли нібито від служби бізнес-оголошень компанії Meta для збору персональних даних та іншої чутливої інформації користувачів. Механізм такого збору описано у дослідницькому звіті компанії. Мішенню такої атаки може стати будь-хто.

Lazarus APT використовує три трояни для атак на користувачів у Північній Америці

Cisco Talos відстежує нову кампанію, керовану групою Lazarus APT, яку уряд Сполучених Штатів приписує Північній Кореї. Кампанія проходить із використанням вразливостей у VMWare Horizon та спрямована проти постачальників енергії з усього світу, включаючи ті, що мають штаб-квартири в Сполучених Штатах, Канаді та Японії.

Кампанія направлена на проникнення в організації по всьому світу для встановлення довгострокового доступу та подальшого викрадання даних, які становлять інтерес для держави супротивника. Cisco Talos виявив використання двох відомих сімейств шкідливих програм – VSingle і YamaBot. Також виявлено використання нещодавно оприлюдненого імплантату, який отримав назву «MagicRAT».

Пов’язані з Китаєм хакери вкрали у громадян Індії близько 529 мільйонів доларів

У вересні 2022 року індійські ЗМІ повідомили про надзвичайно успішну операцію китайських кіберзлочинців, в межах якої вони викрали у громадян Індії 529 мільйонів доларів. Для цього злочинці використали додатки для миттєвого кредитування, «прості» схеми швидкого підробітку та фіктивні схеми торгівлі криптовалютою.

Злочинці створили численні фіктивні сайти та додатки, які просували за допомогою масової розсилки СМС операторами, деякі з яких знаходились у Непалі. Отримані гроші були спочатку виведені на цифрові гаманці індійських банків, а потім через крипто платформи Zebpay та Binance.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

CISA оприлюднила рекомендації для кібербезпеки 5G OPEN RAN архітектури

CISA спільно з АНБ США оприлюднили набір рекомендацій щодо основних підходів із забезпечення кібербезпеки мереж, які будуються на основні Open RAN архітектури. Підкреслено, що це лише загальні підходи до проблеми та базуються на вивчені поточного досвіду реалізації проектів Open RAN.

MITRE створило новий інструмент протидії інсайдерським атакам проти ОКІ

Корпорація MITRE спільно з DTEX Systems 19 вересня презентували програму Inside-R Protect – комплексний інструмент для захисту великих організацій від інсайдерських атак. Це програма моніторингу мережевої активності співробітників організації з метою виявлення відхилень від шаблонної чи типової діяльності, як можливого фактору діяльності інсайдера. Основна спрямованість програми – допомога ОКІ в країнах, що належать до альянсу «Five eyes».

CyberCube випустила звіт щодо діяльності рф у кіберпросторі протягом 6 місяців війни

12 вересня аналітики кіберризиків з CyberCube, опублікували новий звіт, в якому розглядають ідею створення суверенного російського Інтернету як безпековий ризик. На їх думку, його поява може призвести до появи безпечних місць для переховування кіберзлочинців, більшої впевненості в тому, що широкомасштабні атаки можна здійснити без наслідків, і появи місць, недосяжних для розвідки.

У звіті описується як протягом шести місяців після вторгнення росії в Україну кібервійна слугувала важливим інструментом для сприяння кінетичній складовій військових дій. Серед іншого у звіті описано, як росія використовує програми-вимагачі аби підірвати економіку США. При цьому уникаючи прямої війни зі США, а також атаки проти Європейських енергетичних компаній, що має на меті підірвати їх стратегічну цінність.

Описані також атаки російських зловмисних груп націлені на інші уряди. Такі атаки мають на меті збір розвідданих про західних союзників, які допомагають Україні у військових діях.

5. КРИТИЧНА ІНФРАСТРУКТУРА

CISA та NSA випустила спільний порадник щодо захисту OT/ICS

22 вересня CISA та NSA оприлюднили спільний матеріал «Як кіберактори компрометують OT/ICS та як захиститись від цього». У матеріалі підкреслюється, що останнім часом APT-групи все частіше націлюються на системи OT/ICS (характерні для сфери критичної інфраструктури), щоб досягти політичних цілей, економічних переваг і, можливо, здійснити руйнівний вплив на них. Деякі з цих груп вже розробили інструменти для сканування, зламу та контролю цільових пристроїв OT.

