НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

УКРАЇНСЬКА ФУНДАЦІЯ БЕЗПЕКОВИХ СТУДІЙ

CYBER DIGEST

Огляд подій в сфері кібербезпеки,
квітень 2024

Ця публікація стала можливою завдяки підтримці, наданій Агентством США з міжнародного розвитку, згідно з умовами гранту Української фундації безпекових студій в рамках Проєкту USAID "Кібербезпека критично важливої інфраструктури України".

Думки автора, висловлені в цій публікації, не обов'язково відображають погляди Агентства США з міжнародного розвитку або Уряду США.

ЗМІСТ

ОСНОВНІ ТЕНДЕНЦІЇ

США продовжують ротацію фахівців з кібербезпеки та розширення кібербезпекового блоку. На фоні запиту Білого дому щодо кібербезпекової складової бюджету 2025 року у 13 мільярдів доларів США, було призначено нового директора з кібербезпеки в АНБ та створено департамент кіберполітики в Пентагоні. АНБ та CISA продовжує випускати рекомендації з безпеки (передусім щодо впровадження Zero Trust). Водночас кількість інцидентів зростає. У квітні прокотилась хвиля кібератак на муніципальні ресурси США, міські IT-системи та продовжились атаки на водний сектор США. За останніми були виявлені зусилля російських кіберугрупувань. США все ще розбирається з наслідками кібератаки на Change Healthcare.

З'являються все нові деталі кіберінциденту, який наніс компанії UnitedHealth (якій належить Change Healthcare) 872 млн доларів збитків. Також стало відомо, що хакерам вдалось викрасти значний обсяг персональних даних клієнтів компанії, а її генеральний директор буде свідчити перед Палатою представників США. Це не єдиний інцидент з американськими компаніями у сфері охорони здоров'я у квітні – медичний конгломерат Kaiser повідомив про витік даних мільйонів своїх клієнтів (всього він має 13,4 мільйона клієнтів). Вочевидь, ці події призведуть до змін підходів до кібербезпеки сфери охорони здоров'я та розробки відповідних стандартів. Останнє може стати проблемою в тому числі через недофінансування ключової американської агенції, що опікується розробкою таких стандартів – NIST.

В рамках наближення до європейських стандартів та стандартів НАТО у цифровій та кіберсфері, Україна провела першу зустріч з представниками ЄС як країна-кандидат, присвячену сфері цифровізації. В її рамках відбулася пояснювальна сесія Європейської комісії для України щодо переговорного Розділу 10 «Цифрова трансформація та медіа». Міністерство оборони наказом затвердило основні засади інформаційної безпеки та кібербезпеки в інформаційно-комунікаційних системах міністерства. Вони враховуватимуть кращі підходи НАТО, міжнародні стандарти та практики з інформаційної та кібербезпеки. В рамках третього міжнародного засідання Національного кластера кібербезпеки на тему: «Розбудова партнерств для кіберстійкості Південно-Східної Європи» було обговорено тему поглиблення співпраці з ЄС та НАТО та практичні кроки, що Україна робить у сфері кібербезпеки. Секретар НКЦК Наталя Ткачук закликала країни ЄС та НАТО до спільної протидії кіберагресії рф.

Україна підвищує кваліфікацію та збільшує обізнаність у питаннях кібербезпеки на всіх рівнях. Серед іншого, НКЦК провів навчання «Управління вразливостями» для фахівців з кібербезпеки з обласних військових адміністрацій, що дозволить їм покращити навчки у проведенні комплексного аналізу стану кібербезпеки своїх установ та розуміти принципи та підходи кіберзловмисників. Національна академія СБУ презентувала міжвідомчу освітню платформу для представників сектору безпеки та оборони, на якій, серед іншого, можна буде пройти курси захисту об'єктів критичної інфраструктури та протидії злочинам із використанням віртуальних активів. CERT-UA оприлюднила інструкцію щодо встановлення двоетапної аутентифікації для деяких месенджерів та інформаційних систем, а Кіберполіція запустила новий проєкт «Кібер Брама» для підвищення рівня кібергігієни українців.

Різко зросла активність китайських хакерів та поглибився аналіз їх діяльності з боку урядів західних країн. З'являються все нові повідомлення про кампанію кібершпигунства проти членів Міжпарламентського альянсу щодо Китаю – стало відомо, що ще однією жертвою китайських хакерів стала Голова парламентського комітету закордонних справ Бельгії. А в контексті американських виборів китайські хакери використовують штучний інтелект для розпалювання соціальної напруги в США. Зі свого боку КНР також трансформує свої кіберсили, створивши в цьому місяці Сили інформаційної підтримки. Попри ці зростаючі загрози, експерти вказують на те, що кількість пристроїв китайського виробництва в мережах США зросла протягом останнього року – до 300 000, що на 40% більше ніж минулого року (185 000).

Європейський Союз здійснює заходи адаптації до нового, більш динамічного ландшафту кіберзагроз. Зокрема, ЄС розробляє Закон про космос, що включатиме питання кібербезпеки – це особливо актуально на фоні зростаючих зусиль державних та приватних компаній з освоєння космічного простору (в тому числі через виведення супутникових систем на орбіту). Також ЄС поступово готується до загального впровадження постквантової криптографії аби не допустити нових кіберзагроз – для цього Єврокомісія випустила рекомендації для членів ЄС, які прямо вказують їм на необхідність розробки відповідних дорожніх карт. Зі свого боку Німеччина для швидшого реагування на нові загрози планує створити окремий рід військ – кіберсили.

Правоохоронці продовжують вдалі кібероперації проти інфраструктури кіберзловмисників. У квітні британська поліція зупинила діяльність LabHost, яка надавала послуги PaaS. Водночас довготривалий ефект від цих операцій викликає дискусії. Так, експерти Trellix виявили, що інфраструктура начебто розгромленого угрупування LockBit активно відновлюється і починає функціонувати.

Інфраструктура ПЗ з відкритим кодом, що базується на використанні відкритих бібліотек, у квітні могла стикнутись з глобальною загрозою, пов'язаною зі складною та добре підготовленою спробою компрометації бібліотеки XZ Utils невідомими злочинцями. Загроза була виявлена випадково співробітником Microsoft. Цей інцидент знову актуалізував питання безпечності використання open source продуктів та зміни підходів в цій сфері на користь більшої безпеки застосунків. CISA в цьому контексті актуалізувала свої ініціативи щодо Самітів для розробників ПЗ з відкритим кодом та впровадження secure by design.

російські хакери продовжують атакувати союзників України (не лише атакуючи локальні муніципальні системи в США, але і запускаючи нові бекдори під час атак у Східній Європі). Водночас Україна активно наносить контрудари. Наприклад, це успішна операція проукраїнського хакерського угрупування Blackjack, яке атакувало інфраструктуру російського «Москолектору».

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

ДЕЙВА ЛЮБЕРА ПРИЗНАЧЕНО ДИРЕКТОРОМ З КІБЕРБЕЗПЕКИ АГЕНТСТВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ США

З 1 квітня Дейв Любер призначений новим директором з кібербезпеки Агентства національної безпеки (АНБ) США. Він має понад 37 років досвіду роботи в системі АНБ, обіймаючи найрізноманітніші посади, в тому числі заступника директора з кібербезпеки АНБ та виконавчого директора Кіберкомандування США.

МІНІСТЕРСТВО ОБОРОНИ США СТВОРИЛО ОФІС З КІБЕРПОЛІТИКИ

1 квітня Пентагон оголосив про створення офісу помічника міністра оборони з кіберполітики. Обов'язки офісу включатимуть:

- розробку та нагляд за впровадженням кіберполітики та стратегії;
- затвердження бюджету операцій у кіберпросторі та координація з кіберкомандуванням;
- розробку керівництв для приватного сектору.

Офіс має надати всю необхідну допомогу новопризначеному першому помічнику міністра оборони з питань кіберполітики Майклу Салмайеру.

CISA СТВОРИЛА ВЕБСТОРІНКУ ДЛЯ СПІЛЬНОТ ВИСОКОГО РИЗИКУ

2 квітня CISA запустила нову вебсторінку, спрямовану на посилення кібербезпеки для спільнот з високим рівнем ризику (CISA включає в такі спільноти активістів, журналістів, правозахисників, науковців та інших співробітників, пов'язаних з організаціями громадянського суспільства). Ініціатива є частиною JCDC та надає доступ до низки важливих ресурсів:

- Project Upskill (покращення кібергігієни за допомогою простих кроків);
- доступ до місцевих волонтерських програм з кібербезпеки;
- набори інструментів і послуг з кібербезпеки.

Ці зусилля мають допомогти захистити від кіберзагроз організації, що просувають демократію та права людини.

НІМЕЧЧИНА СТВОРИТЬ НОВИЙ РІД ВІЙСЬК – КІБЕРВІЙСЬКА

4 квітня видання Politico повідомило, що Німеччина планує створити новий рід військ у рамках ініціативи міністра оборони Бориса Пісторіуса щодо оновлення збройних сил країни задля збільшення їх здатності до ведення війни. Нова німецька армія буде організована у чотири види: сухопутні війська, військово-морський флот і військово-повітряні сили, а також новий рід військ у кібер- та інформаційному просторі. Також будуть оперативні та допоміжні командування. Кібервідділ відповідатиме за боротьбу з гібридними загрозами, а також за виконання тактичних завдань, таких як РЕБ.

ANSSI ОГОЛОСИЛО КОНКУРС НА ПРОЄКТИ З КІБЕРБЕЗПЕКИ В РАМКАХ ПРОГРАМИ FRANCE 2030

4 квітня ANSSI оголосило про те, що у рамках плану «Франція 2030» планує підтримати проєкти зміцнення цифрової безпеки. Передбачається 3 вектори підтримки:

- інноваційні проєкти (створення повністю нових продуктів чи створення нового функціоналу для наявних);
- проєкти місцевих ініціатив (надання місцевим органам влади допомоги з розгортанням кібербезпекових рішень або придбання базових рішень кібербезпеки);
- проєкти розгортання «фундаменту» (проєкти кібердопомоги для місцевої влади, яка лише починає процес впровадження заходів кібербезпеки).

Загальний бюджет програми невідомий.

МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я США ПОПЕРЕДЖАЄ ЛІКАРНІ ПРО НАПАД ХАКЕРІВ НА СЛУЖБИ ПІДТРИМКИ ІТ

6 квітня Міністерство охорони здоров'я та соціальних служб США (HHS) випустило попередження про те, що хакери використовують тактику соціальної інженерії для атаки на служби підтримки ІТ у секторі охорони здоров'я та громадського здоров'я (HPH). Ці тактики включають видавання себе за співробітників фінансового відділу, надання вкрадених даних для підтвердження ідентифікаційної інформації та переконання персоналу служби підтримки зареєструвати нові пристрої для багатофакторної автентифікації під контролем зловмисника. Отримавши доступ, зловмисники перенаправляють банківські транзакції та законні платежі на контрольовані зловмисниками рахунки.

Подібна тактика спостерігалася в інцидентах, приписуваних кіберзлочинній групі Scattered Spider, відомої фішинговими атаками та кампаніями програм-вимагачів. Щоб пом'якшити такі атаки, організаціям рекомендується запроваджувати протоколи перевірки, відстежувати підозрілі дії та проводити навчання персоналу служби підтримки розпізнаванню методів соціальної інженерії.

СЕКРЕТНІ КІБЕРСИЛИ США У 2023 РОЦІ РОЗГОРТАЛИ 22 РАЗИ ДЛЯ ДОПОМОГИ УРЯДАМ ІНШИХ КРАЇН

У письмовому свідченні, яке було представлено на слуханнях Комітету зі Збройних Сил Сенату США у середу, 10 квітня, генерал Тімоті Д. Хо, командувач Кіберсил США, зазначив, що Кібербезпекова національна місійна група Кіберсил США виконала 22 кампанії Hunt Forward у 2023 році. Загалом ці сили було застосовано 55 разів з моменту їх піднесення до статусу Об'єднаного бойового командування у 2018 році. Місії Hunt Forward виконуються за запитом іноземних урядів і не завжди розголошуються. Вони є частиною стратегії постійного залучення, спрямованої на підтримку постійного контакту з противниками та забезпечення можливості проактивних дій (на відміну від реактивних).

