НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

УКРАЇНСЬКА ФУНДАЦІЯ БЕЗПЕКОВИХ СТУДІЙ

CYBER DIGEST.

Огляд подій в сфері кібербезпеки,
жовтень-листопад 2023

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

Світ продовжує формувати системну кібербезпекової політики щодо штучного інтелекту. Наприкінці жовтня Президент США Дж. Байден підписав новий указ. На його реалізацію CISA вже оприлюднила власну Дорожню карту щодо того, як це ключове кібербезпекове федеральне відомство буде враховувати виклики ШІ у своїй діяльності, а спільно з NCSC Великобританії випустила спільні рекомендації щодо безпечної розробки системи ШІ. Європейський Союз, своєю чергою, планує провести оцінку ризиків, створених ШІ – результати цієї оцінки будуть використані при розробці нормативно-правової бази та політики для зменшення ризиків і зміцнення позицій ЄС у світовому технологічному ландшафті. Ця активізація зусиль урядів обумовлена все ширшим використанням технологій на базі ШІ – від розробки нових програм до загроз автономним системам управління морським транспортом.

Глобальне суперництво між США та Китаєм в цифровому просторі триває. RAND Corporation у своїх дослідженнях вказує на те, що саме конкуренції між США та Китаєм за цифрову інфраструктуру буде матиме вирішальне значення для військових сил та операцій в регіоні. Китайські APT-групи активізують свої кібершпигунські операції, при чому як проти державних організацій (як, наприклад, велика кампанія проти державних установ Камбоджі), так і приватного сектору (зокрема, проти групи компаній-виробників напівпровідників у Східній Азії).

Боротьба з вірусами-вимагачами продовжується. Наразі США розглядає як наступний крок протидії не лише боротьбу з інфраструктурою злочинців чи конкретними групами, але і зміну поведінки жертв. Зокрема це стосується посилення заходів із недопущення виплати викупів аби не заохочувати злочинців до зловмисних дій. Поки що ці зусилля є лише частково успішними – ransomware групи продовжують досить успішну діяльність, атакуючи все нові цілі. Так у листопаді від дій таких груп постраждав один з великих банків Китаю (ICBC), а також Британська бібліотека. В США під ударом залишається сектор охорони здоров'я. Про недостатність уваги до власної кібербезпеки в цьому секторі свідчить той факт, що за даними компанії Sophos зловмисникам вдалося зашифрувати дані під час майже трьох чвертей атак.

Останній квартал року – традиційний час для появи прогнозів щодо кібербезпекового ландшафту на наступний рік. У жовтні-листопаді з'явилось два таких прогнози – від компаній Proofpoint та Trellix. Попри різні акценти обидві компанії відзначають зростання загроз від ШІ (його використання зловмисниками для організації фішингових атак, голосове шахрайство), фішингові атаки проти мобільних пристроїв, підвищена увага злочинців до облікових записів користувачів та приховані атаки на периферійні пристрої. Ці прогнози доповнюються оцінками британський NCSC який зазначив, що ОКІ зіштовхуються із «тривалою та значною загрозою» на тлі зростання сил державних угруповань, а також як наслідок зростання загальної агресивної кіберактивності та нових геополітичних викликів.

Загалом все більше компаній відзначають зростання уваги зловмисників до соціальної інженерії. Хоча «атаки на людину» і раніше були ключовим методом на початкових стадіях кібератак, однак ШІ дав новий поштовх цій діяльності. Можливості ШІ у створені більш достовірних фішингових імейлів, імітації голосу і навіть відео людей, поява можливості динамічного управління великою кількістю акаунтів в соціальних мережах – істотно змінює ландшафт загроз.

У сфері загроз критичній інфраструктурі найбільш помітним випадком стала вдала атака іранського кіберугрупування Cyber Av3ngers проти системи управління пов'язану з гідропідйомною станцією. Хоча компанія заявила про відсутність загроз для споживачів, але факт атаки на промислову систему є сталою тенденцією до спроб хакерів впливати на функціонування ОКІ. Це викликає особливе занепокоєння, оскільки багато промислових систем керування доступні через мережу Інтернет – наразі дослідники виявили близько сто тисяч таких систем, хоча посилення безпекових правил призвів до зменшення цієї цифри порівняно з 2019 роком. Це доповнюється виявленням нових 0-day вразливостей в промислових маршрутизаторах. Як контрзаходи безпекові організації (CISA, NSA) оприлюднюють все нові рекомендації щодо безпеки ОТ з відкритим кодом, а також відкрили репозиторій ОТ Intrusion Detection Signature and Analytics для швидшої ідентифікації та виявлення потенційно зловмисної кіберактивності у промислових ОТ-середовищах. Попри всі ці зусилля сектор охорони здоров'я США демонструє слабкий прогрес у поліпшенні власної кібербезпеки

Протягом жовтня-листопада 2023 року українським правоохоронним структурам вдалось провести декілька успішних операцій проти міжнародних груп кіберзлочинців. Один з найбільших успіхів – ліквідація угрупування, яке за допомогою використання ransomware заподіяла шкоду на 80 мільйонів доларів. Ці успіхи доповнюються іншими операціями Кіберполіції спільно з чеськими колегами, а також операцією проти групи, яка починаючи з 2020 року атакувала 168 компаній.