Оприлюднений документ базується на попередніх вказівках NSA та CISA щодо припинення зловмисної діяльності проти ICS та зменшення ризику для OT. Документ розкриває основні техніки зловмисників, порядок їх дій та надає рекомендації щодо попередження такої зловмисної діяльності.

Виявлено вразливість у системі керування резервуарами для води, які використовуються в усьому світі

Дослідник Максім Рупп (*Maxim Rupp*) дослідив систему керування резервуаром для води *Kingspan TMS300 CS*. Він виявив, що система має критичну вразливість (CVE CVE-2022-2757), спричинену відсутністю належним чином реалізованих правил контролю доступу. Це дозволяє неавтентифікованому зловмиснику переглядати або змінювати налаштування пристрою (в т.ч. показники датчиків, функціонування деталей резервуарів та порогові значення тривоги). Продукт, який зазнав впливу, використовується в усьому світі в системі водопостачання та водовідведення.

ФБР надало п'ять рекомендацій для поліпшення безпеки медичних пристроїв

12 вересня ФБР оприлюднило свої рекомендації для забезпечення кібербезпеки медичних пристроїв (*devices*). Ці рекомендації з'явилися на фоні збільшення кількості кібератак проти медичних установ, а також заяви ФБР, що вони відзначають зростаючу кількість вразливостей, пов’язаних із медичними пристроями, які досі не виправлені, працюють із застарілим програмним забезпеченням і пристроями, які не мають відповідних функцій безпеки. Це може негативно вплинути як на заклади охорони здоров’я, так і на їх клієнтів.

З метою мінімізації ризиків ФБР рекомендує зосередитись на таких заходах: захист кінцевих точок (*endpoint protection*), управління ідентифікацією та доступом, управління активами, управління вразливостями, проведення навчань з кібербезпеки для персоналу.

6. АНАЛІТИЧНІ ОЦІНКИ.

Новий аналітичний звіт попереджає, що США відстає від Китаю у сфері деяких ключових технологій

12 вересня було опубліковано новий звіт *Special Competitive Studies Project*, в якому досліджується стан конкуренції між США та Китаєм у сфері новітніх технологій.

На думку авторів звіту, Китай випереджає Сполучені Штати у сфері 5G, комерційних дронів, наступальної гіперзвукової зброї та виробництва літієвих батарей. Тоді як США випереджають Китай у біотехнологіях, квантових обчисленнях, хмарних обчисленнях, комерційних космічних технологіях та мають невелику перевагу в області штучного інтелекту.

Вважається, що результат цієї конкуренції буде дуже важливим не лише для США та їх національної безпеки, але й для усіх демократичних країн світу. Звіт містить низку рекомендації для органів влади США, які мають на меті покращити конкурентоспроможність країни.

Злам Uber може бути більш масштабний, ніж передбачалось – потенційно скомпрометовано всі системи

14 вересня стало відомо, про масштабний злам внутрішніх систем компанії Uber. Хакер, який зламав доступ до кількох внутрішніх систем, отримав адміністративний доступ до хмарних сервісів Uber, зокрема Amazon Web Services (AWS) і Google Cloud (GCP).

За попередньою інформацією злам став можливий завдяки використанню соціальної інженерії – хакери змогли переконати співробітника компанії повідомити йому пароль після того, як він назвався співробітником відділу з корпоративних інформаційних технологій. За іншою версією доступ було отримано через скомпрометований доступ компанії-підрядника.

Компанія Uber вважає, що за зламом стоїть група Lapsus$.

Дослідники детально описали OriginLogger RAT

14 вересня підрозділ 42 Palo Alto Networks повідомив, що детально описав внутрішню роботу шкідливого програмного забезпечення під назвою OriginLogger, відомого як наступник широко використовуваного трояна Agent Tesla. Це зловмисне програмне забезпечення використовує перевірені та надійні методи та серед іншого здатне вести кейлог, викрадати облікові дані, робити знімки екрана, завантажувати додаткові корисні дані, завантажувати ваші дані безліччю способів і намагатися уникнути виявлення.

Загрози вірусів-вимагачів для ланцюжків постачань зростають. І компанії не готові до цього

20 вересня компанія Trend Micro поширила результати свого дослідження «Все пов'язано: виявлення загрози програм-вимагачів в глобальних ланцюгах постачань». Його мета – шляхом інтерв'ю майже 3000 керівників IT-рішень у 25 країнах з'ясувати їх рівень готовності відповісти на загрози використання вірусів-вимагачів проти ланцюжків постачань.