ЄВРОКОМІСІЯ ОПУБЛІКУВАЛА РЕКОМЕНДАЦІЇ ПЕРЕХОДУ ДО ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ

11 квітня Європейська комісія оприлюднила Рекомендації щодо скоординованої імплементації дорожньої карти переходу до постквантової криптографії. Єврокомісія сподівається, що ці рекомендації заохотять держави-члени розробити комплексні стратегії для впровадження постквантової криптографії. Стратегія повинна визначати чіткі цілі, етапи та часові рамки впровадження постквантової криптографії. Це має призвести до розгортання в ЄС технологій постквантової криптографії в системах державного управління та критичних інфраструктурах за допомогою гібридних схем, які можуть поєднувати постквантову криптографію з існуючими криптографічними підходами або квантовим розподілом ключів.

CISA ПРОВЕЛА НАВЧАННЯ З КІБЕРБЕЗПЕКИ ДЛЯ КЕРІВНИКІВ ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДІВ ШТАТУ АЙДАХО

15 квітня керівники вищих навчальних закладів штату Айдахо взяли участь у навчаннях з кібербезпеки під керівництвом CISA. Мета навчань – навчитися протистояти атакам зловмисників за допомогою реальних сценаріїв. Специфічним аспектом саме цих навчань стало залучення до них не IT-персоналу організацій, а керівників. Це підкреслило важливість прийняття стратегічних рішень в умовах кіберкризових ситуацій.

РІЧАРД ХОРН СТАНЕ НОВИМ ГЕНЕРАЛЬНИМ ДИРЕКТОРОМ БРИТАНСЬКОГО NCSC

19 квітня Національний центр кібербезпеки (NCSC) Великобританії оголосив, що Річард Хорн стане його новим головним виконавчим директором (CEO) вже восени 2024 року. Наразі він працює у PwC UK, де очолює практику кібербезпеки. До приходу у PwC Хорн був керуючим директором із кібербезпеки Barclays PLC, від імені якої допомагав Кабінету Міністрів у 2011 році сформувати та запровадити першу урядову стратегію кібербезпеки. Хорн має ступінь доктора філософії з математики Royal Holloway (Університет Лондону).

CISA ОГОЛОСИЛА ПЕРЕМОЖЦІВ 5-ГО ЩОРІЧНОГО КОНКУРСУ З КІБЕРБЕЗПЕКИ НА КУБОК ПРЕЗИДЕНТА США

19 квітня 2024 року CISA оголосила переможців 5-го щорічного конкурсу з кібербезпеки на Кубок Президента США. Цього року команда-переможець Artificially Intelligent складалася з представників Міністерства оборони, армії США та військово-повітряних сил США. В індивідуальних заліках перемогли майор армії США та сержант штабу Корпусу морської піхоти США. Переможці будуть запрошені на церемонію нагородження в Білому домі на знак вдячності за їхні досягнення.

ЄС ГОТУЄ ЗАКОН ПРО КОСМОС, ЩО ВКЛЮЧАТИМЕ ПИТАННЯ КІБЕРБЕЗПЕКИ

24 квітня керівник відділу інновацій та NewSpace Єврокомісії Гільйом де ла Броссе озвучив деякі деталі майбутнього Закону ЄС про космос (це робоча назва – наразі невідомо яким саме типом нормативного акту буде впроваджено цей документ). Основною ідеєю Закону стане визнання космічної інфраструктури критичною, а в частині кібербезпеки документ буде зосереджений на кібербезпеці by design, посиленні безпеки ланцюжка постачання космічної галузі та застосуванні заходів кібербезпеки пропорційно до того, наскільки критичними вважаються певні продукти. Також за словами Броссе, компанії, які працюють у сфері космічних технологій, повинні будуть запобігати, виявляти і захищатися від кіберінцидентів.

В РАМКАХ НАЙБІЛЬШОЇ ЗА ОСТАННІ 9 РОКІВ ВІЙСЬКОВОЇ РЕСТРУКТУРИЗАЦІЇ КИТАЙ ДОДАЄ ІНФОРМАЦІЙНІ, КІБЕРБЕЗПЕКОВІ ТА КОСМІЧНІ ПІДРОЗДІЛИ

22 квітня видання NIKKEI Asia повідомило, що Китай провів суттєву військову реорганізацію, розділивши старі Сили стратегічної підтримки на три нові незалежні підрозділи: Сили інформаційної підтримки, Космічні сили та Кіберсили. Президент Сі Цзіньпін підкреслив важливість Сил інформаційної підтримки у зборі та аналізі інформації, побудові комунікаційних мереж і захисті критично важливих систем. Ці зміни відображають націленість Китаю на модернізацію свого військового потенціалу, зокрема в кіберпросторі та космічному просторі, згідно з вказівками президента.

Реорганізація має на меті підвищити спеціалізацію та ефективність кожного підрозділу і безпосередньо контролюється Центральною військовою комісією. Цей крок став наступним після реформ 2015 року, спрямованих на модернізацію Народно-визвольної армії. Нові Сили стали третім елементом (на додачу до вже двох раніше створених Сил кіберпростору та Аерокосмічних сил), які будуть відповідати за «координовану розробку та застосування мережевих інформаційних систем».

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

CCDCOE ПРОВЕЛО ЧЕРГОВІ НАВЧАННЯ LOCKED SHIELDS 2024

У квітні 2024 року Центр передового досвіду з кібербезпеки НАТО (CCDCOE) провів щорічні кібернавчання Locked Shields 2024. Цього року до навчань було залучено 4000 експертів із понад 40 для протидії симуляції атаки на критичну інфраструктуру вигаданої країни.

АВСТРАЛІЯ ТА ТАЙВАНЬ ПОСИЛЮЮТЬ СПІВПРАЦЮ У СФЕРІ КІБЕРБЕЗПЕКИ

8 квітня австралійський депутат Ендрю Уоллес (заступник голови Об'єднаного парламентського комітету з питань розвідки та безпеки Австралії) зустрівся з президентом Цай Ін Вень, зазначивши, що обидві сторони зацікавлені в підтримці регіональної стабільності. Сторони вже співпрацюють над ініціативами у сфері кібербезпеки для захисту критично важливої інфраструктури та важливих цифрових мереж, але планують розширити її в частині обміну інформацією.

В РАМКАХ ГЛОБАЛЬНОЇ ПОЛІЦЕЙСЬКОЇ ОПЕРАЦІЇ ПРИПИНЕНО РОБОТУ ФІШИНГОВОГО СЕРВІСУ LABHOST

18 квітня близько 37 осіб було заарештовано в рамках міжнародної операції проти кіберзлочинного сервісу під назвою LabHost, який використовували злочинці для викрадення особистих даних жертв по всьому світу.
LabHost, який називають одним із найбільших постачальників фішингових послуг (PhaaS), пропонував фішингові сторінки, націлені на банки, високопоставлені організації та інших постачальників послуг, розташованих переважно в Канаді, США та Великобританії.

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

НЕЗАЛЕЖНИЙ ДОСЛІДНИК БЕЗПЕКИ ВИЯВИВ ПРИХОВАНИЙ БЕКДОР У БІБЛІОТЕЦІ З ВІДКРИТИМ КОДОМ XZ UTILS, ЯКИЙ МІГ УРАЗИТИ СИСТЕМИ ПІД УПРАВЛІННЯМ DEBIAN ТА RED HAT LINUX

1 квітня співробітник Microsoft та дослідник безпеки Андрес Фройнд виявив незвичну активність у бібліотеці з відкритим кодом XZ Utils. Як стало пізніше відомо, невідомі особи взяли під контроль проєкт з підтримки XZ Utils (забравши його в основного розробника), а потім витратили значний час та зусилля аби повільно вбудувати бекдор в бібліотеку так, аби він не виявлявся штатними засобами безпеки. Бекдор мав потрапити в усі комп'ютери та системи, які використовують його у своїй діяльності, під час одного з оновлень. У випадку вдалої реалізації під ударом опинились би мільйони систем і атака могла б стати найбільш вдалою supply chain attack в історії. Проблема вкотре поставила питання про необхідність впровадження більш жорстких методів контролю за сторонніми ПЗ та впровадження secure by design.

ЗІРВАНИЙ ЗЛОМ ЛАНЦЮГА ПОСТАЧАННЯ ВИКЛИКАВ ТРИВОГУ У ВАШИНГТОНІ

Як 1 квітня пише видання Politico, виявлення зловмисного коду, прихованого в інструменті стиснення даних з відкритим кодом Xz, викликало занепокоєння щодо безпеки ланцюжка постачання із відкритим кодом і потенційної можливості його використання з боку держав. Інцидент, пов'язаний з користувачем GitHub, який завоював довіру, а потім скористався нею, підкреслює вразливість екосистем з відкритим кодом до внутрішніх загроз.

Поки тривають розслідування можливої участі держав, експерти порівнюють масштаб атаки з великими російськими зломами, такими як шпигунська кампанія SolarWinds. Ця подія підкреслює необхідність переоцінки безпеки програмного забезпечення з відкритим кодом, яке часто покладається на волонтерську підтримку та може бути вразливим до експлуатації через свою критичну роль у цифровій економіці.

Як попереджала компанія CISSecurity, вразливість у XZ Utils може дозволити віддалене виконання коду. Компанія Microsoft видала пояснення щодо бекдора XZ Utils.

AT&T ПІДТВЕРДЖУЄ АВТЕНТИЧНІСТЬ ВИТОКУ ІНФОРМАЦІЇ ПРО 73 МІЛЬЙОНИ ЛЮДЕЙ

1 квітня AT&T підтвердила, що набір даних щодо 73 мільйонів її поточних і колишніх клієнтів є легітимних майже через два тижні після того, як хакер виклав його на кримінальному ринку у даркнет. У пресрелізі телеком гігант заявив, що набір даних, схоже, датується 2019 роком, або раніше, і стосується приблизно 7,6 мільйона поточних власників облікових записів AT&T і приблизно 65,4 мільйона колишніх клієнтів.

Це порушення є критичним, оскільки містить дуже конфіденційну інформацію, як-от номери соціального страхування, імена та адреси електронної пошти тощо. Джерело витоку даних досі залишається невизначеним, що ускладнює виявлення та усунення порушень. AT&T ще не з'ясувала, чи сталося порушення через її власні системи чи постачальника.

DHS ЗВИНУВАЧУЄ «КАСКАД ЗБОЇВ У СИСТЕМІ БЕЗПЕКИ В MICROSOFT» У ЗЛАМІ КИТАЄМ УРЯДУ США

Як 3 квітня повідомило видання The Record, компанія Microsoft досі не має повного розуміння того, яким чином, вірогідно, урядові хакери Китаю зламали її системи та отримали доступ до електронних листів високопоставлених урядовців США. Про це йдеться в огляді Міністерства внутрішньої безпеки, опублікованому на початку квітня. У 34-сторінковому документі, підготовленому Радою з огляду кібербезпеки (CSRB), офіційні особи США дійшли висновку, що китайські хакери, відомі як Storm-0558, змогли досягти успіху «через каскад збоїв у системі безпеки в Microsoft».

Відсутність прозорості та запізніле реагування Microsoft щодо виправлення неточних заяв про злам та надання необхідних даних слідчим вказує на ділову культуру компанії, яка викликає занепокоєння, адже підриває безпеку та управління ризиками. Це служить суворим нагадуванням про те, що великі технологічні компанії повинні віддавати перевагу довірі клієнтів і захисту даних, а не намаганню зменшити збитки своєї корпорації.

IVANTI ОБІЦЯЄ ТРАНСФОРМУВАТИ СВОЮ ОПЕРАЦІЙНУ МОДЕЛЬ БЕЗПЕКИ ТА ВИЯВЛЯЄ НОВІ ВРАЗЛИВОСТІ

4 квітня Ivanti випустила виправлення для нових вразливостей DoS, які впливають на Ivanti Connect Secure та Ivanti Policy Secure, деякі з вразливостей можуть призвести до виконання довільного коду або розкриття інформації. У всіх підтримуваних версіях Ivanti Connect Secure та Ivanti Policy Secure було виявлено та виправлено чотири вразливості. Водночас дослідники виявили кілька китайських хакерських груп, які використовують недоліки безпеки Ivanti.

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ США РОЗСЛІДУЄ ЙМОВІРНУ КРАДІЖКУ УРЯДОВИХ ДАНИХ

3 квітня видання BleepingComputer повідомило, що Державний департамент США розслідує ймовірну крадіжку секретної інформації в урядового підрядника зі штату Вірджинія. Зловмисник, відомий як IntelBroker, опублікував на BreachForums заяву про викрадення «секретної інформації та комунікацій між Five Eyes, 14 Eyes і союзниками США». Зловмисник також стверджує, що володіє «повними іменами, електронними адресами, номерами офісів і особистими номерами мобільних телефонів урядовців, військових і співробітників Пентагону». Представник Державного департаменту сказав, що Держдепартамент зараз проводить розслідування. З міркувань безпеки він відмовився надавати подробиці.