Розвиток міжнародної співпраці залишається вважливим вектором діяльності українських кібербезпекових структур. У листопаді 2023 року Україна (НКЦК РНБО та ДССЗЗІ) підписали Робочу угоду про співпрацю з ENISA (Європейською агенцією кібербезпеки). Для ENISA це стало першою такою угодою з партнером з-поза меж ЄС. Підписання таких документів – важливий елемент на шляху формування глобальної кіберкоаліції для протидії загрозам, що походять із росії та інших держав, які стоять по один бік з агресором.

Не припиняється ворожа діяльність – лише у звітному періоді російська APT29 атакувала посольства по всій Європі, угрупування UAC-0165 намагалось втрутитись в роботу 11 українських провайдерів – ці дані доповнюються черговим звітом Держспецзв'язку, який відзначає, що кількість зареєстрованих кіберінцидентів у першому півріччі 2023 року зросла більше ніж удвічі.

Українські кібербезпекові структури (Держспецзв'язку, СБУ) оприлюднили власні оцінки поточного українського ландшафту кіберзагроз в Україні та прогнозів на найближче майбутнє. Серед таких оцінок – зростання кількості складних атак на ланцюжки постачання, а компанії, які розробляють програмне забезпечення для критичної інфраструктури та військових, зазнаватимуть активних цілеспрямованих кібернападів у довгостроковій перспективі. З іншого боку вже зараз більшість ворожих кібератак спрямовані на доступ до електронного документообігу українських держустанов і технологічних систем інфраструктури. Саме тому СБУ та Держспецзв'язку звернули увагу енергетичних компаній на підвищені загрози кібербезпеці з боку росії у зимовий період. Базуючись на досвіді минулих років спеціальні служби вказують на вірогідність активних спроб російських хакерів вплинути на роботу об'єктів критичної інформаційної інфраструктури, енергетичної сфери та надання ними життєво-важливих сервісів.

Україна продовжує нарощувати власні спроможності щодо реагування на кіберінциденти. Зокрема, розширює практику проведення кібернавчань (наприклад НКЦК проведено змагання з кібербезпеки HackWave та INCIDENT RESPONSE DAYS 2.0, а також відбулись перші секторальні кібернавчання для транспортного сектору CIREX.CoBridge), запускає нові інструменти кібергігієни (наприклад Мінцифра запустила тест на знання правил безпеки в мережі «Кіберграм», а ДССЗЗІ провела всеукраїнський онлайн-урок з кібербезпеки для понад 20 тисяч глядачів) та стимулює інновації в секторі кібербезпеки.

Продовжується дискусія щодо більш радикальних змін у діяльності українських безпекових органів у сфері кібербезпеки. Так, у листопаді 2023 року українська військова розвідка вперше провела наступальну кібероперацію про яку оголосила публічно. Також секретар НКЦК при РНБО України Наталія Ткачук підкреслила необхідність якнайшвидшого створення українських кіберсил на основі досвіду України та успішних міжнародних кейсів.

Перша світова кібервійна триває й агресор не зменшує інтенсивність власних дій. При цьому відповідно до даних компанії Microsoft, у 2023 році авторитарні уряди (росії, КНР, Ірану та Північної Кореї) сконцентрувались на кібершпигунських операціях, намагаючись отримати більше інформації щодо важливих для них зовнішньополітичних ініціатив.

Водночас атаки на КІ – все ще важлива мета кібероперацій. Про це свідчить і звіт Mandiant щодо кібератаки угруповання SandWorm на системи операційних технологій (ОТ) української енергокомпанії наприкінці 2022 року. Актор вперше використав методи OT-level liveing off the land (LotL), щоб, ймовірно, спрацювали автоматичні вимикачі підстанції жертви, спричинивши незаплановане відключення електроенергії, яке збіглося з масовими ракетними ударами по критичній інфраструктурі по всій Україні. Кібератаки проти енергетики по всьому світу з боку російських злочинних груп – помітна тенденція, і такі дії стають все більш небезпечними. Прикладом є Данія, чиї 22 енергетичні кампанії зазнали скоординованої кібератаки у травні 2023 року. Підозрюється, що за цією атакою стоїть та ж Sandworm (APT28).

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

ПАСПОРТНА БАЗА ДАНИХ ВЕЛИКОБРИТАНІЇ ВИКОРИСТОВУВАТИМЕТЬСЯ ДЛЯ ІДЕНТИФІКАЦІЇ ПІДОЗРЮВАНИХ НА ЗАПИСАХ КАМЕР ВІДЕОСПОСТЕРЕЖЕННЯ

3 жовтня видання The Record повідомило, що згідно з планом, нещодавно оголошеним Міністром поліції Великої Британії Крісом Філіпом, зображення облич понад 45 мільйонів людей у британській паспортній базі будуть використовуватися для ідентифікації підозрюваних у кримінальних справах. Платформу з такими можливостями планують запустити протягом наступних двох років.

Запропонована платформа даних об'єднає кілька баз даних, наприклад біометричну систему імміграції та надання притулку для іноземців, покращуючи здатність поліції знаходити збіги за допомогою зображень з різних джерел, таких як камери відеоспостереження, камери дверних дзвінків або відеореєстратори. Такі заходи планують запровадити у відповідь на скарги керівників підприємств роздрібної торгівлі, що поліція не реагує на виклики, пов'язані з крадіжками та нападами на працівників закладів торгівлі. Використання цієї технології для ідентифікації підозрюваних викликає менше заперечень, ніж її використання в реальному часі, що призводить до підвищення ризику арешту невинуватих осіб. Разом з тим, правозахисники вважають застосування такої практики значною загрозою приватності громадян.