На думку авторів звіту, основа кіберзахисту в ланцюжках постачань – обмін інформацією про кіберзагрози між учасниками. Відповідно до результатів, лише 47% компаній діляться інформацією про кіберзагрози зі своїми постачальниками, а 25% – ніколи цього не робить.

Нове дослідження Fortinet чіткіше показує зв'язок між браком кібербезпекових навичок та зростанням зламів

12 вересня компанія Fortinet оприлюднила своє дослідження «2022 Cybersecurity Skills Gap». Воно охопило 1,223 IT-керівників у 29 країнах. Мета дослідження – з'ясувати стан з кібернавичками в приватному секторі та зрозуміти вплив цих навичок на кібербезпеку організацій.

Відповідно до цього дослідження 80% респондентів щонайменше раз протягом останнього року стикались з порушеннями безпеки (витоками), а для 40% їх усунення коштувало понад один млн доларів. 67% вказують на те, що брак кібернавичок збільшує ризики для їх організацій. 95% IT-керівників вважають, що міжнародні сертифікати важлива перевага для їх співробітників і намагаються наймати людей з сертифікатами (або готові платити за навчання співробітників). 87% вже запровадили програми поліпшення навичок кібербезпеки для співробітників.

Компанії, які впровадять Zero Trust, зможуть зберегти до одного млн доларів внаслідок витоків

Компанія IBM оприлюднила 23 вересня свій звіт «2022 IBM Cost of a Data Breach Report». В ньому досліджуються фінансові наслідки витоку даних для компаній з різних секторів та індустрій. Зокрема, 80% досліджених компаній мали більше ніж один витік даних. Середня вартість витоку для компанії становить близько 4,35 млн доларів у 2022 році (що на 12,7% вище, ніж в попередні два роки). 60% компаній розв'язали проблеми цих втрат збільшивши вартість послуг для користувачів.

Основна рекомендація звіту – впровадження підходу Zero Trust, що дозволить істотно зменшити вірогідність витоків даних та зменшити втрати від них (до 1 млн на кожному витоку). Станом на момент проведення дослідження 80%

досліджених компаній, що належать до критичної інфраструктури, не впровадили Zero Trust підхід.

Атаки з логікою «Збери зараз, розшифруй пізніше» викликають занепокоєння з огляду на розвиток квантових обчислень

Згідно з опитуванням проведеним компанією Deloitte, більш ніж половина опитаних спеціалістів в організаціях, які розглядають переваги квантових обчислень, вважають, що їхні організації піддаються ризику атак типу «збери зараз, розшифруй пізніше» (HNDL[2]) (50,2%). Дослідники зазначають, що такий ризик актуальний для всіх організацій, але далеко не всі вони вживають заходів, щоб йому запобігти.

GAO опублікувала звіт з рекомендаціями щодо покращення управління IT на федеральному рівні

У звіті порівнюються обов'язки, кваліфікація та тривалість роботи 71 опитаних IT-директорів у приватному та держаному секторі. Автори звіту досліджують як досвід IT-директорів приватного сектора можна застосувати до викликів, з якими стикаються IT-директори федеральних агентств. Вони надають рекомендації законодавчій та виконавчій гілкам влади США щодо покращення управління IT у державному секторі.

GAO розкритикувала Управління з ядерної безпеки США за збої в кібербезпеці

22 вересня Управління звітності уряду США (GAO) опублікувало звіт, в якому описуються недоліки у сфері кібербезпеки Національного управління ядерної безпеки (NNSA) – окремого відомства в рамках Міністерства енергетики (DOE), яке відповідає за управління ядерною зброєю США в восьми лабораторіях та виробничих майданчиках по всій країні.

Згідно з GAO, NNSA та його підрядники не повністю запровадили шість федеральних практик щодо кібербезпеки, серед яких впровадження базових практик управління ризиками та інші настанови. Як наслідок, «NNSA та його підрядники не мають повного розуміння свого стану кібербезпеки та обмежені у своїй здатності ефективно реагувати на нові кіберзагрози», – йдеться у звіті GAO.

[2] Злочинці збирають навіть зашифровану чутливу інформацію із «довгим строком життя» (наприклад, державні таємниці чи об'єкти інтелектуальної власності) в надії використати її (розшифрувавши) після появи потужних квантових комп'ютерів.