НОВА ФІШИНГОВА КАМПАНІЯ НАЦІЛЕНА НА НАФТОГАЗОВИЙ СЕКТОР ЗА ДОПОМОГОЮ ВДОСКОНАЛЕНОГО ЗЛОВМИСНОГО ПЗ ДЛЯ КРАДІЖКИ ДАНИХ

Оновлена версія зловмисного програмного забезпечення під назвою Rhadamanthys для крадіжки інформації використовується у фішингових кампаніях, націлених на нафтогазовий сектор. Ця кампанія з'явилася через кілька днів після ліквідації правоохоронними органами групи програм-вимагачів LockBit. Хоча це може бути випадковістю, у серпні 2023 року Trend Micro показала варіант Rhadamanthys, який постачався в комплекті з витоком корисного навантаження LockBit, а також зловмисним програмним забезпеченням для кліпера та майнером криптовалюти.

КІБЕРЗЛОЧИННА ГРУПА MEDUSA ВЗЯЛА НА СЕБЕ ВІДПОВІДАЛЬНІСТЬ ЗА ЧЕРГОВУ АТАКУ НА МУНІЦИПАЛІТЕТ США

9 квітня видання The Record повідомило, що група програм-вимагачів Medusa взяла на себе відповідальність за атаку на державну установу в Техасі. Оцінювальний відділ округу Таррант, який визначає вартість майна для цілей оподаткування в районі Форт-Ворт, підтвердив, що став жертвою атаки програм-вимагачів двома тижнями раніше. Окрім інциденту в окрузі Таррант, група Medusa нещодавно атакувала уряд округу Іллінойс на кордоні з Айовою. Вона вперше з'явилася у 2023 році, і список її жертв швидко зріс, охоплюючи різні сектори та регіони від США до Африки.

ENISA ОНОВИЛА ІНСТРУМЕНТАРІЙ AR-IN-A-BOX ДЛЯ ПІДВИЩЕННЯ КУЛЬТУРИ КІБЕРБЕЗПЕКИ В ОРГАНІЗАЦІЯХ

10 квітня ENISA оновила свій інструментарій «Підвищення обізнаності в коробці» (AR-in-a-BOX) для підвищення культури кібербезпеки в організаціях. Нова версія містить елементи ігрового дизайну для кращого залучення учасників та новий посібник з розробки планів комунікації в умовах кіберкризи. Інструментарій був успішно протестований Управлінням цифрової безпеки Кіпру та Кіпрським національним координаційним центром. AR-in-a-Box дозволяє фахівцям малих і середніх (МСП) підприємств, а також великих підприємств та державних органів покращити свої знання щодо методів кібербезпеки.

КОМПАНІЯ З БІЗНЕС-АНАЛІТИКИ SISENSE БУЛА ВДАЛО АТАКОВАНА ХАКЕРАМИ

12 квітня з'явились повідомлення про те, що компанія Sisense була піддана масштабному зламу з численними втратами даних клієнтів. Sisense спеціалізується на послугах бізнес-аналізу для підприємств різного рівня, надаючи клієнтам можливість завантажити їх дані на платформу Sisense та піддати їх аналізу засобами кампанії. Хоча представники Sisense не поширюють точні дані про втрати інформації, однак окремі безпекові сайти підкреслюють, що схоже атака дозволила хакерам викрасти терабайти даних клієнтів, які включають мільйони паролів облікових записів, дані електронної пошти, сертифікати SSL. Також за деякими даними хакерам вдалось отримати доступ до сховища коду GitLab Sisense, яке містило облікові дані для облікового запису Sisense Amazon S3.

СПРОБА ЗЛОМУ НЬЮ-ЙОРКА ПРОДОВЖУЄ ХВИЛЮ КІБЕРАТАК НА МУНІЦИПАЛЬНІ ОРГАНИ ВЛАДИ

5 квітня видання The Record написало, що у 2024 році вже десятки місцевих органів влади постраждали від програм-вимагачів і кібератак, що обмежило надання послуг мільйонам людей у Сполучених Штатах. Останній резонансний інцидент стосується Нью-Йорка, який був змушений вимкнути міський вебсайт із заробітною платою та видалити його з загального огляду після фішингового інциденту.

Кіберзлочинці демонструють глибоке розуміння заходів безпеки, таких як багатофакторна автентифікація, і використовують ці знання для створення ефективних фішингових атак. Створюючи автентичні несанкціоновані сайти, зловмисники обманом змушують співробітників розкрити конфіденційні облікові дані, що робить компанії більш уразливими до злому.

ВИЯВЛЕНА НОВА ТЕХНІКА ОБМАНУ РОЗРОБНИКІВ ПІД ЧАС АТАКИ НА ЛАНЦЮГ ПОСТАЧАННЯ З ВІДКРИТИМ КОДОМ – CHEKMARKS

Компанія Chekmarks виявила, що під час нещодавньої кампанії атак кіберзлочинці вміло маніпулюють функціями пошуку GitHub і використовують ретельно створені сховища для розповсюдження шкідливого програмного забезпечення. Звіт, опублікований компанією 10 квітня, детально розповідає про те, як відбувається маніпуляція. Про ще один спосіб розповсюдження зловмисного ПЗ через GitHub повідомила компанія MCAfee.

АНБ США ВИДАЄ ВКАЗІВКИ ЩОДО ВПРОВАДЖЕННЯ ZERO TRUST

9 квітня Агентство національної безпеки США випустило нові рекомендації щодо посилення безпеки даних через запровадження принципів архітектури «нульової довіри» (Zero Trust). Інформаційний бюлетень з кібербезпеки «Просування архітектури нульової довіри на всіх рівнях захисту даних» пропонує низку стратегій як принципи Zero Trust можуть бути запроваджені на практиці. Це включає: забезпечення лише авторизованого доступу до даних, шифрування, маркування даних та використання інструментів управління правами доступу до даних.

ГРУПА ОНЛАЙН ВИМАГАЧІВ ПОЧИНАЄ ЗЛИВАТИ ЙМОВІРНО ВКРАДЕНІ ДАНІ CHANGE HEALTHCARE

15 квітня видання BleepingComputer повідомило, що група здирників RansomHub почала зливати дані, які, за її словами, були вкрадені під час атаки ALPHV/Blackcat на Change Healthcare у лютому. Група публікує скріншоти, які містять «угоди про обмін даними між Change Healthcare і постачальниками страхових послуг. Інші документи містять бухгалтерські дані, включаючи звіти про старіння, звіти про страхові виплати та іншу фінансову інформацію. Набір даних також містить «інформацію про пацієнта, включаючи суми заборгованості та рахунки за надані послуги з догляду за пацієнтами».

Change Healthcare не підтвердила, що після атаки вона заплатила викуп у розмірі 22 мільйонів доларів або що дані RansomHub є законними. За повідомленням The Record, атака програм-вимагачів коштувала UnitedHealth 872 мільйони доларів. Очікується, що загальна сума перевищить 1 мільярд доларів.

АНБ США ОПУБЛІКУВАЛО РЕКОМЕНДАЦІЇ ЩОДО ПОСИЛЕННЯ БЕЗПЕКИ СИСТЕМ ШІ

15 квітня Агентство національної безпеки (АНБ) США опублікувало новий інформаційний бюлетень з кібербезпеки під назвою «Безпечне розгортання систем штучного інтелекту». Цей посібник, розроблений у співпраці з кількома міжнародними агентствами з кібербезпеки, зосереджується на найкращих практиках розгортання безпечних і стійких систем ШІ, з акцентом на діяльність суб'єктів системи національної безпеки та оборонно-промислової бази.

ПІВНІЧНОКОРЕЙСЬКА APT ГРУПА TA427 АКТИВНО ВИКОРИСТОВУЄ DMARC ДЛЯ ПРОВЕДЕННЯ КІБЕРШПИГУНСЬКИХ МІСІЙ

16 квітня фахівці Proofpoint оприлюднили свій аналіз діяльності північнокорейської APT групи TA427 (також відома як APT43, THALLIUM та інші), яка спеціалізується на роботі з західними експертами, журналістами та посадовцями. Мета TA427 – зібрати інформацію про позиції цих експертів або їх установ про Північну Корею та закріпитись в інформаційних системах дослідницьких організацій. Для цього зловмисники використовують відточені техніки соціального інжинірингу (імітуючи з себе журналістів та експертів, організаторів наукових заходів тощо), а також проблеми у налаштуваннях DMARC – відкритому протоколі автентифікації електронної пошти, який забезпечує захист каналу пошти на рівні домену. Деякі особливості його налаштування дозволяють листам TA427 обходити політики безпеки організацій.

CISA, ФБР І ODNI ВИПУСКАЮТЬ РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ ВИБОРЧОЇ ІНФРАСТРУКТУРИ ВІД ІНОЗЕМНИХ ОПЕРАЦІЙ ЗЛОВМИСНОГО ВПЛИВУ

17 квітня CISA спільно з ФБР та ODNI (Офіс директора національної розвідки) випустили посібник із захисту виборчої інфраструктури від іноземних операцій зловмисного впливу. У цьому посібнику детально описано тактику, яка використовується для зриву виборів у США, з акцентом на використанні штучного інтелекту для поширення дезінформації. Посібник включає опис наступних тактик:

- використання псевдомедіа;
- створення фейкових аудіо повідомлень відомих особистостей;
- операції впливу за допомогою кібероперацій;
- створення фальшивих «доказів» кібервтручання;
- проплачені повідомлення для здійснення впливу;
- залучення соціальних платформ.

РЕЗЕРВ БЕРЕГОВОЇ ОХОРОНИ США ВИПАДКОВО РОЗКРИВ ОСОБИСТІ ДАНІ ПОНАД ТИСЯЧІ СВОЇХ ЧЛЕНІВ

18 квітня Резерв берегової охорони США повідомив громадськість про те, що у січні 2024 року було виявлено витік персональних даних, який торкнувся 10 700 членів організації. Наразі мова не йде про кібератаку, а про неналежне використання доступу до такої інформації членів організації. Їх дані були надіслані 85 членам організації, однак потенційно могли стати відомі зловмисникам. Розкриті дані містили домашні адреси, імена та ідентифікаційні номери співробітників.

MITRE СТИКНУЛАСЬ З КІБЕРАТАКОЮ З БОКУ ІНОЗЕМНОЇ КРАЇНИ

19 квітня MITRE повідомила, що вона стикнулась з кібератакою з боку іноземної країни. Підозріла активність була виявлена в мережевому середовищі експериментів, досліджень і віртуалізації (NERVE) – спільної мережі, яка використовується для досліджень, розробки та створення прототипів. Саме на її компрометацію були спрямовані зусилля іноземного актора, що швидше за все, підтримується іноземною країною. За попередніми даними MITRE немає жодних ознак того, що цей інцидент вплинув на основну корпоративну мережу або системи партнерів MITRE.

CISCO TALOS ВИЯВИВ ШПИГУНСЬКУ КАМПАНІЮ ARCANEDOOR, ЯКА НАЦІЛЕНА НА ПРИСТРОЇ ПЕРИМЕТРА МЕРЕЖ ВІД РІЗНИХ ПОСТАЧАЛЬНИКІВ

24 квітня фахівці Cisco Talos заявили, що виявили підвищену активність не атрибутованого державного зловмисного актора UAT4356 (або STORM-1849), що проводить шпигунську кампанію ArcaneDoor. Мета зловмисників – отримати доступ до пристроїв периметральної мережі, та, використовуючи їх, розгорнути операцію з кібершпигунства. UAT4356 розгорнув два бекдори як компоненти цієї кампанії – «Line Runner» та «Line Dancer» – які разом використовувалися для здійснення зловмисних дій, що включало модифікацію конфігурації пристроїв, розвідку, захоплення/виведення мережевого трафіку та потенційно переміщення зловмисників в мережі.