CISA ВИЗНАЧИЛАСЬ ІЗ НАСТУПНИМИ КРОКАМИ НА ШЛЯХУ ПЕРЕГЛЯДУ НАЦІОНАЛЬНОГО ПЛАНУ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

20 жовтня CISA оголосила наступні кроки для оновлення Національного плану реагування на кіберінциденти (NCIRP) в частині взаємодії з промисловістю та урядом. В межах ініціативи JCDC, CISA проведе збір інформації від партнерів з державного та приватного секторів, включаючи федеральні міжвідомчі агентства з управління ризиками (SRMA), регуляторів та OKI, щоб визначити ключові зміни для включення в оновлений NCIRP.

ПРЕЗИДЕНТ США ПІДПИСАВ УКАЗ ЩОДО БЕЗПЕЧНОГО ТА ДОВІРЧОГО РОЗВИТКУ І ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

30 жовтня на сайті Білого Дому було оприлюднено Указ (Executive Order) «Щодо безпечного та довірчого розвитку і використання штучного інтелекту» (on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence). Документ що складається з 13 розділів, охоплює широкий спектр питань розвитку ШІ – від охорони порядку та біозахисту до захисту споживачів і робочої сили. Кібербезпеці присвячено окремий четвертий розділ документа. Указом передбачено низку ініціатив, які містять в собі стандартизацію практик розробки та використання, ширші програми навчання персоналу, недопущення використання ШІ в зловмисних цілях. Основні обов'язки щодо виконання цього документу покладено на NIST та CISA.

CISA ПІДПИСАЛА МЕМОРАНДУМ ПРО ВЗАЄМОРОЗУМІННЯ З РЕСПУБЛІКОЮ КОРЕЯ

9 листопада Директор CISA Джен Істерлі та заступник директора Національної розвідувальної служби Республіки Корея (NIS) Бек Чон Ук підписали Меморандум про взаєморозуміння. Документ охоплює такі сфери співпраці як:

- регулярні консультації щодо технічних можливостей і механізмів реагування на загрози кібербезпеці;
- покращення зв'язку між відповідними групами реагування на комп'ютерні надзвичайні ситуації (CERT);
- співпраця над стійкістю ланцюжків постачання критичної інфраструктури;
- обмін передовим досвідом за допомогою спільних навчань;
- обмін експертами та проведення тренінгів;
- обмін найкращими практиками щодо політики, що регулює нові технології, такі як ШІ.

CISA ОПРИЛЮДНИЛО ДОРОЖНЮ КАРТУ ДЛЯ ШТУЧНОГО ІНТЕЛЕКТУ

14 листопада CISA, на виконання Розпорядження Президента США, яке наказало DHS сприяти впровадженню стандартів безпеки ШІ у всьому світі, оприлюднило свою першу Дорожню карту для штучного інтелекту (ШІ). Документ охоплює п'ять основних напрямків:

- відповідальне використовувати ШІ самою CISA при виконанні своїх завдань;
- оцінка та сприяння впровадженню безпечного програмного забезпечення на основі штучного інтелекту для різноманітних зацікавлених сторін;
- захист критичної інфраструктури від зловмисного використання ШІ;
- співпраця з міжвідомчими, міжнародними партнерами та громадськістю щодо ключових зусиль ШІ;
- навчання співробітників CISA використанню систем та технік програмного забезпечення на базі штучного інтелекту.

ЗАПУСК НАЦІОНАЛЬНОЇ КАМПАНІЇ «ЗАВТРАКІБЕРСПЕЦІАЛІСТ»

14 листопада ANSSI запустила національну кампанію «TomorrowCyberSpecialist» для підвищення обізнаності про кіберпрофесії серед учнів середньої та старшої школи.

Дефіцит навичок у цій сфері оцінюється у 15 000 вакантних посад лише у Франції та може зрости в майбутньому. Першочерговим завданням є залучення більшої кількості молодих людей до сектору кібербезпеки, представлення їм різноманітних профілів і професій, щоб деконструювати поточні упередження в секторі.

ФРАНЦІЯ ЗАБОРОНИЛА МІНІСТРАМ КОРИСТУВАТИСЯ WHATSAPP, SIGNAL ТА ВИМАГАЄ ФРАНЦУЗЬКИХ АЛЬТЕРНАТИВ

У меморандумі від 22 листопада Прем'єр-міністр Франції Елізабет Борн заборонила міністрів та їхнім командам популярні застосунки WhatsApp, Telegram і Signal через уразливі місця в безпеці. До 8 грудня уряд мав перейти на використання французького застосунку Olvid чи Tchap, які сертифіковано французьким агентством з кібербезпеки ANSSI.

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

ПРОТЯГОМ ЖОВТНЯ US CYBERCOM ЗДІЙСНЮВАВ МІЖНАРОДНУ СКООРДИНОВАНУ ОБОРОННУ КІБЕРАКТИВНІСТЬ (INCCA)

23 жовтня US CYBERCOM повідомив, що з метою підвищення своєї готовності до реагування на інциденти та розбудови оперативної сумісності, CYBERCOM провів серію заходів під назвою Міжнародна скоординована діяльність з кібербезпеки (INCCA). Серед іншого, CYBERCOM залучив оборонних кіберпрофесіоналів у всьому світі для пошуку, ідентифікації, пом'якшення та публічного поширення відомого зловмисного програмного забезпечення, націленого на мережеву інфраструктуру Міністерства оборони.