GAO опублікувала звіт з рекомендаціями щодо покращення управління IT на федеральному рівні

У звіті порівнюються обов’язки, кваліфікація та тривалість роботи 71 опитаних IT-директорів у приватному та держаному секторі. Автори звіту досліджують як досвід IT-директорів приватного сектора можна застосувати до викликів, з якими стикаються IT-директори федеральних агентств. Вони надають рекомендації законодавчій та виконавчій гілкам влади США щодо покращення управління IT у державному секторі.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ.

Секретар РНБО України О. Данілов провів засідання НКЦК

22 вересня відбулось двадцяте засідання Національного координаційного центру кібербезпеки. На ньому були розглянуті питання про стан реалізації Стратегії кібербезпеки України і затвердження індикаторів її виконання.

«Кіберскладова цієї війни є не менш важливою, ніж військова, це фундаментально важливий фронт. Зараз важлива максимальна координація та командна робота всіх суб'єктів забезпечення кібербезпеки у питаннях реагування на кіберінциденти та відбиття кібератак в умовах воєнного стану», – наголосив Секретар Ради національної безпеки і оборони України Олексій Данілов.

Затверджено Порядок взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки

Документ одноголосно був затверджений на засіданні НКЦК 22 вересня. Порядок взаємодії був розроблений створеною при НКЦК робочою групою, до складу якої входили представники усіх основних суб'єктів національної системи кібербезпеки, а також Мінцифри, МЗС та Національного інституту стратегічних досліджень.

У Порядку взаємодії висвітлені питання інформаційного обміну, координації та спільних дій суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки. Зокрема, документ визначає принципи, на яких ґрунтуватиметься застосування цього Порядку та передбачає створення при НКЦК постійної Об'єднаної групи реагування на кіберінциденти та кібератаки.Також залежно від ступеня негативних наслідків, що можуть настати в результаті реалізації кіберінциденту/кібератаки, запроваджується шість рівнів критичності, які були розроблені з урахуванням кращих світових практик

Ознайомитись з Порядком взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки можна тут.

СБУ повідомило про підозру колишньому заступнику міністра охорони здоров'я щодо порушень під час запуску цифрової медицини

Кіберфахівці СБУ викрили ексзаступника міністра, чиї дії призвели до збитків держави на 2 млн гривень та зашкодили створенню реєстру донорів. Зокрема, Єдиної державної інформаційної системи трансплантації органів та її інтегрування до систем іноземних держав та міжнародних організацій.

Триває досудове розслідування для встановлення всіх обставин правопорушення і притягнення до відповідальності винних осіб.

СБУ нейтралізувала хакерське угруповання, яке «зламало» майже 30 млн акаунтів громадян України та ЄС

Служба безпеки нейтралізувала хакерське угруповання, яке діяло в інтересах країни-агресора у Львові. Використовуючи шкідливе програмне забезпечення, зловмисники зламували активні облікові записи інтернет-користувачів з України та Євросоюзу, отримуючи доступ до персональних даних громадян.

Цю конфіденційну інформацію вони продавали через анонімну платформу «Даркнет», а гроші отримували на заборонені в нашій державі електронні платіжні системи ЮMoney, Qiwi та WebMoney. За попередніми даними, хакери продали орієнтовно 30 млн акаунтів і одержали «прибуток» у розмірі майже 14 млн грн.

Їхніми «оптовими клієнтами» були прокремлівські пропагандисти. Саме вони використовували одержані установчі дані українських та іноземних громадян для поширення фейкових «новин» з фронту та створення панічних настроїв. Метою таких маніпуляцій була масштабна дестабілізація в країнах.

Кіберполіція створила спеціальну вебплатформу з шифруванням інформації, щоб допомогти компаніям, які постраждали від хакерських атак

Наприкінці минулого року правоохоронці викрили транснаціональне злочинне угруповання, учасники якого здійснювали атаки з використанням програмного забезпечення типу Ransomware. Під час слідчих дій отримано техніку та носії інформації, які дозволяють потерпілим дешифрувати закриптовані дані без оплати викупу хакерам.

За результатами аналізу носіїв отримано численні приватні ключі від атак програм-вимагачів. Зазначені ключі дають можливість потерпілим компаніям і установам відновити раніше зашифровані дані. Для цього кіберполіцейські у співпраці з Європолом, проєктом «No More Ransom» та компанією «BitDefender» створили спеціалізований вебресурс – www.nomoreransom.org.