КОМПРОМЕТАЦІЯ БІЗНЕС-ЕЛЕКТРОННОЇ ПОШТИ (BEC) – НАЙПОШИРЕНІША ЗАГРОЗА ПЕРШОГО КВАРТАЛУ 2024 РОКУ

25 квітня фахівці Cisco Talos оприлюднили результати своїх спостережень за перший квартал 2024 року. За їх даними компрометація бізнес-електронної пошти (BEC) є абсолютним лідером (понад 50% всіх інцидентів) у спробах зловмисників отримати доступ до атакованих систем (майже у всіх випадках ці спроби реалізуються через фішинг). Наступні за небезпекою ransomware становлять лише 17% від всіх випадків.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

ГРУПА ЕКСПЕРТІВ CCDCOE ПІДГОТУЄ «ПОСІБНИК ІЗ ФОРМУВАННЯ НАЦІОНАЛЬНОЇ ПОЗИЦІЇ ЩОДО МІЖНАРОДНОГО ПРАВА В КІБЕРПРОСТОРІ»

Експерти з Університету Ексетера, Міністерства закордонних справ Естонії, Міністерства закордонних справ Японії та CCDCOE НАТО 28 травня офіційно розпочнуть роботу над документом «Посібник із формування національної позиції щодо міжнародного права в кіберпросторі: практичний посібник для держав». Проєкт базується на попередніх дослідженнях CCDCOE та Університеті Ексетера, а також на інструментарії Cyber Law Toolkit. Посібник має запропонувати набір рекомендацій для розробки національних або спільних позицій щодо міжнародного права.

ЩО МОЖНА ДІЗНАТИСЯ ПРО БЕЗПЕКУ ШІ ЗІ СПРОБИ ЗЛАМАТИ ЧАТБОТИ

Минулого літа понад 2000 учасників, у тому числі представники технологічних компаній, зібралися на велику хакерську конференцію в Лас-Вегасі, щоб перевірити потенційну шкоду чатботів зі ШІ за допомогою публічних вправ «red teaming», наголошуючи на ризиках неправильного використання та небажаних наслідків у сценаріях з реального життя. Навчання, в яких брали участь генеративні ШІ моделі від восьми компаній, виявили випадки дезінформації, упередженості та вразливості кібербезпеки, наголошуючи на необхідності надійних заходів безпеки ШІ. Такі навчання стають дедалі важливішими на тлі глобальних зусиль щодо регулювання технології ШІ та забезпечення її безпечного та надійного використання, хоча вони лише поверхнево розкривають потенційну шкоду, пов'язану зі штучним інтелектом, підкреслюючи необхідність постійних досліджень і спільних зусиль для ефективного подолання наслідків для суспільства.

ВИРОБНИКИ АВТОМОБІЛІВ І ФЕДЕРАЛЬНА КОМІСІЯ ЗВ'ЯЗКУ США ГОТУЮТЬСЯ ОБГОВОРЮВАТИ ПОТЕНЦІЙНІ ПРАВИЛА ДЛЯ ПІДКЛЮЧЕНИХ АВТОМОБІЛІВ

Виробники автомобілів і Федеральна комісія зі зв'язку (FCC) готуються до потенційної боротьби за те, чи слід регулювати підключені автомобілі як невеликі частини телекомунікаційної інфраструктури – рішення, яке матиме величезні наслідки для того, як транспортні засоби обробляють споживчі дані. У нещодавніх листах, отриманих Recorded Future News, автомобільні компанії відмовилися від запитів голови FCC Джесіки Розенворсел про те, чи повсякденні транспортні засоби настільки технологічно просунуті, що можуть підпадати під дію нових правил.

ПОЛІТЕХНІЧНИЙ ІНСТИТУТ РЕНССЕЛЕРА СТАВ ПЕРШИМ У СВІТІ УНІВЕРСИТЕТОМ, ЯКИЙ ОТРИМАВ КВАНТОВИЙ КОМП'ЮТЕР

5 квітня IBM і Rensselaer Polytechnic Institute перерізали стрічку першого квантового комп'ютера IBM, який буде встановлено в університетському містечку. Розробники сподіваються, що студенти та професори сприятимуть просуванню досліджень у цій сфері.

На сьогодні технологія квантових обчислень є надто «молодою» та дорогою для використання у повсякденному житті, а більшість досліджень планується присвятити базовим речам, як, наприклад, створення алгоритмів для таких комп'ютерів. Разом з тим, вона вважається революційною і різні країни роблять значні інвестиції. Наприклад, США розраховують на такі проєкти, як співпраця IBM-RPI, як на головний компонент своєї гри на майбутнє. Обидві установи є частиною Північно-східного регіонального центру оборонних технологій, який у вересні отримав 40 мільйонів доларів від Міністерства оборони через CHIPS and Science Act.

Згідно зі звітом Центру стратегічних і міжнародних досліджень, Китай також зробив великий ривок до квантової технології, і на його долю припадає половина з 30 мільярдів доларів, витрачених у всьому світі на цю технологію.

CISA ЗАПУСТИЛА НОВУ СИСТЕМУ АНАЛІЗУ ЗЛОВМИСНОГО ПЗ

10 квітня CISA представила систему Malware Next-Gen Analysis, спрямовану на автоматизацію аналізу нового шкідливого програмного забезпечення та посилення захисту від кіберзагроз. Система дозволяє зареєстрованим користувачам доменів .gov і .mil надсилати зразки шкідливого програмного забезпечення для аналізу. Це має сприяти своєчасному та ефективному реагуванню на кіберзагрози.

73% СПЕЦІАЛІСТІВ ІЗ БЕЗПЕКИ МАЛИХ ТА СЕРЕДНІХ ПІДПРИЄМСТВ НЕ РЕАГУЮТЬ НАВІТЬ НА КРИТИЧНІ СПОВІЩЕННЯ БЕЗПЕКИ

24 квітня компанія Coro оприлюднила результати свого дослідження щодо зв'язку між проблемами фахівців з кібербезпеки та обсягами їх робочих навантажень. Було опитано 500 осіб (з акцентом на МСП), які працюють у сфері кібербезпеки в компаніях від 200 до 2000 співробітників. Серед результатів – 73% фахівців із кібербезпеки МСП повідомили, що вони пропустили, проігнорували або не вжили заходів щодо навіть високопріоритетних попереджень безпеки. Двома основними причинами цього були брак персоналу та часові обмеження.

АВСТРАЛІЙСЬКІ БЕЗПЕКОВІ СТРУКТУРИ ХОЧУТЬ ВПРОВАДЖЕННЯ «ПІДЗВІТНОГО ШИФРУВАННЯ»

Під час виступу 25 квітня у Національному пресклубі Австралії Генеральний директор головного розвідувального агентства Австралії Майк Берджесс та комісар Федеральної поліції Австралії Ріс Кершоу наголосили, що безпекові органи потребують «підзвітного шифрування» (фактично – надання технологічними компаніями правоохоронним органам ключів шифрування) аби ліпше боротися з терористами та злочинцями. На їхню думку, наскрізне шифрування та брак співпраці з боку техгігантів створюють для злочинців «безпечні кімнати» де вони можуть планувати свої злочини.

NIST СТИКАЄТЬСЯ З ПРОБЛЕМАМИ ДОСЛІДЖЕНЬ У СФЕРІ ШІ ЧЕРЕЗ СЛАБКЕ ФІНАНСУВАННЯ

25 квітня оглядач Security Intelligence Джош Надо провів огляд ситуації з проблемами функціонування NIST як ключової структури, що відповідає за стандартизацію нових сфери діяльності, як то ШІ. Він звертає увагу, що Уряд США покладає на NIST все нові обов'язки та задачі (як то розробку стандартів для розвитку ШІ), однак при цьому постійно скорочує фінансування. Сама будівля NIST (якій 125 років) перебуває у поганому стані (організації не вистачає ресурсів навіть на ремонт даху), а фінансування організації знову скорочено на 10%. Висновок Джоша Надо – NIST може виявитись неспроможною ефективно відреагувати на нові запити влади якщо не будуть вжиті заходи з поліпшення фінансування.

КИТАЙСЬКІ ХАКЕРИ ВИКОРИСТОВУЮТЬ ШТУЧНИЙ ІНТЕЛЕКТ ДЛЯ РОЗПАЛЮВАННЯ СОЦІАЛЬНОЇ НАПРУГИ В США – СТВЕРДЖУЄ MICROSOFT

Згідно з новими дослідженнями, в рамках пов'язаних з Пекіном операції впливу почалось використання генеративного штучного інтелекту для посилення суперечностей навколо внутрішніх проблем у таких місцях, як США та Тайвань. В таких кампаніях в основному використовували технологію для створення візуального контенту, призначеного для розпалювання конфлікту напередодні виборів, йдеться у звіті, опублікованому Microsoft 4 квітня.

FIVE EYES ОПУБЛІКУВАЛИ ДОКУМЕНТ ІЗ ІНСТРУКЦІЯМИ ЩОДО ШІ

Розвідувальні служби країн Five Eyes спільно опублікували документ з інструкціями щодо штучного інтелекту «Безпечне розгортання систем штучного інтелекту: найкращі практики розгортання безпечних і стійких систем штучного інтелекту». У документі зазначається, що «ці найкращі практики найбільше застосовні до організацій, які розгортають і експлуатують зовнішньо розроблені системи ШІ на власній території або в приватних хмарних середовищах, особливо в середовищах з високою загрозою та високою цінністю. Вони не стосуються організацій, які не розгортають системи ШІ самостійно, а замість цього використовують системи ШІ, розгорнуті іншими».

5. КРИТИЧНА ІНФРАСТРУКТУРА

ФЕДЕРАЛЬНА КОМІСІЯ ЗВ'ЯЗКУ ДОСЛІДИТЬ «СЕРЙОЗНІ» НЕДОЛІКИ В ІНФРАСТРУКТУРІ ТЕЛЕФОННОЇ МЕРЕЖІ

Як 1 квітня повідомило видання The Record, Федеральна комісія зв'язку вживає заходів для усунення значних недоліків у телекомунікаційних мережах, які можуть сприяти кіберзлочинності та шпигунству. Агентство досліджує, як уразливості в протоколах Signaling System № 7 (SS7) і Diameter, які спільно забезпечують передачу телефонних дзвінків і текстових повідомлень у мережах, можуть сприяти зламам, зокрема, розкриваючи місцеперебування споживачів зловмисним хакерам і шпигунам.

MANDIANT ПОВ'ЯЗУЄ АТАКИ НА ОТ З РОСІЙСЬКИМ ГРУ

У звіті, оприлюдненому 17 квітня, Mandiant пов'язує угруповання Sandworm, яке відстежує компанія як APT44, з декількома хактивістськими групами, які взяли на себе відповідальність за атаки на системи ОТ у США та ЄС, включаючи водопровідне підприємство в Техасі, станцію очищення стічних вод у Польщі та дамбу гідроелектростанції у Франції. Здається, що ці атаки не мали жодних серйозних наслідків, але дослідники відзначають, що «постійне просування та використання у вільному доступі руйнівних можливостей групи, ймовірно, знизило бар'єр входу для інших держав відтворювати та розвивати власні програми кібератак».

НЕВІДОМІ ХАКЕРИ РЕЗУЛЬТАТИВНО АТАКУВАЛИ КІЛЬКА ФРАНЦУЗЬКИХ МУНІЦИПАЛЬНИХ СЛУЖБ

12 квітня стало відомо, що неназвані хакери провели ряд успішних кібератак проти французьких муніципальних служб. Була порушена робота їх сайтів та сервісів. Атаковані були муніципалітети Монтуар-де-Бретань, Донж, Ла-Шапель-де-Маре та Порніш, Сонадев і Агентство сталого розвитку регіону Сен-Назер. Роботу сервісів було відновлено.

НІДЕРЛАНДСЬКИЙ ВИРОБНИК МІКРОСХЕМ NEXPERIA СТАВ ЖЕРТВОЮ КІБЕРАТАКИ

12 квітня китайський власник голландської компанії виробників мікросхем Nexperia повідомив, що штаб-квартира компанії була атакована хакерами, які отримали доступ до певних IT-серверів Nexperia в березні 2024 року. Наразі невідомо масштаби наслідків, однак за даними журналістів злочинці могли вкрасти сотні гігабайтів конфіденційної інформації, включно з комерційною таємницею, дизайном чіпів і даними про клієнтів, зокрема Apple, Huawei і SpaceX. Nexperia – колишній підрозділ Standard Products виробника мікросхем NXP, який був виділений у 2016 році та придбаний китайською компанією Wingtech у 2018 році. Він виробляє базові мікросхеми, транзистори та діоди.

ЗА ОЦІНКАМИ CHANGE HEALTHCARE КІБЕРАТАКА НА НЕЇ У ПЕРШОМУ КВАРТАЛІ 2024 РОКУ ЗАВДАЛА ШКОДИ 872 МЛН ДОЛАРІВ

16 квітня 2024 року UnitedHealth Group, материнська компанія Change Healthcare, повідомила у своїх результатах за перший квартал про негативний вплив у розмірі 872 млн доларів США від кібератаки, яка була здійснена на компанію у першому кварталі 2024 року. Ця оцінка не фінальна – компанія передбачає додаткові витрати, пов'язані з атакою. Крім того, навколо викупу у 22 мільйони доларів, який начебто сплатила компанія, спостерігається протиборство двох ransomware угрупувань – BlackCat/ALPHV та RansomHub – які, вочевидь, не поділили викуп.