CCDCOE ГОТУЄТЬСЯ ДО ОНОВЛЕННЯ CYBER LAW TOOLKIT

30 жовтня Центр передового досвіду НАТО з питань кібербезпеки (CCDCOE) оприлюднив пропозицію для всіх зацікавлених сторін щодо оновлення своєї розробки – Cyber Law Toolkit. Це інтерактивний вебресурс з міжнародного права з питань кібероперацій, який складається з кількох гіпотетичних сценаріїв, кожен із яких містить опис кіберінциденту та його детальний правовий аналіз.

ПЛАН БІЛОГО ДОМУ ЩОДО ПРИПИНЕННЯ ДІЯЛЬНОСТІ ПРОГРАМ-ВИМАГАЧІВ ПРОПАГУЄ ВІДМОВУ ВІД СПЛАТИ ВИКУПУ

1 листопада за результатами третьої зустрічі учасники Міжнародної ініціативи протидії вірусам-вимагачам (CRI) прийняли спільну заяву, одним з ключових меседжів якої була відмова сплачувати викуп операторам програм-вимагачів.

У заяві також йшлося про те, що цьогорічна зустріч CRI була зосереджена на розробці можливостей створювати перешкоди для зловмисників та інфраструктури, яку вони використовують для здійснення атак, покращенні кібербезпеки шляхом обміну інформацією та діям у відповідь на використання програм-вимагачів. Більш детальну інформацію можна знайти у тексті заяви. У зустрічі взяли участь представники 50 країн.

США, ПІВДЕННА КОРЕЯ ТА ЯПОНІЯ СТВОРЮЮТЬ ГРУПУ ДЛЯ БОРОТЬБИ З ХАКЕРСЬКИМИ АТАКАМИ З БОКУ ПІВНІЧНОЇ КОРЕЇ

6 листопада Сполучені Штати, Південна Корея та Японія вирішили заснувати консультативний орган високого рівня в першу чергу для реагування на кіберактивність Північної Кореї. Група зосередить свої зусилля на зміцненні практичного спільного реагування на глобальні кіберзагрози.

Значна частина кібердіяльності Північної Кореї пов'язана зі зломом криптовалютних платформ, оскільки країна прагне фінансувати розробку зброї, і звіти вказують на те, що пов'язані з північнокорейськими військовими угруповання очолили більшу частину хакерської діяльності проти криптокомпаній в останні роки.

Зусилля щодо посилення кіберспівробітництва між демократичними країнами Тихоокеанського регіону набрали обертів, коли адміністрація Байдена запустила Партнерство Quad Cybersecurity зі США, Індією, Японією та Австралією з метою зміцнення програмного забезпечення, ланцюжків постачання і захисту даних користувачів. Цей крок викликав критику з боку китайських чиновників.

КЛЮЧОВІ КІБЕРЗЛОЧИНЦІ, ЯКІ СТОЯТЬ ЗА СУМНОЗВІСНИМИ РОДИНАМИ ПРОГРАМ-ВИМАГАЧІВ, ЗАТРИМАНІ В УКРАЇНІ

28 листопада Європол повідомив, що правоохоронці семи країн взяли участь в операції із затримання зловмисників у Києві, Черкасах, Рівному та Вінниці. Підозрювані мали зв'язки з сімействами програм-вимагачів LockerGoga, MegaCortex і Dharma. Європол заявив, що затримав ватажка угруповання, а також кількох ключових спільників. Деякі з осіб перевіряли IT-мережі, проводячи атаки грубої сили, ін'єкції SQL і фішингові атаки, а інші – зосереджувалися на відмиванні платежів викупу в криптовалюті. Загалом група брала участь в операціях з програмами-вимагачами, жертвами яких стали щонайменше 1800 осіб з 2019 року.

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

НАТО ЗАЯВЛЯЄ, ЩО БОРЕТЬСЯ З ВІРОГІДНОЮ КІБЕРАТАКОЮ ПІСЛЯ ПУБЛІКАЦІЇ СТРАТЕГІЧНИХ ДОКУМЕНТІВ В ІНТЕРНЕТІ

На початку жовтня, група хактивістів, відома як SiegedSec, злила документи НАТО на платформу Telegram і заявила, що вони зламали несекретні вебсайти НАТО вдруге за три місяці. Хакери заявили, що зламали онлайн-портал «вивчені уроки», де НАТО ділиться стратегічною ідеєю з військовими офіційними особами альянсу. Такі інциденти викликають сумніви щодо здатності НАТО захищати комунікаційні мережі, де альянс ділиться незасекреченими, але закритими даними про нові технології та загрози безпеці. У відповідь НАТО заявив, що «активно займається цими інцидентами» і наголосив на тому, що є об'єктом постійних кібератак.

ХАКЕРИ ВИКРАЛИ БАЗУ ДАНИХ КОРИСТУВАЧІВ З ЄВРОПЕЙСЬКОГО ІНСТИТУТУ ТЕЛЕКОМУНІКАЦІЙНИХ СТАНДАРТІВ

2 жовтня Європейський інститут телекомунікаційних стандартів (ETSI), який є некомерційною установою з розробки стандартів зв'язку, заявив, що хакери викрали базу даних, що ідентифікує його користувачів. Мотивація хакерів лишається незрозумілою.