Окупанти готують масовані кібератаки на об’єкти критичної інфраструктури України та її союзників

Кремль планує здійснити масовані кібератаки на об’єкти критичної інфраструктури українських підприємств й установ критичної інфраструктури союзників України. У першу чергу удар буде спрямовано на підприємства

енергетичної галузі. При проведенні операцій використовуватиметься досвід кібератак на енергосистеми України 2015 та 2016 років.

Цим ворог спробує посилити ефект ракетних ударів по об’єктах електрозабезпечення насамперед у східному та південному регіонах України. Командування окупантів переконано, що це призведе до сповільнення наступальних дій українських Сил оборони.

Також кремль має намір збільшити інтенсивність DDoS-атак на критичну інфраструктуру найближчих союзників України, насамперед Польщі та країн Балтії.

8. ПЕРША СВІТОВА КІБЕРВІЙНА

Що ми насправді знаємо про російську кібервійну проти України?

Стефані Карвін (*Stephanie Carvin*) з Карлтонського університету намагається надати загальну оцінку кіберпротистоянню в Україні. Вона висловлює думку, що можливо низька ефективність російських кібератак обумовлена не стільки гарним кіберзахистом України, скільки тим, що Росія не розглядала кібератаки важливим елементом вторгнення. І що відсутність можливості кібератакувати саме військові цілі зменшила привабливість такого типу атак для агресора.

Саме розуміння того, «чи йде в Україні кібервійна» багато в чому залежить від того, як її собі уявляють експерти. Відповідно ті, хто очікував «Цифрового Перл Харбору» вважають, що кібервійни немає. В той час як ті, хто сприймає кібервійну як приховані операції, констатують її наявність.

Східноєвропейська організація зазнала потужної DDoS-атаки

16 вересня компанія Akamai (надавач хмарних послуг) повідомила, що допомогла своєму клієнту, неназваній компанії зі Східної Європи, відбити DDOS-атаку потужністю понад 700 Mpps. Ані атакована компанія, ані потенційні зловмисники не називаються, однак у довідкових матеріалах щодо цієї атаки Akamai посилається на два Оповіщення (alerts) CISA, які присвячені кіберзагрозам, що походять від спонсорованих росією хакерських угрупувань.

Компанії, які надають хмарні послуги протягом всього останнього півріччя, фіксують стрімке збільшення кількості та потужності DDOS-атак.

Проросійська хактивістська мережа Killnet атакує Європу

Група російських хактивістів під назвою Killnet атакує уряди європейських країн, інфраструктуру та навіть престижний пісенний конкурс Євробачення, намагаючись утримати їх від підтримки України у війні за допомогою кібератак і кампанії з дезінформації. Фахівці з кібербезпеки ставляться до цієї групи швидше як до незначної неприємності, ніж як до серйозної загрози. На сьогодні немає інформації, яка б підтверджувала, що діяльність угруповання керується російською державою.

Чорногорія продовжує боротися з наслідками російської кібератаки

Станом на 16 вересня, Чорногорія все ще не оговталась від кібератак, яких вона зазнала з боку рф через підтримку України. Хоча атаки відбулися за три тижні до того, їх наслідки досі відчутні. Адміністрація Elektroprivreda Crne Gore оголосила, що чорногорські гідроелектростанції перейшли на ручну систему керування, а деякі системи тимчасово відключені.

Урядові сервери також продовжують функціонувати офлайн від 26 серпня з огляду на можливі подальші атаки. Глава Державної служби кібербезпеки Душан Полович 15 вересня заявив, що система може знову стати публічно доступною протягом кількох наступних тижнів, підкресливши, що системи мають резервну копію, тобто дані збережені. Так само як і випадок Албанії, цей кейс є цікавим з точки зору того, що відбулась атака на країну-члена НАТО.

Російські хакери Gamaredon атакують український уряд за допомогою зловмисного програмного забезпечення для крадіжки інформації

Згідно з результатами дослідження, яким 15 вересня дослідники Cisco Talos Ашир Малхотра та Гільєрме Венере поділилися з Hacker News, триває шпигунська кампанія, яку проводить пов’язана з росією група «Гамаредон». Ціллю зловмисників є співробітники українських урядових, оборонних і правоохоронних органів.

Мета – крадіжка інформації за допомогою спеціально створеної шкідливої програми для такої крадіжки. «Щоб заманити користувачів, зловмисники використовують фішингові документи з приманками, пов’язаними з російським вторгненням в Україну», – йдеться у повідомленні.