UNITEDHEALTH ЗАЯВИЛА, ЩО ХАКЕРАМ ВДАЛОСЬ ВИКРАСТИ ВЕЛИКУ КІЛЬКІСТЬ ПЕРСОНАЛЬНИХ ДАНИХ АМЕРИКАНЦІВ

22 квітня UnitedHealth Group в межах продовження оцінки наслідків кібератаки на неї повідомила, що швидше за все хакерам вдалось викрасти велику кількість персональних даних американців. Компанія не заявляла, які саме дані були викрадені, але вони стосуються даних про здоров'я та особистої інформації. Також 19 квітня стало відомо, що Генеральний директор UnitedHealth Ендрю Вітті мав дати свідчення перед підкомітетом Палати представників США 1 травня щодо кібератаки проти його компанії. Свідчення мають на меті дати зрозуміти як цей інцидент вплинув на функціонування компанії (яка опрацьовує 50% всіх медичних претензій в США), а також на пацієнтів і постачальників. Свідчення були ініційовані Комітетом з питань енергетики та торгівлі.

ПРОМИСЛОВИЙ ПРОДУКТ SIEMENS МОЖЕ БУТИ ВРАЗЛИВИЙ ПРИ ВИКОРИСТАННІ ЗЛОВМИСНИКАМИ ВРАЗЛИВОСТІ БРАНДМАУЕРА PALO ALTO

23 квітня компанія Siemens оприлюднила заяву, в якій звертає увагу, що її продукт Ruggedcom APE1808, на якому налаштовано віртуальний брандмауер Palo Alto Networks (NGFW), може постраждати від використання вразливості CVE-2024-3400. Експлуатація вразливості дозволяє зловмиснику виконувати довільні команди з підвищеними привілеями на скомпрометованому брандмауері. Наразі дослідники безпеки відмічають, що вже є приклади експлуатації цієї вразливості, але не в контексті атак на продукт Siemens.

ПІВНІЧНОКОРЕЙСЬКІ ХАКЕРИ АТАКУВАЛИ ОБОРОННИХ ПІДРЯДНИКІВ ПІВДЕННОЇ КОРЕЇ

23 квітня поліція Південної Кореї повідомила, що основні північнокорейські хакерські угруповання протягом року здійснювали масштабну кібератаку проти південнокорейських оборонних компаній. Як наслідок, були зламані внутрішні мережі компаній і викрадено частину технічних даних. Хакери використовували як прямі методи атак, так і підрядників (supply chain attack) у своїх діях.

МЕДИЧНИЙ КОНГЛОМЕРАТ KAISER ПОВІДОМИВ ПРО ВИТІК ДАНИХ МІЛЬЙОНІВ КЛІЄНТІВ

25 квітня Американський медичний конгломерат Kaiser повідомив, що стався витік даних 13,4 мільйона персональних даних клієнтів. Наразі не повідомляється причина витоку та які саме дані були поширені. Kaiser Permanente, є одним із провідних постачальників медичних послуг у США.

6. АНАЛІТИЧНІ ОЦІНКИ

XZ UTILS: ВИКЛИКИ ДЛЯ ЕКОСИСТЕМИ ПРОГРАМ З ВІДКРИТИМ КОДОМ

12 квітня експерти CISA аналізують ситуацію з XZ Utils. Вони вказують, що CISA активно працює зі спільнотою розробників ПЗ з відкритим кодом аби пом'якшити можливі загрози. Як частину таких ініціатив CISA згадуються Перший саміт із безпеки програмного забезпечення з відкритим кодом (проведений у березні 2024), а також ініціативу Secure by Design.

ЗБИТКИ ЧЕРЕЗ ШАХРАЙСТВО, ПОВ'ЯЗАНЕ ІЗ ВИДАВАННЯМ СЕБЕ ЗА ІНШУ ОСОБУ, ПЕРЕВИЩУЮТЬ ОДИН МІЛЬЯРД ДОЛАРІВ НА РІК, ПОВІДОМЛЯЄ FTC

1 квітня, The Record пише про те, що згідно з федеральною статистикою, класичний тип шахрайства – коли шахрай видає себе за компанію чи державну установу – здається більш розповсюдженим, ніж будь-коли. Зараз таке шахрайство починається з текстового повідомлення чи електронного листа замість телефонного дзвінка. Шахрайство з видаванням себе за іншу особу, про яке повідомляється Федеральній торговій комісії, коштувало жертвам приблизно 1,1 мільярда доларів у 2023 році, що «більш ніж у три рази більше, ніж повідомляли споживачі у 2020 році».

Попри те, що традиційні шахрайські телефонні дзвінки є поширеним методом, Федеральна торгова комісія (FTC) у 2023 році помітила тенденцію, коли близько 40% зареєстрованих випадків шахрайства з видаванням себе за іншу особу починалися онлайн, наприклад, через текстові повідомлення чи електронну пошту.

КІЛЬКІСТЬ КИТАЙСЬКИХ ПРИСТРОЇВ У МЕРЕЖАХ США ЗРОСТАЄ

3 квітня кібербезпекова компанія Forescout оприлюднила дослідження, яке вказує на те, що кількість пристроїв китайського виробництва в мережах США зросла протягом останнього року – до 300 000, що на 40% більше ніж минулого року (185 000). Це становить близько 4% від загальної кількості з 7,5 мільйонів пристроїв, розташованих у США, які зараз підключені до корпоративних пристроїв Forescout. Приблизно 88% пристроїв китайського виробництва є IT-продуктами, за ними йдуть IoT (9%), OT (2%) та IoMT (1%). Компанія підкреслює, що це відбувається на фоні постійних спроб Уряду США обмежити вплив китайських виробників та профінансувати заходи з заміни такого обладнання.

КІБЕРБЕЗПЕКОВІ ВИДАТКИ БЮДЖЕТУ США НА 2025 РІК ЗОСЕРЕДЯТЬСЯ НА ЧОТИРЬОХ ПРІОРИТЕТАХ

У матеріалі від 8 квітня журналісти видання Security Intelligence аналізують бюджет США на 2025 рік та як саме Уряд США планує підтримати сферу кібербезпеки. Бюджет передбачає понад 13 мільярдів доларів США на потреби кібербезпеки (в бюджеті 2024 року – 12,7 млрд) для цивільних агенцій. До чотирьох пріоритетів відносяться:

- підтримка кіберрозслідувальних можливостей ФБР та контррозвідка в кіберсфері (це включає і створення нового відділ кіберзагроз у Міністерстві юстиції);
- захист від іноземних ворогів і захист федерального устрою (передусім – підвищення безпеки державних послуг та фінансування CISA);
- розвиток ШІ, його безпека та стійкість (включає видатки для Міністерства енергетики на розвиток ШІ для потреб енергетичної безпеки, національної безпеки та боротьбою зі зміни клімату);
- захист системи охорони здоров'я США від кіберзагроз.

ХАКЕРСЬКА ГРУПА TA547 ШВИДШЕ ЗА ВСЕ ПОЧАЛА ВИКОРИСТОВУВАТИ ІНСТРУМЕНТИ, ЩО СТВОРЕНІ ГЕНЕРАТИВНИМ ШІ

10 квітня кіберексперти з Proofpoint виявили діяльність групи TA547, що спрямували свої зусилля на німецькі організації. Зловмисники націлені на компрометацію електронної пошти організацій після чого в систему жертви доставляється зловмисне програмне забезпечення Rhadamanthys. Rhadamanthys це викрадач інформації, який використовується кількома кіберзлочинними групами. Однак TA547 додатково використовує сценарій PowerShell, який, як підозрюють дослідники, був створений великою мовною моделлю (LLM), такою як ChatGPT, Gemini, CoPilot тощо.

ДЕТАЛЬНИЙ АНАЛІЗ ШКІДЛИВИХ ПРОДУКТІВ WATERBEAR І DEUTERBEAR ВІД TRENDMICRO

11 квітня фахівці компанії TrendMicro представили докладний аналіз двох інструментів, які активно використовуються невідомою (але швидше за все пов'язаною з державою) зловмисною групою Earth Hundun / BlackTech – Waterbear і Deuterbear. Бекдор Waterbear (Deuterbear є його новою модифікацією) є складним інструментом із широким набором методів захисту від виявлення. Він містить в собі захист від «пісочниць» та загальних методів захисту від вірусів. На думку дослідників бекдори Waterbear/Deuterbear використовуються для кібершпигунських операцій, що спрямовані на технологічні компанії та державний сектор Азійсько-Тихоокеанського регіону.

КИТАЙСЬКА EARTH FREYBUG ВИКОРИСТОВУЄ UNAPIMON ДЛЯ ВІДКЛЮЧЕННЯ КРИТИЧНИХ API – TREND MICRO

Компанія Trend Micro опублікувала звіт про Earth Freybug, що є підрозділом пов'язаного з Китаєм загрозливого актора APT41. Зловмисник використовує зловмисне програмне забезпечення DLL під назвою «UNAPIMON», яке «застосовує методи ухилення від захисту, щоб запобігти моніторингу дочірніх процесів». Дослідники зазначають: «Унікальною та помітною особливістю цього зловмисного ПЗ є його простота та оригінальність. Використання існуючих технологій, таких як Microsoft Detours, показує, що будь-яку просту та готову бібліотеку можна використати зловмисно, якщо використовувати її творчо. Це також показало майстерність кодування та креативність автора зловмисного ПЗ. У типових сценаріях саме зловмисне програмне забезпечення виконує підключення. У цьому, випадку, одначе, все навпаки», – зазначили фахівці компанії.

ЯК ПОДОЛАТИ РОЗРИВ МІЖ IT ТА ЮРИДИЧНИМ ПЕРСОНАЛОМ ДЛЯ КРАЩОЇ БОРОТЬБИ З ВНУТРІШНІМИ РИЗИКАМИ

У статті для SC Media президент і генеральний директор компанії Code42 Джо Пейн пише про необхідність об'єднати зусилля співробітників відділу IT, безпеки та юристів, щоб захистити організації від внутрішніх загроз, серед яких різноманітні ризики від звільнених співробітників до випадкового розкриття даних. Попри існуючі заходи захисту даних, багато організацій все ще стикаються з їх витоком, що призводить до фінансових втрат і юридичних наслідків. Співпраця між командами IT, безпеки та юристів має вирішальне значення для розробки політик і дотримання норм. Три стратегії пом'якшення внутрішніх загроз включають своєчасне виявлення, забезпечення повної видимості операцій з файлами та впровадження постійного навчання персоналу. На думку автора, усунення розриву між командами IT, безпеки та юристів може покращити стратегії захисту даних.

ІНФРАСТРУКТУРА RANSOMWARE ГРУПИ LOCKBIT ПРОДОВЖУЄ ФУНКЦІОНУВАТИ

11 квітня експерти Центру передових досліджень Trellix повідомили, що вони спостерігають сплеск кіберактивності, пов'язаної з ransomware LockBit. Цей сплеск свідчить про те, що, попри «Операцію Cronos», яка була проведена у лютому 2024 року правоохоронними органами 11 країн, і яка була спрямована на демонтаж інфраструктури LockBit, операторам ransomware якимось чином вдалося вижити та залишитися на плаву. Ситуація погіршується спробами одразу декількох хакерських груп видавати себе за групу LockBit шляхом використання конструктору LockBit, який став доступний через витік у 2022 році. Загалом експерти Trellix вказують, що група LockBit активно відновлює свою діяльність та інфраструктуру, а отже успіх Операції Cronos був лише тимчасовим.

ЗНИЖЕННЯ КІЛЬКОСТІ АТАК ПРОГРАМ-ВИМАГАЧІВ У 2024 РОЦІ ТА ЩО ЦЕ ОЗНАЧАЄ

Як пише видання The Hacker News, індустрія програм-вимагачів різко зросла у 2023 році, оскільки кількість жертв у всьому світі зросла на 55,5% і досягла приголомшливих 5070. Але 2024 рік від початку показує зовсім іншу картину. У той час як у четвертому кварталі 2023 року цифри стрімко зросли (1309 випадків), у першому кварталі 2024 року вони знизилися до 1048 випадків. Це на 22% менше атак програм-вимагачів порівняно з четвертим кварталом 2023 року.