Після кібератаки ETSI залучив французьке агентство з кібербезпеки ANSSI для розслідування та відновлення системи. Виявлену вразливість було виправлено, але залишається незрозумілим, чи була вона відома раніше, чи це була вразливість нульового дня під час атаки. Було ініційовано судовий розгляд справи, а, також, ETSI звернувся до своїх користувачів з рекомендацією змінити паролі.

ПІВНІЧНОКОРЕЙСЬКА LAZARUS GROUP ОНОВЛЮЄ СВОЄ ОСНОВНЕ ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

4 жовтня видання The Register повідомило, що відоме хакерське угруповання північнокорейського походження Lazarus Group оновило свої можливості використання шкідливих програм, отримавши новий інструмент під назвою LightlessCann. Вважається, що це шкідливе програмне забезпечення є складнішим і потужнішим, ніж його попередники. Схоже, що LightlessCann використовується переважно проти фінансових установ, зокрема в Південній Кореї, у рамках постійних кампаній Lazarus Group з кібершпигунства та крадіжок грошей. У статті наголошується на мінливому ландшафті загроз, створених передовими хакерськими групами, та на необхідності посилених заходів кібербезпеки, особливо у фінансовому секторі.

АКТОРИ, ПОВ'ЯЗАНІ З QAKBOT, РОЗПОВСЮДЖУЮТЬ ЗЛОВМИСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ RANSOM KNIGHT, ПОПРИ ЛІКВІДАЦІЮ ЇХ ІНФРАСТРУКТУРИ – CISCO TALOS

5 жовтня дослідники Cisco Talos повідомили, що оператори ренсомвер Qackbot повертаються. Вони розповсюджують програмне забезпечення-вимагач Ransom Knight у рамках кампанії, яка почалася на початку серпня і триває на момент публікації дослідження. Діяльність угруповання триває, попри знищення інфраструктури Qakbot, яке відбулося під керівництвом ФБР.

Дослідники відзначають, що ця діяльність, здається, почалася до того, як ФБР захопило інфраструктуру Qakbot наприкінці серпня, і триває з того часу. На їх думку, це вказує на те, що операція правоохоронних органів, можливо, не вплинула на інфраструктуру доставлення спаму операторів Qakbot, а лише на їхні командні та контрольні сервери (C2). Оператори Qakbots втратили важливу частину своєї інфраструктури, але вони залишаються на свободі та, можливо, працюють над відновленням своєї роботи, зазначає Cisco Talos.

ПОЛОВИНА ФАХІВЦІВ З КІБЕРБЕЗПЕКИ ПОВІДОМЛЯЮТЬ ПРО ЗБІЛЬШЕННЯ КІЛЬКОСТІ КІБЕРАТАК

Згідно з дослідженням Sapio Research, про яке 3 жовтня повідомило видання Infosecurity Magazine, більша частина (52%) опитаних організацій повідомили про значне збільшення кількості кібератак. Дослідження показує поширену та зростаючу тенденцію щодо викликів кібербезпеці, причому значна кількість компаній відчуває сплеск кіберзагроз. Разом з тим, компанії не проводять регулярних оцінок кіберризиків: менше ніж кожна десята (8%) організацій здійснює оцінку кіберризиків щомісяця, тоді як дві з п'яти (40%) проводять їх щорічно.

Ці цифри підкреслюють необхідність для організацій визначити пріоритети та впровадити надійні заходи кібербезпеки, оскільки еволюція цих загроз створює постійний ризик для безпеки конфіденційних даних і мережі. Отримані результати підкреслюють вкрай важливу потребу в проактивних стратегіях кібербезпеки та постійній адаптації для ефективної протидії зростаючій кількості кіберзагроз.

КИТАЙСЬКІ ШПИГУНИ ЗЛАМУЮТЬ СХІДНОАЗІЙСЬКІ НАПІВПРОВІДНИКОВІ КОМПАНІЇ – ЗВІТ ECLECTICIQ

У статті The Record, опублікованій 6 жовтня, обговорюється звіт ThreatConnect, який розкриває кампанію кібершпигунства APT27 (Emissary Panda), націлену на напівпровідникові компанії у Східній Азії. Зловмисник, також відомий як China Budworm, використовує новий варіант шкідливого програмного забезпечення під назвою SparrowDoor для компрометації організацій у напівпровідниковій промисловості. Кампанія включає фішингові електронні листи, що містять шкідливі вкладення, використовуючи вразливості в макросах Microsoft Excel. Після зараження зловмисне програмне забезпечення дозволяє APT27 отримати несанкціонований доступ до конфіденційної інформації та інтелектуальної власності. У звіті підкреслюється важливість безпеки ланцюга постачання напівпровідників через його критичну роль у різних галузях промисловості та національній безпеці.

MICROSOFT ТА AMAZON СПІЛЬНО З ПРАВООХОРОННИМИ ОРГАНАМИ ПОСИЛЮЮТЬ БОРОТЬБУ З ШАХРАЙСЬКИМИ КОЛ-ЦЕНТРАМИ

19 жовтня стало відомо про спільну ініціативу Microsoft, Amazon та індійської поліції спрямованої проти шахрайства з використанням нелегальних колл-центрів. Злочинці, які керують нелегальними колл-центрами, намагаються видавати себе за легальні, завдали жертвам збитків на понад 1 мільярд доларів. Індійська поліція провела низку масштабних рейдів по країні з метою припинення діяльності таких центрів. 22 енергетичні компанії стали жертвами найбільшої скоординованої атаки на критичну інфраструктуру Данії.