Russia-Nexus UAC-0113 імітує телекомунікаційних провайдерів в Україні

19 вересня аналітики Recorded Future опублікували звіт, в якому, серед іншого, йдеться про те, що російські державні хакери маскуються під українських телеком провайдерів, щоб проводити фішингові атаки проти України. Йдеться про пов’язане з ГРУ угрупування Nexus UAC-0113, яке українська CERT-UA пов'язує з Sandworm.

Боротьба з російськими хакерами вимагає визнання складності мережі російських кіберактерів

Відповідно до оприлюдненого 19 вересня звіту Атлантичної ради, політики не можуть протистояти російським кібератакам, поки не визнають, що «російська» кіберактивність охоплює різноманітний ландшафт підтримуваних державою, напівнезалежних і незалежних кіберактерів. Окрім операторів російських військових і розвідувальних служб, до нього входять підставні компанії, патріотичні хакери та кіберзлочинці.

Враховуючи калейдоскопічну природу загрози, автор звіту Джастін Шерман рекомендує США та їх союзникам вивчити стосунки кожної російської групи з Кремлем, розробити конкретні відповіді для окремих хакерських груп та вивчити як Москва розглядає свої зв’язки з кожною хакерською групою.

Як білоруські хактивісти використовують цифрові інструменти у політичній боротьбі

Білоруські кіберпартизани роблять свій внесок у повалення Лукашенка, розкриваючи державні таємниці та атакуючи комп'ютерні системи підприємств, які підтримують режим диктатора. Хоча група складається здебільшого з молодих технічних спеціалістів та активістів, Cyber Partisans нагадують аматорську розвідувальну службу: вони мають політичні завдання, чіткі цілі та докладають багато зусиль для збору та аналізу конфіденційних даних.

Кіберпартизани збирають пожертви у криптовалюті на утримання дорогих серверів та розробку нових інструментів для хакерської діяльності, а також мобільних застосунків для активістів. Крім того, вони створюють відео, які висміюють Лукашенка та його соратників і хочуть спровокувати припинення дружніх стосунків між росією та Білоруссю.

Російська компанія Positive Technology планує дотримуватись раніше визначеної стратегії розвитку

Positive Technology, проти якої ще у 2021 році США ввели санкції, розмістила на Московській біржі пакет власних акцій. Це відповідає раніше затвердженій стратегії розвитку компанії. Попри істотне падіння російського фондового ринку та російської економіки, компанія не лише не згортає свою діяльність, але й розширює її.

Positive Technology підозрюють у тісній співпраці з російськими спеціальними службами.

Anonymous «злили» особисті дані 300 тисяч осіб, яких планують мобілізувати в рф

Хакерська група Anonymous продовжує атаки на органи державної влади росії. У вересні вони зламали міністерство оборони росії та «злили» в мережу особисті дані понад 300 тисяч росіян, яких планують мобілізувати найближчим часом. «Ознайомитися» зі списком можливо за посиланням. Це TXT-файл розміром 90 МБ.

Хакери показали виступ Зеленського на кримському «ТБ»

24 вересня невідомі зламали ефір кримського. На Першому каналі було показано звернення президента України Володимира Зеленського із закликом до мобілізованих.

В промові Зеленський прокоментував ситуацію з мобілізацією у росії. Після цього по телебаченню показали мітинги проти мобілізації із закадровим голосом путіна, збори військових росії, а також їхні трупи.

9. РІЗНЕ

12 вересня компанія Google завершила придбання фірми Mandiant

12 вересня Google завершила придбання кібепбезпекової фірми Mandiant. «Ми раді розпочати нашу спільну місію зі створення комплексного та найкращого у своєму класі рішення кібербезпеки для клієнтів і партнерів», – заявили у Mandiant.

США працюють над залученням можливостей Штучного Інтелекту для прогнозування потреб України у зброї та боєприпасах

Міжнародний центр координації донорів (International Donor Coordination Center, or IDCC) вивчає можливість залучення ШІ не просто для оптимізації постачання озброєння в Україну, але завчасного прогнозування таких потреб України для поліпшення стратегічного планування.

Це допоможе партнерам ефективніше підтримувати Україну у її боротьбі із рф у довгостроковій перспективі. Також ця система має сприяти кращому обліку наданої Україні допомоги. На цей час невідомо, коли така система буде введена в дію.