Згідно зі статтею, такі результати стали наслідком кількох факторів, серед яких робота правоохоронних органів та зменшення виплат викупу. І хоча з'являються нові угрупування, вони не компенсують падіння кількості атак та їх жертв.

ПІДРИВ ДОВІРИ ДО УРЯДУ: ЩО ІГРИ, ОПИТУВАННЯ ТА СЦЕНАРІЇ ПОКАЗУЮТЬ ПРО АЛЬТЕРНАТИВНЕ КІБЕРМАЙБУТНЄ

Звіт Центру стратегічних і міжнародних досліджень (CSIS), опублікований 8 квітня попереджає, що критично важливі державні програми, на які мільйони американців покладаються для задоволення основних потреб, таких як їжа та охорона здоров'я, можуть стати основними цілями майбутніх кібератак, чия мета – посіяти хаос та підірвати довіру до інститутів США. У звіті про падіння довіри до уряду, який базується на шести військових іграх і аналітичних внесках десятків кіберекспертів, описано сценарії, коли хакери зривають роботу таких служб, як система розподілу їжі SNAP та система медичної допомоги Medicaid під час виборів, щоб розпалити паніку серед найбільш уразливих членів суспільства.

Щоб запобігати таким випадкам, CSIS рекомендував федеральному уряду вжити заходів для підвищення рівня кібербезпеки базових послуг, посилити просвітницькі кампанії щодо кібербезпеки та створити в уряді систему кіберзвітування.

ЯК ЕНЕРГЕТИЧНИЙ СЕКТОР МОЖЕ ПІДВИЩИТИ СВОЮ СТІЙКІСТЬ ДО АТАК ПРОГРАМ-ВИМАГАЧІВ?

Оскільки енергетичний сектор відіграє життєво-важливу роль у кожному функціонуючому суспільстві, він завжди був головною мішенню для підтримуваних державою кіберзлочинців, йдеться у статті видання Help Net Security. Оскільки рівень кібератак і програм-вимагачів продовжує зростати, постачальник електроенергії насправді стурбовані рівнем операційної стійкості галузі. Ризики в енергетичному секторі зумовлені його залежністю від застарілих і успадкованих технологій і розгортанням пристроїв Інтернету речей (IoT). Щоб усунути ці критичні ризики, енергетичні компанії повинні проводити систематичну оцінку вразливості та тестування на проникнення, приділяючи особливу увагу додаткам, які взаємодіють між IT та OT системами. Організаціям також слід запровадити комбінацію рішень для керування ідентифікаційним доступом (IAM) і керування привілеями (PAM).

ЛІДЕРСТВО, КУЛЬТУРА ТА ВІЙСЬКОВА КІБЕРТРУДОВА СИЛА

У статті на War on the Rocks йдеться про те, що військова кіберспільнота стикається з постійними проблемами у вербуванні, навчанні та утриманні кваліфікованого персоналу, попри дедалі більше визнання важливості кібероперацій. Хоча дискусії часто зосереджуються на перевагах приватного сектору, важливо враховувати нематеріальні переваги військової служби, такі як можливості лідерства та унікальна культура. Ефективне управління талантами вимагає балансування конкуруючих пріоритетів і визнання взаємозалежності процесів найму, навчання та утримання. Розбудова сильної кіберкультури та розвиток лідерів є ключовими компонентами управління талантами, що підкреслює потребу в особливому військовому досвіді. Охоплюючи та покращуючи унікальні аспекти військового життя, кіберробоча сила може диференціювати себе та ефективно залучати й утримувати таланти, попри конкуренцію з боку приватного сектору.

ПОЛОВИНА БРИТАНСЬКИХ КОМПАНІЙ ПОСТРАЖДАЛА ВІД КІБЕРІНЦИДЕНТІВ ЗА МИНУЛИЙ РІК

Половина компаній Великобританії повідомили, що протягом останніх 12 місяців стикнулися з кіберінцидентами або порушенням цілісності даних, згідно з опитуванням уряду Великобританії про порушення кібербезпеки за 2024 рік.

Близько третини (32%) благодійних організацій також зазнали порушення кібербезпеки або атаки протягом цього періоду. Це свідчить про збільшення порівняно з торішнім опитуванням, коли 32% компаній і 24% благодійних організацій зазнали певної форми кібератак або зламу. Фішингові повідомлення були причиною більшості кібератак – 84% для компаній і 83% для благодійних організацій.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

УКРАЇНА ПОГЛИБЛЮЄ СПІВПРАЦЮ З КІБЕРБЕЗПЕКОВИМИ АГЕНЦІЯМИ ЄС, НАТО ТА РУМУНІЇ

Делегація представників основних суб'єктів забезпечення кібербезпеки України на чолі з секретарем НКЦК, керівником служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Наталією Ткачук 11 квітня 2024 року відвідала Європейський центр компетенції з кібербезпеки (ECCC), Євроатлантичний центр стійкості (EARC), Проєктний Офіс Конвенції Ради Європи з кіберзлочинності (C-PROC), Національний директорат Румунії з кібербезпеки (DNSC), а також Політехнічний університет Бухареста.

Під час зустрічі з керівником ECCC Лукою Тагліаретті було обговорено перспективні напрями взаємодії та передано лист за підписом Секретаря РНБО України Олександра Литвиненка про наміри щодо партнерства та співпраці НКЦК з ECCC. Також обговорено участь України у програмах ECCC «Digital Europe» та «Horizon Europe».

СЕКРЕТАР НКЦК ЗАКЛИКАЛА КРАЇНИ ЄС ТА НАТО ДО СПІЛЬНОЇ ПРОТИДІЇ КІБЕРАГРЕСІЇ РФ

12 квітня 2024 року у м. Бухарест (Румунія) НКЦК та CRDF Global провели третє міжнародне засідання Національного кластера кібербезпеки на тему: «Розбудова партнерств для кіберстійкості Південно-Східної Європи». Під час заходу керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України, секретар НКЦК Наталія Ткачук зазначила, що сьогодні рф веде кібервійну не лише проти України, а й країн Європейського Союзу та НАТО. «Є важливим чіткий меседж від наших партнерів, що такі дії є неприпустимим, а також забезпечення публічного атрибутування до рф. В іншому випадку відчуття безкарності призведе до більшої ескалації прихованої кіберагресії рф проти країн євроатлантичної спільноти та їх громадян», – сказала Секретар НКЦК. Під час заходу учасники обговорили кілька тем, серед яких:

- ризики ескалації кібервійни в Південно-Східній Європі;
- синергія держави та бізнесу для зміцнення колективної безпеки;
- поглиблення співпраці з ЄС та НАТО: практичні кроки для України у сфері кібербезпеки.

УКРАЇНА ВЗЯЛА УЧАСТЬ У НАВЧАННЯХ З КІБЕРОБОРОНИ NATO CCDCOE LOCKED SHIELDS

Представники України взяли участь у Locked Shields 2024 – це найбільші у світі реалістичні навчання з кібероборони, що підкреслюють зобов'язання глобальної спільноти боротися з кіберзагрозами. У навчаннях, організованих Об'єднаним центром передових технологій з кібероборони НАТО (NATO CCDCOE), цього року взяли участь близько 4000 експертів із понад 40 країн. Заступник Секретаря РНБО України Сергій Демедюк наголосив на важливості участі українських фахівців у кібернавчаннях Locked Shields для зміцнення як національної, так і міжнародної кіберстійкості. «У цьому році Україна об'єднує зусилля з Чехією у спільній команді на цих навчаннях. Спільне відпрацювання навичок, обмін досвідом та співпраця є ключовими елементами на шляху до ефективного протистояння сучасним кіберзагрозам».

УКРАЇНА ВПЕРШЕ ВЗЯЛА УЧАСТЬ У ПОЯСНЮВАЛЬНІЙ СЕСІЇ ЄВРОПЕЙСЬКОЇ КОМІСІЇ, ПРИСВЯЧЕНІЙ ЦИФРОВІЗАЦІЇ

23 квітня відбулася пояснювальна сесія Європейської комісії для України щодо переговорного Розділу 10 «Цифрова трансформація та медіа». Це перша зустріч України як країни-кандидата та представників ЄС, що присвячена сфері цифровізації. Під час зустрічі сторона ЄС висловила готовність надалі підтримувати Україну на шляху євроінтеграційних реформ. Зокрема, через механізм Ukraine Facility, який є стратегією у впровадженні всеосяжних реформ та інвестицій на наступні 4 роки.

Також Єврокомісія представила понад 100 актів права ЄС, описала особливості застосування кожного них і надала відповіді щодо реалізації цих актів. Перелік актів містить чинне законодавство ЄС, яке Україна впроваджує в межах Угоди про асоціацію. А також акти, які перебувають на стадії проєктів, але найближчим часом будуть ухвалені в ЄС та стануть обов'язковими для України. Наприклад, eIDAS 2, Акт про штучний інтелект, Акт про кіберстійкість, Акт про кіберсолідарність.

ЄДИНІ СТАНДАРТИ КІБЕРБЕЗПЕКИ: МІНОБОРОНИ ЗМІЦНЮЄ ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ ВІДПОВІДНО ДО СТАНДАРТІВ НАТО

Міністерство оборони ухвалило наказ щодо затвердження основних засад інформаційної безпеки та кібербезпеки в інформаційно-комунікаційних системах. Він визначає уніфіковані базові вимоги (політику верхнього рівня) щодо захисту інформації та кіберзахисту у системах Міністерства оборони. Це означає, що усі системи, сервіси, застосунки та цифрові інструменти Міністерства оборони матимуть єдині, чітко визначені правила щодо кібербезпеки. Вони враховуватимуть кращі підходи НАТО, міжнародні стандарти та практики з інформаційної та кібербезпеки.

ПРЕДСТАВНИКИ НКЦК ПРОВЕЛИ ЗУСТРІЧ З ДЕЛЕГАЦІЄЮ РЕСПУБЛІКИ КЕНІЯ

В ході зустрічі представники Національного координаційного центру кібербезпеки розповіли про діяльність Центру та потенційні напрямки співпраці з кенійською стороною. Зокрема, наголошено на потенціалі співробітництва щодо обміну досвідом та інформацією у сфері кібербезпеки, проведенню навчальних заходів та посиленню протидії поширенню російської дезінформації щодо України в країнах Африки. Зі свого боку представники кенійської делегації зазначили, що зацікавлені у допомозі України у протидії кіберзагрозам та поширенню дезінформації рф, зокрема шляхом проведенням спільних навчальних заходів та наданням експертизи українськими фахівцями.

«АРМІЯ+» МАЄ СПЕЦИФІЧНУ АРХІТЕКТУРУ, ЯКА ДОЗВОЛЯЄ ЗАХИСТИТИ ДАНІ МАКСИМАЛЬНО БЕЗПЕЧНО – КАТЕРИНА ЧЕРНОГОРЕНКО

Заступниця Міністра оборони Катерина Черногоренко розповіла, що головним завданням, що стоїть перед командою спеціалістів-розробників, є надійний захист персональних даних військовослужбовців та службової інформації. Навіть якщо процес потребуватиме більше часу. «Сам мобільний застосунок є своєрідним запобіжником від витоків, тому що має специфічну архітектуру, яка дозволяє захистити агрегацію даних щодо людини. Ми залучаємо найкращих експертів вже зараз, на етапі конструювання і розробки застосунку. Окремо працюємо над комплексною системою, щоб додаток був захищений на належному рівні. Безпека даних — це наш топ-пріоритет. І ми готові пожертвувати частково строками релізу на користь безпеки», – розповіла заступниця Міністра оборони.

Н. ТКАЧУК НАГОЛОСИЛА НА АКТУАЛЬНОСТІ ТА НЕОБХІДНОСТІ ВІДПРАЦЮВАННЯ СЕКТОРАЛЬНОЇ ТА МІЖВІДОМЧОЇ ВЗАЄМОДІЇ ПІД ЧАС РЕАГУВАННЯ НА КІБЕРАТАКИ

Керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Наталія Ткачук взяла участь у командно-штабних навчаннях (ТТХ), спрямованих на відпрацювання механізму реагування на ситуації, спричинені кібер- та гібридними загрозами в енергетичному секторі. Під час відкриття заходу вона зазначила, що практику проведення командно-штабних навчань в Україні було запроваджено НКЦК та закріплено в Стратегії кібербезпеки України. Адже ТТХ дають змогу визначити слабкі місця у механізмі реагування на кіберзагрози та усунути існуючі прогалини. «Важливу роль відіграють секторальні ТТХ, зокрема в енергетичному секторі. На фоні загострення кіберагресії з боку рф, яка навіть почала координувати кібератаки з ракетними обстрілами об'єктів критичної інфраструктури, такі навчання стають більш ніж актуальними та необхідними», – сказала секретар НКЦК.