DDOS-АТАКА СТАЛА ПРИЧИНОЮ ЗБОЮ ОНЛАЙН-СЕРВІСУ В ДЕРЖАВНИХ ЗАКЛАДАХ ОХОРОНИ ЗДОРОВ'Я СІНГАПУРУ

1 листопада відбулась масштабна DDoS-атака на медичні заклади Сінгапуру. Як наслідок низка державних медичних закладів протягом 7 годин не могли надавати онлайн-сервіси споживачам. Атака зачепила і ресурси Національної агенції охорони здоров'я Synapxe. В агентстві заявили, що аномальний сплеск мережевого трафіку вранці 1 листопада обійшов наявні інструменти для блокування помилкових дій.

APPLE ПОПЕРЕДЖАЄ ВІРМЕН ПРО СПОНСОРОВАНІ ДЕРЖАВОЮ СПРОБИ ЗЛОМУ

Як 3 листопада повідомило видання The Record, Apple надсилає попередження вірменським користувачам телефонів про потенційні спроби злому з боку держави, ймовірно, пов'язані зі шпигунським програмним забезпеченням Pegasus. У зростанні кількості заражень шпигунським програмним забезпеченням Pegasus у Вірменії підозрюють уряд Азербайджану, як виявило розслідування CyberHUB, яке включає вірменських журналістів, активістів і урядовців. Кількість хакерських спроб зараження Pegasus у Вірменії зростає, ймовірно, через ескалацію конфлікту з Азербайджаном, однак справжні масштаби важко визначити через небажання жертв оприлюднювати інформацію, про те, що з ними сталося.

ЕКСПЕРТИ PALO ALTO NETWORKS ВИЯВИЛИ КИТАЙСЬКУ APT, ЯКА НАЦІЛЕНА НА УРЯД КАМБОДЖІ

7 листопада фахівці команди Unit 42 (Palo Alto Networks) поширили звіт, в якому розкривають деталі діяльності невідомої раніше китайської APT групи, яка маскує свою діяльність під хмарні служби резервного копіювання. За результатами аналізу телеметрію, фахівці роблять висновок, що діяльність зловмисної групи спрямована проти щонайменше 24 камбоджійських урядових організацій. Ця діяльність узгоджується з геополітичними цілями китайського уряду, оскільки він прагне використати свої міцні відносини з Камбоджею для розширення своїх військово-морських операцій у регіоні.

ГОЛОВНИЙ БАНК КИТАЮ ICBC ПОСТРАЖДАВ ВІД ПРОГРАМИ-ВИМАГАЧА

10 листопада стало відомо, що найбільший банк Китаю ICBC постраждав від програми-вимагача. Це призвело до збою в роботі систем фінансових послуг. За даними Financial Times, яка першою повідомила про цю історію, цей інцидент спричинив збій на ринках казначейства США. Як повідомляється, Асоціація індустрії цінних паперів і фінансових ринків США (SIFMA) повідомила своїм членам, що інцидент може перешкодити розрахункам за угодами від імені інших гравців ринку. Експерт з кібербезпеки Кевін Бомонт зробив припущення, що було використано програмне забезпечення Citrix Netscaler, в якому не була виправлена помилка CitrixBleed, яка дозволяє обходити автентифікацію.

ПРОПАЛЕСТИНСЬКА ГРУПА TA402 ВИКОРИСТОВУЄ IRONWIND ДЛЯ НАЦІЛЮВАННЯ НА ДЕРЖАВНІ УСТАНОВИ НА БЛИЗЬКОМУ СХОДІ

14 листопада фахівці компанії Proofpoint продемонстрували детальний аналіз діяльності групи TA402 (яку вони пов'язують із пропалестинськими хакерськими угрупованнями). Група TA402 бере участь у фішингових кампаніях, через які намагаються використати новий завантажувач початкового доступу під назвою IronWind. За завантажувачем слідували додаткові етапи, які складалися із завантаження шелл-коду. Діяльність групи зосереджена на державних установах Близького Сходу та в Північної Африки.

ЧИ Є DarkGate і PikaBot НОВИМ QakBot?

20 листопада компанія Confence оприлюднила звіт, в якому описала масштабну фішингову операцію зловмисного програмного забезпечення, яка почала розповсюджувати Dark-Gate у вересні та PikaBot у жовтні. Дослідники вважають, що ця кампанія є наступником операції QakBot, яка була закрита правоохоронними органами США в серпні 2023 року: «Нова кампанія, яка доставляє DarkGate і PikaBot, дотримується тієї ж тактики, що використовувалася у фішингових кампаніях QakBot. До них належать зламані потоки електронної пошти як початкове зараження, URL-адреси з унікальними шаблонами, які обмежують доступ користувачів, і ланцюг зараження, майже ідентичний тому, що ми бачили з доставленням QakBot. Сімейства шкідливих програм, що використовуються, також відповідають тому, що ми очікуємо від афілійованих QakBot», – йдеться у звіті.

ЯК БАГАТОЕТАПНІ ФІШИНГОВІ АТАКИ ВИКОРИСТОВУЮТЬ QR, CAPTCHA ТА СТЕГАНОГРАФІЮ

У статті, опублікованій The Hacker News 21 листопада, йдеться про те, що фішингові атаки неухильно стають все більш витонченими. Кіберзлочинці інвестують у нові способи обману жертв, щоб вони розкрили конфіденційну інформацію або встановили шкідливе програмне забезпечення. Одним з останніх трендів у фішингу є використання QR-кодів, CAPTCHA та стеганографії. Стаття розповідає, як вони здійснюються, і вчить їх виявляти.

RANSOMWARE RHYSIDA АТАКУВАЛО БРИТАНСЬКУ БІБЛІОТЕКУ

У повідомленні від 27 листопада наводяться дані про успішну атаку Ransomware Rhysida проти інформаційних систем Британської бібліотеки. Зловмисникам вдалось отримати значну кількість кадрової інформації за викуп якої вони вимагають 20 біткоїнів. Також було сильно пошкоджено інформаційну інфраструктуру установи, що майже припинило можливість користуватись вебсайтом, бездротовим доступом тощо.

УПРАВЛІННЯ СИГНАЛІВ АВСТРАЛІЇ (ASD) ОНОВИЛО НАЦІОНАЛЬНУ МОДЕЛЬ ESSENTIAL EIGHT MATURITY MODEL

27 листопада одна з ключових кібербезпекових агенцій Австралії Управління сигналів Австралії (ASD) оновило рекомендації щодо зменшення кіберризиків для компаній, включаючи графік застосування критичних виправлень і обмеження прав адміністратора. Ці зміни було внесено до Essential Eight Maturity Model – національної моделі, яка вперше була представлена в червні 2017 року. Її мета – створити базові вимоги кіберзахисту аби допомогти компаніям захистити свої IT-мережі, підключені до Інтернету від найбільш поширених кіберзагроз.

ЯПОНСЬКЕ КОСМІЧНЕ АГЕНТСТВО ЗАЗНАЛО КІБЕРАТАКИ

29 листопада Японське агентство космічних досліджень (JAXA) повідомило про кіберінцидент. JAXA закрила частину своєї мережі та розпочала повне розслідування, щоб визначити масштаби порушення та його наслідки. Агентство працює з центральним урядом, а також з поліцією з цього питання. Наразі кібератака на японське агентство аерокосмічних досліджень має всі ознаки того, що воно було діями спонсорованих державою акторів.

ДОСЛІДНИКИ ВИЯВИЛИ, ЩО БРОКЕРИ ДАНИХ ПРОДАЮТЬ СЕКРЕТИ ВІЙСЬКОВОСЛУЖБОВЦІВ США

6 листопада видання The Record оприлюднило результати дослідження, яке виявило, що брокери даних продають величезні обсяги надзвичайно конфіденційних даних про американських військовослужбовців. Дослідження цієї тривожної практики було проведено Стенфордською школою державної політики Університету Дюка, яка отримала значні обсяги даних від брокерів лише за 12 центів за військовослужбовця. Дані включають особисті дані, дані про здоров'я та фінанси військовослужбовців, ветеранів та їхніх родин.

Цей факт становить загрозу національній безпеці. Вороги можуть отримати ці дані та використовувати їх для різних цілей, таких як шантаж або компрометація військового персоналу. Наприклад, дані можуть виявити проблеми психічного здоров'я людини, особисті борги тощо, що може слугувати важелем для тиску.

Дослідники Duke висловили шок з приводу простоти отримання даних від брокерів і відсутності належної обачності з боку брокерів у перевірці своїх покупців і наголосили, що існує гостра потреба в законодавстві, яке б регулювало галузь брокерів даних.

ЗЛОВМИСНИЙ ПАКЕТ PYTHON ПРОДОВЖУЄ ТЕНДЕНЦІЮ АТАК НА РОЗРОБНИКІВ

Хакери, що атакують розробників програмного забезпечення з відкритим кодом, роблять це за допомогою оманливих пакетів, прихованих у бібліотеках відкритого коду, – повідомила фірма з кібербезпеки Checkmarx. Такі пакети створені так, щоб виглядати як правомірні інструменти, але містять приховані шкідливі сценарії.

Основне шкідливе програмне забезпечення, ідентифіковане Checkmarx, отримало назву BlazeStealer. Воно активується, щойно розробник запускає код і вводить бота в службу обміну повідомленнями Discord. Цей бот надає зловмисникам повний контроль над комп'ютером жертви, уможливлюючи все – від викрадання даних до прямого шпигунства.

Розробники Python, зокрема, стають привабливою мішенню для хакерів, особливо тих, хто намагається приховати свій код. Було виявлено, що фальшиві пакети, що починаються з «pyobf», здійснюють зловмисну діяльність. Важливо, що хакери тепер можуть використовувати програму цільової машини, щоб таємно робити скриншоти за допомогою вебкамери та надсилати їх назад, не залишаючи жодних слідів.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

ЄС ОЦІНИТЬ РИЗИКИ, СТВОРЕНІ ЧОТИРМА КЛЮЧОВИМИ ТЕХНОЛОГІЯМИ, І РОЗГЛЯНЕ ЕКСПОРТНИЙ КОНТРОЛЬ

Як 3 жовтня повідомило видання The Record, Європейський Союз до кінця року проведе оцінку ризиків, створених чотирма ключовими технологіями: штучним інтелектом (ШІ), блокчейном, квантовими обчисленнями та Інтернетом речей (IoT). Ця ініціатива є частиною ширших зусиль ЄС щодо посилення свого технологічного суверенітету та забезпечення безпеки критичної інфраструктури. Оцінка спрямована на виявлення потенційних загроз, вразливостей і стратегічних залежностей, пов'язаних із цими технологіями. Отримані результати сприятимуть розробці нормативно-правової бази та політики для зменшення ризиків і зміцнення позицій ЄС у світовому технологічному ландшафті. Цей крок відображає прагнення ЄС випереджати нові виклики в цифровій сфері та сприяти відповідальним і безпечним технологічним досягненням.