НКЦК ПРОВІВ НАВЧАННЯ «УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ» ДЛЯ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ ОВА

Національний координаційний центр кібербезпеки при РНБО України за підтримки Державного департаменту США та CRDF Global в Україні провів навчальну програму «Управління вразливостями» (VDP) для фахівців з кібербезпеки обласних військових адміністрацій. У заході взяли представники з усіх регіонів України. Здобутий досвід дозволить фахівцям покращити свій практичний рівень знань у проведенні комплексного аналізу стану кібербезпеки своїх установ та розуміти принципи та підходи, якими керуються зловмисники при проведенні кібератак.

ДЕРЖСПЕЦЗВ'ЯЗКУ РАЗОМ З ПРЕДСТАВНИКАМИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ДЕРЖОРГАНІВ ПРОПРАЦЮВАЛИ ПЛАНИ КІБЕРЗАХИСТУ УСТАНОВ

Державна служба спеціального зв'язку та захисту інформації України за підтримки Національного агентства України з питань державної служби, Вищої школи публічного управління та проєкту ЄС «Підтримка комплексної реформи державного управління в Україні» (EU4PAR 2) провела третій одноденний офлайн семінар «Реагування на кіберінциденти» для представників державних органів та об'єктів критичної інфраструктури.

Представники 21 організації працювали над розробкою та оновленням планів кіберзахисту. Зокрема, формували мінімальний набір завдань, які насамперед мають бути впроваджені або заплановані для впровадження на об'єкті критичної інфраструктури. Вся робота проходила під контролем фахівців Департаменту кіберзахисту Адміністрації Держспецзв'язку, Урядової команди реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Держспецзв'язку, та Державного центру кіберзахисту Держспецзв'язку.

В УКРАЇНІ ЗАПУСТИЛИ МІЖВІДОМЧУ ОСВІТНЮ ПЛАТФОРМУ ДЛЯ ПРЕДСТАВНИКІВ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ

Національна академія Служби безпеки України презентувала представникам сектору безпеки і оборони України та міжнародним партнерам міжвідомчу освітню платформу з 12 сертифікатних програм. Завдяки міжвідомчій освітній платформі фахівці сектору безпеки і оборони зможуть пройти короткострокові навчання в Академії СБУ за напрямами боротьби з тероризмом, оперативно-розшукової діяльності, захисту об'єктів критичної інфраструктури, оперативної психології, охорони держтаємниці, переговорної діяльності у кризових ситуаціях, протидії злочинам із використанням віртуальних активів тощо. Програми є гнучкими та можуть враховувати індивідуальні потреби підрозділів сектору безпеки та оборони.

У ХМЕЛЬНИЦЬКОМУ КІБЕРПОЛІЦЕЙСЬКІ ПРОВЕЛИ НАВЧАННЯ З ЦИФРОВОЇ БЕЗПЕКИ ДЛЯ ПРЕДСТАВНИКІВ ОРГАНІВ ВЛАДИ ТА САМОВРЯДУВАННЯ

Тренінг для посадовців від фахівців хмельницької кіберполіції відбувся у рамках дводенного семінару на тему «Формування мережі цифрових лідерів», організованого програмою розвитку ООН (ПРООН) в Україні за підтримки уряду Швеції. У заході взяли участь представники органів влади і самоврядування, місцевих центрів підвищення кваліфікації та запрошені експерти. Учасників ознайомили з найпоширенішими кібершахрайствами, найважливішими правилами кібергігієни та розповіли про проєкт кіберполіції «BRAMA», який спеціалізується на протидії дезінформації та незаконному контенту в інформаційному просторі.

ФАХІВЦІ ДЕРЖСПЕЦЗВ'ЯЗКУ ПРОВЕЛИ ТРЕНІНГ ДЛЯ ФАСИЛІТАТОРІВ КОМАНДНО-ШТАБНИХ НАВЧАНЬ

Фахівці Держспецзв'язку провели тренінг для фасилітаторів командно-штабних навчань (Table Top Exercises) з представниками секторальних органів у сфері захисту критичної інфраструктури. Участь у триденному тренінгу, проведеному за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України», взяли представники майже двох десятків центральних органів виконавчої влади. Тренінг дав змогу запрошеним представникам міністерств здобути необхідні знання з питань фасилітації ТТХ та інших типів вправ.

ПРЕДСТАВНИКИ МЕДИЧНИХ УСТАНОВ ВЧИЛИСЯ БОРОТИСЯ З КІБЕРАТАКАМИ ТИПУ RANSOMWARE

Фахівці Держспецзв'язку провели чергові командно-штабні навчання CIREX.Cyber.Ransomware, спрямовані на посилення навичок протистояння хакерським атакам з використанням програм-вимагачів (ransomware). У заході взяли участь понад три десятки представників закладів та установ медичної сфери, а також фахівці основних суб'єктів національної системи кібербезпеки. Навчання підготовлені з використанням передових методик Агентства США з питань кібербезпеки та захисту інфраструктури (CISA), які були адаптовані до українського ландшафту загроз фахівцями Держспецзв'язку та Міністерства охорони здоров'я.

МЗС АНОНСУВАВ ПРОВЕДЕННЯ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ З ПИТАНЬ КІБЕРДИПЛОМАТІЇ

5 квітня заступник міністра закордонних справ України з питань цифрового розвитку, цифрових трансформацій і цифровізації Антон Демьохін взяв участь в установчому засіданні оргкомітету міжнародного «Форуму з кібердипломатії». У вітальному слові заступник міністра Антон Демьохін зазначив, що «враховуючи науково-освітній потенціал учасників, Форум покликаний стати провідною платформою для співпраці та розвитку інновацій у сфері кібердипломатії, а також підґрунтям для забезпечення миру, стабільності та стійкості в цифрову епоху». Першим заходом стане «Перша науково-практична конференція з питань кібердипломатії», яка відбудеться 15-16 травня 2024 року в м.Київ, метою якої є дослідження потенціалу сфери кібердипломатії, її ролі у формуванні майбутнього міжнародних відносин.

СБУ ІДЕНТИФІКУВАЛА ХАКЕРІВ РОСІЙСЬКОГО ГРУ, ЯКІ АТАКУВАЛИ «КИЇВСТАР»

Кіберфахівці та слідчі Служби безпеки України збирають доказову базу на хакерів головного розвідувального управління генерального штабу рф (більш відомого як гру), які здійснили атаку на одного з національних операторів мобільного зв'язку «Київстар». Після проведення всіх експертиз та оголошення підозр матеріали цього розслідування будуть передані до Міжнародного кримінального суду у Гаазі.

Наразі СБУ встановила, що атаку на «Київстар» реалізувало хакерське угруповання Sand-Worm, яке є штатним підрозділом російського гру. Зараз СБУ проводить низку експертиз щодо уражених хакерами систем і завданих збитків. Також спецслужба спрямувала запити на отримання додаткової інформації від міжнародних партнерів.

КІБЕРПОЛІЦІЯ ТА ЦПД ПІДПИСАЛИ МЕМОРАНДУМ ПРО СПІВПРАЦЮ

2 квітня начальник Департаменту кіберполіції Юрій Виходець та керівник Центру протидії дезінформації РНБО України Андрій Коваленко підписали меморандум про співпрацю. Сторони відзначили важливість координації дій державних органів та обміну досвідом з протидії дезінформації, зокрема: проведення спільних тренінгів, конференцій, навчань для підвищення рівня кібер- та медіаграмотності серед українців. Також керівники обговорили наявні напрямки співпраці та актуальні виклики у сфері інформаційної безпеки, які постали перед Україною через повномасштабну агресію рф.

КІБЕРПОЛІЦІЯ ЗАПУСТИЛА НОВИЙ ПРОЄКТ «КІБЕР БРАМА» ДЛЯ ПІДВИЩЕННЯ РІВНЯ КІБЕРГІГІЄНИ УКРАЇНЦІВ

4 квітня правоохоронці презентували запуск онлайн-платформи, метою якої є надання користувачам інтернету інструментів та знань, необхідних для безпечного перебування в цифровому просторі. Проєкт створено Консультативною місією Європейського Союзу в Україні за ініціативи Департаменту кіберполіції Національної поліції України, у партнерстві з громадською організацією МІНЗМІН. Він реалізується завдяки підтримці Міжнародного Фонду «Відродження» та Представництва Європейського Союзу в Україні.

«Кібер Брама» розрахована на різні категорії користувачів, включаючи студентів, освітян та підприємців. Ресурс містить практичні рекомендації та інструменти для захисту від кіберзагроз, фейків і дезінформації. Завдяки проєкту громадяни зможуть отримувати корисну інформацію та з легкістю освоїти нюанси безпечного користування онлайн-платформами, зокрема, соцмережами.

CERT-UA ОПУБЛІКУВАЛА ІНСТРУКЦІЮ ЩОДО ВСТАНОВЛЕННЯ ДВОЕТАПНОЇ АУТЕНТИФІКАЦІЇ В ПОПУЛЯРНИХ МЕСЕНДЖЕРАХ

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA розробила інструкцію щодо встановлення двоетапної аутентифікації (скорочено 2FA) для деяких месенджерів та інформаційних систем, зокрема: Telegram, Signal, WhatsApp, Viber, Ukr.net, Google та Facebook. Використання цих налаштувань є особливо важливим у ситуації, коли публічні поштові сервіси використовуються як основний «корпоративний» засіб електронного листування: https://cert.gov.ua/article/6278274

ГОЛОВА ДЕРЖСПЕЦЗВ'ЯЗКУ ЗУСТРІВСЯ З КЕРІВНИЦТВОМ АМЕРИКАНСЬКОЇ ТОРГОВЕЛЬНОЇ ПАЛАТИ В УКРАЇНІ

Голова Держспецзв'язку Юрій Мироненко та його команда провели робочу зустріч з віцепрезидентом Американської торговельної палати в Україні (AmCham Ukraine) Тетяною Прокопчук, відповідальним членом Ради директорів AmCham Ukraine Сергієм Мартинчуком, а також членами Комітету з питань безпеки та оборони AmCham. У ході діалогу сторони обговорили низку актуальних питань, зокрема:

- законодавчі ініціативи, до розробки яких може бути залучений бізнес;
- питання кібербезпеки та захисту критичної інфраструктури;
- регулювання сфери хмарних послуг.

CERT-UA ПОПЕРЕДИЛА ПРО КІБЕРЗАГРОЗУ ДЛЯ СИЛ ОБОРОНИ УКРАЇНИ

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, яка діє при Держспецзв'язку, повідомила про підвищену активність угруповання UAC-0184, яке намагається отримати доступ до комп'ютерів військовослужбовців з метою викрадення документів та даних месенджерів. Зловмисники використовують популярні месенджери, соціальні мережі та інші платформи для знайомств та спілкування з метою розповсюдження шкідливих програм. Їхні методи включають:

- супровідні повідомлення-приманки: наприклад, про відкриття виконавчого провадження/кримінальної справи; відео бойових дій; запит на знайомство тощо;
- файли (архіви) з проханням допомогти у їх відкритті/обробці.

Зловмисники застосовують такі шкідливі програми, в тому числі для викрадення та вивантаження даних з комп'ютера, зокрема повідомлень і контактних даних месенджера Signal, який є доволі популярним серед військових.

РОСІЙСЬКІ ХАКЕРИ ВИКОРИСТОВУЮТЬ СОЦІАЛЬНУ ІНЖЕНЕРІЮ ДЛЯ КІБЕРАТАК НА ЗСУ

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, яка діє при Держспецзв'язку, попередила про нову кіберзагрозу, спрямовану проти військовослужбовців Сил оборони України. Зловмисники розсилають шкідливі файли через месенджер Signal, маскуючи їх під документи, необхідні для заміщення посади в Департаменті операцій з підтримки миру ООН.

CERT-UA відстежує цю ворожу хакерську групу під ідентифікатором UAC-0149. Саме вона дуже активно працює проти окремих військовослужбовців, застосовуючи обман та різноманітні пропозиції.

ШАХРАЇ ВИКРАДАЮТЬ АКАУНТИ WHATSAPP, ВИКОРИСТОВУЮЧИ ФЕЙКОВІ ПЕТИЦІЇ ПРО ПРИСВОЄННЯ «ГЕРОЯ УКРАЇНИ» ЗАГИБЛИМ ЗАХИСНИКАМ

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA попередила про нову шахрайську схему, спрямовану на крадіжку в українців акаунтів WhatsApp. Зловмисники розсилають повідомлення в WhatsApp, закликаючи проголосувати за електронну петицію про присвоєння звання «Герой України» посмертно військовослужбовцям ЗСУ. Повідомлення містять посилання на фейковий сайт, який імітує офіційну вебсторінку «Електронних петицій».

Описана активність відстежується CERT-UA з квітня 2024 року за ідентифікатором UAC-0195. Станом на 20.04.2024 CERT-UA виявила 18 доменних імен та направила відповідні запити щодо їх блокування.

СБУ ЗАТРИМАЛА У КИЄВІ ПРОРОСІЙСЬКИХ ХАКЕРІВ, ЯКІ СТВОРИЛИ ФЕЙКОВІ АКАУНТИ КЕРІВНИКІВ УКРАЇНСЬКИХ СПЕЦСЛУЖБ

Служба безпеки ліквідувала у Києві ботоферми, які проводили інформаційні диверсії на користь російської розвідки. У ході комплексних заходів затримано двох організаторів, які масово поширювали дезінформацію про війну в Україні та намагались штучно дискредитувати Сили оборони. Для цього створювали фейкові акаунти у соцмережах та месенджерах, зокрема від імені Голови Служби безпеки та начальника ГУР МО. Також в соцмережах вони реєстрували фейкові сторінки українців з різних регіонів. Загалом потужності ботоферми дозволяли її організаторам щодня генерувати понад тисячу фейкових акаунтів. Зловмисники координували свої дії з представниками російської розвідки, від яких отримували «методички» для проведення підривної діяльності. Фігуранти перебувають під вартою, їм загрожує до 7 років тюрми.

8. ПЕРША СВІТОВА КІБЕРВІЙНА

ВСЕРЕДИНІ РОСІЙСЬКОЇ ТІНЬОВОЇ ТОРГІВЛІ ЗАПЧАСТИНАМИ ДО ЗБРОЇ, ЯКУ ПІДЖИВЛЮЄ КРИПТОВАЛЮТА

1 квітня видання The Wall Street Journal описало, як стейблкойн Tether став «незамінним» для російської військової промисловості. У той час як Міністерство фінансів США запровадило санкції, намагаючись обмежити здатність москви виробляти зброю та розвивати свою військову промисловість, кремль зміг обійти санкції за допомогою криптовалюти та заплатити Китаю мільйони у криптовалюті за виробництво компонентів до високотехнологічної зброї.

ХАКЕРИ ВИКРАЛИ РОСІЙСЬКУ БАЗУ УВ'ЯЗНЕНИХ, ЩОБ ПОМСТИТИСЯ ЗА СМЕРТЬ НАВАЛЬНОГО

1 квітня CNN повідомила, що хакери отримали контроль над вебсайтом пенітенціарної системи рф та опублікували фотографію Навального та його вдови Юлії на мітингу з повідомленням «Хай живе Олексій Навальний!». Вони також заявили, що викрали базу даних, що містить інформацію про сотні тисяч російських ув'язнених, включаючи дані про ув'язнених у виправній колонії, де Навальний помер 16 лютого. Повідомляється, що російській владі знадобилося кілька днів, щоб відновити контроль над своєю комп'ютерною мережею. Хакери, серед яких, за словами CNN, були представники різних національностей, кажуть, що вони оприлюднили цю інформацію, включаючи контактну інформацію родичів ув'язнених, «в надії, що хтось зможе зв'язатися з ними та допомогти зрозуміти, що сталося з Навальним».

ДОСЛІДНИКИ ВИЯВИЛИ НОВУ БАНДУ ПРОГРАМ-ВИМАГАЧІВ «МУЛЯКА», ЯКА АТАКУЄ РОСІЙСЬКИЙ БІЗНЕС

Раніше невідома банда програм-вимагачів атакує російські компанії за допомогою зловмисного програмного забезпечення на основі витоку вихідного коду хакерської групи Conti. Банда, яку дослідники московської компанії з кібербезпеки F.A.C.C.T. назвали «Муляка», залишила мінімальні сліди від своїх атак, але, ймовірно, діє принаймні з грудня 2023 року. Просунуті методи роблять цю групу вартою уваги. В одному з зареєстрованих інцидентів у січні «Муляка» атакувала бізнес, зашифрувавши його системи Windows і віртуальну інфраструктуру VMware ESXi за допомогою власної служби віртуальної приватної мережі (VPN) її жертви. Зловмисне ПЗ було замасковане під звичайну корпоративну антивірусну програму, що дозволило йому обійти протоколи безпеки та зашифрувати файли мережі.

Геополітичний контекст у росії створює оптимальне середовище для такої кіберзлочинної діяльності. F.A.C.C.T. припускає, що поточна політична ситуація породжує безкарність, недбалість у сфері кібербезпеки бізнесу та велику кількість потенційних жертв, що робить її привабливою для фінансово вмотивованих груп хакерів.

УКРАЇНА НАГОРОДИЛА ІНОЗЕМНИХ ІТ-ФАХІВЦІВ ЗА ДОПОМОГУ В КІБЕРПРОТИСТОЯННІ З РОСІЄЮ

4 квітня BBC оприлюднила матеріал, присвячений іноземним IT-волонтерам, які допомагають Україні протидіяти російській агресії. Автор статті Джо Тіді (Joe Tidy) висловлює сумнів в етичності нагородження таких кіберекспертів відзнаками Збройних Сил України (зокрема – Десантно-штурмовими військами України), адже, на його думку, це сприяє розмиттю понять між комбатантами та нон-комбатантами в кіберпросторі. Україна нагородила кіберекспертів з групи One Fist які допомогли Україні отримати дані з камер в окупованому Криму, щоб каталогізувати російські танки та техніку, які переміщують через Керченський міст, а також викрали 100 гігабайтів даних російського виробника зброї.

КОМПАНІЯ CLAROTY ПРОВЕЛА АНАЛІЗ КІБЕРАТАКИ ПРОУКРАЇНСЬКОЇ ГРУПИ BLACKJACK НА ФІЗИЧНУ ІНФРАСТРУКТУРУ РОСІЙСЬКОГО «МОСКОЛЕКТОРУ»

15 квітня фірма з кібербезпеки промислового та корпоративного Інтернету речей Claroty провела аналіз шкідливого програмного забезпечення Fuxnet, що розроблене для атак систем промислового контролю (ICS) – саме його нещодавно використали проукраїнські хакери для атаки на інфраструктуру російської організації «Москолектор». За оцінками Claroty угрупуванню не вдалось повною мірою досягти результатів, про які вони заявляли – замість компрометації 87 000 датчиків, у тому числі пов'язаних з аеропортами, системами метро та газопроводами, хакерам вдалось вивести з ладу 500 шлюзів датчиків. Хоча цей обсяг менше, ніж заявлено, однак він також є значним, оскільки «Москолектор» доведеться витрати час на їх фізичну заміну, при тому, що ці датчики територіально розподілені по всій москві.

ЗА ДАНИМИ MICROSOFT В ОСТАННІ ДВА МІСЯЦІ РОСІЯ ІСТОТНО ПОСИЛИЛА ОПЕРАЦІЇ ВПЛИВУ ПРОТИ США

17 квітня Microsoft у своєму звіті щодо ворожої активності іноземних суб'єктів проти американського виборчого процесу, підкреслюють, що росія істотно наростила свою активність аби просувати в США антиукраїнські наративи. Основне угрупування, яке відстежує Microsoft у цьому зв'язку, Storm-1516. Вони використовують стандартну техніку російських/радянських спецслужб, роблячи інформаційний вкид через недостовірне джерело, яке потім розповсюджується мережею вебсайтів, звідки ці повідомлення поширюються легітимними користувачами (російськими мігрантами, чиновниками та просто зацікавленими особами).

РОСІЙСЬКИМ ХАКЕРАМ ВДАЛОСЬ ВПЛИНУТИ НА СИСТЕМУ ВОДОПОСТАЧАННЯ НЕВЕЛИКОГО ТЕХАСЬКОГО МІСТА МУЛШОУ

22 квітня стали відомі подробиці кібератак на системи водопостачання в декількох невеликих американських містах (переважно в Техасі). російське угрупування CyberArmyofRussia_Reborn атакувало системи водопостачання в невеликих населених пунктах (2000-5000 мешканців). В одному випадку атака була вдалою – хакери спричинили переповнення водопровідної системи, перш ніж атаку припинили, а фахівці компанії перевели її функціонування у ручний режим. Ці атаки є логічним продовженням серії атак на схожі об'єкти, з якими США стикнулись у четвертому кварталі 2023 року. Кібербезпекова компанія Mandiant поширила свій звіт в якому звинувачує в цих атаках російську APT групу Sandworm.

НОУТБУК ГОЛОВИ ПАРЛАМЕНТСЬКОГО КОМІТЕТУ ЗАКОРДОННИХ СПРАВ БЕЛЬГІЇ ЗЛАМАНИЙ КИТАЙСЬКИМИ ХАКЕРАМИ

25 квітня Голова парламентського комітету закордонних справ Бельгії Елс Ван Хуф (Els Van Hoof) повідомила, що ще у 2021 році її ноутбук був зламаний китайськими хакерами. За її словами 400 членів Міжпарламентського альянсу щодо Китаю (IPAC), групи, яка об'єднує мережу політиків, що критично ставляться до Китаю (і членом якої є Елс Ван Хуф), стали мішенню цієї кібератаки.

ЯК УКРАЇНСЬКІ ХАКЕРИ-ВОЛОНТЕРИ СТВОРИЛИ «СКООРДИНОВАНУ МАШИНУ» НАВКОЛО АТАК НИЗЬКОГО РІВНЯ

Стаття The Record розповідає про історію створення та роль української IT-армії у кіберпротистоянні з рф. В статті відмічається, що IT-армія була створена Міністерством цифрової трансформації України, щоб боротися з росією в кіберпросторі, використовуючи атаки, як-от псування вебсайтів і виведення їх з ладу.

Залишаються питання щодо зв'язків групи з українським урядом: попри те, що група була створена за розпорядженням українського уряду, як IT-армія, так і чиновники стверджують, що їхня співпраця закінчилася з заснуванням. Однак характер роботи IT-армії змушує деяких світових кібераналітиків припускати, що існує ймовірна неофіційна співпраця між групою та секторами оборони та розвідки України.

РОСІЙСЬКИЙ APT ВИКОРИСТОВУЄ НОВИЙ БЕКДОР KAPEKA ПІД ЧАС АТАК У СХІДНІЙ ЄВРОПІ

Раніше незадокументований «гнучкий» бекдор під назвою Kapeka «спорадично» спостерігався під час кібератак, спрямованих на Східну Європу, включаючи Естонію та Україну, принаймні з середини 2022 року.

Таких висновків дійшла фінська кібербезпекова фірма WithSecure, яка приписала зловмисне програмне забезпечення пов'язаній з Росією групі Sandworm (також APT44 або Seashell Blizzard). Microsoft відстежує ту саму шкідливу програму під назвою KnuckleTouch.

9. РІЗНЕ

СУД ПІДТВЕРДЖУЄ ПРАВО FCC ЗАБОРОНЯТИ ТЕХНОЛОГІЮ ТЕЛЕКОМУНІКАЦІЙНИХ КОМПАНІЙ, ЩО НАЛЕЖАТЬ КИТАЮ, АЛЕ ЗВУЖУЄ ВИЗНАЧЕННЯ ОКІ

Як постановив Апеляційний суд США з округу Колумбія, Федеральна комісія зі зв'язку (FCC) діяла в межах своїх повноважень, коли заборонила продукти відеоспостереження, виготовлені двома китайськими компаніями. Заборона на продукцію Hikvision і Dahua відповідає Закону про безпечне обладнання (SEA) від 2021 року, спрямованого на протидію загрозі національній безпеці, яку створює телекомунікаційне обладнання, доступне китайському уряду.
Однак це рішення ставить під сумнів широке тлумачення FCC «критичної інфраструктури». Суд оголошує загальне застосування агентством терміну, який диктував рамки заборони, як «невиправдано широке», «довільне та примхливе». Конфлікт щодо модифікації широко використовуваного терміну, ймовірно, викличе широку та прискіпливу юридичну дискусію та потенційно змінить межі федерального регулювання.

Не погодившись із широким визначенням критичної інфраструктури, наданим Федеральною комісією зв'язку, суд зобов'язав змінити визначення на основі формулювань Закону про дозвіл на національну оборону 2019 року.