ЗНЕШКОДЖЕННЯ КІБЕРЗАГРОЗ ЗА ДОПОМОГОЮ ATT&CK: ВИГРАШНА КОМБІНАЦІЯ

У статті, опублікованій c4isrnet 2 жовтня, доктор Джорджіанна Ши та Фахад Абдулраззак обговорюють важливість використання фреймворку MITER ATT&CK як цінного інструменту для розуміння та протидії кіберзагрозам. Вони підкреслюють, як структура забезпечує комплексний і стандартизований підхід до класифікації та опису тактики, прийомів і процедур супротивника (TTP). Поєднуючи зусилля з кібербезпеки з ATT&CK, організації можуть покращити свої можливості аналізу загроз, їх виявлення та реагування. У статті йдеться про те, що включення ATT&CK в операції безпеки може забезпечити більш проактивний і ефективний захист від нових кіберзагроз

ОПИТУВАННЯ SAUCE LABS ПОКАЗУЄ: БІЛЬШІСТЬ РОЗРОБНИКІВ ПРОСУВАЮТЬ КОД У ВИРОБНИЦТВО БЕЗ ТЕСТУВАННЯ, ОБХОДЯТЬ ПРОТОКОЛИ БЕЗПЕКИ ТА ПОКЛАДАЮТЬСЯ НА CHATGPT

У статті, опублікованій Globenewswire 3 жовтня, обговорюються результати опитування Sauce Labs, які показують, що більшість розробників (67%) визнають, що просувають код у виробництво без належного тестування, в обхід протоколів безпеки (68%) та покладаються на такі інструменти, як ChatGPT, використовуючи згенерований код без тестування (60%). Опитування висвітлює занепокоєння щодо впливу на якість програмного забезпечення, безпеку та загальні процеси розробки.

Це вказує на те, що попри те, що розробники визнають важливість тестування, часові обмеження та вимога дотримуватись термінів часто призводять до недостатнього тестування. Застосування ChatGPT для завдань, пов'язаних із кодом, також викликає питання про вразливість системи безпеки та потребу в більш ретельному тестуванні та підході до забезпечення якості в робочих процесах розробки програмного забезпечення.

ЦИФРОВЕ ПІРАТСТВО ПОВЕРТАЄТЬСЯ В МОРЕ: ЗАХИСТ АВТОНОМНИХ КОРАБЛІВ ВІД ОНЛАЙН АТАК

У статті, опублікованій на ресурсі War on the Rocks 6 жовтня, Алекс Лі підкреслює, що оскільки морські судна стають більш автоматизованими та підключеними до мережі, вони стають уразливими до кіберзагроз, таких як хакерство, програми-вимагачі та витоки даних. Автор наголошує на потенційних наслідках кібератак на автономні кораблі, включаючи втручання в навігацію та крадіжку вантажу. У статті йдеться про те, що безпека морської цифрової інфраструктури має вирішальне значення для забезпечення безпечної та надійної роботи автономних кораблів. Він досліджує різні стратегії та технології для підвищення кібербезпеки в морській галузі, підкреслюючи важливість міжнародного співробітництва та нормативно-правової бази для вирішення нових викликів цифрового піратства на морі. На його думку, Міжнародна морська організація повинна випустити конкретні вказівки та стандарти для забезпечення безпеки великих автономних мереж, включаючи перелік унікально вразливих систем.

CISA, NSA, FBI, MS-ISAC ОПУБЛІКУВАЛИ ПОСІБНИК ІЗ ЗАПОБІГАННЯ ФІШИНГОВИМ ВТОРГНЕННЯМ

18 жовтня CISA, NSA, FBI, MS-ISAC опублікували «Інструкції з фішингу, зупинка циклу атак», щоб допомогти організаціям зменшити ймовірність і вплив успішних фішингових атак. Посібник має стати єдиним ресурсом, який допоможе всім організаціям захистити свої системи від фішингових загроз. Усі організації, від малого та середнього бізнесу до виробників програмного забезпечення, будуть заохочуватись ознайомитись з посібником, щоб краще зрозуміти методи фішингу і запровадити передові практики для зменшення ризику компрометації.

ЗМАГАННЯ ЗА КОНТРОЛЬ НАД ЦИФРОВОЮ ІНФРАСТРУКТУРОЮ БУДЕ МАТИ ВИЗНАЧАЛЬНИЙ ВПЛИВ НА ВІЙСЬКОВІ ОПЕРАЦІЇ – ЗВІТ RAND CORPORATION

30 жовтня RAND оприлюднив звіт щодо конкуренції між США та Китаєм за цифрову інфраструктуру (DI). На думку дослідників DI матиме вирішальне значення для військових сил та операцій, які покладаються на цю інфраструктуру під час конфліктів. Звіт надає аналіз альтернативного майбутнього того, як глобальний DI може розвиватися до 2050 року, а також якими можуть бути військові наслідки конкуренції навколо такої інфраструктури для Сполучених Штатів і Китаю. У звіті підкреслюється, що ступінь того, наскільки країна має право власності, доступу та контролю (OAC) над DI, може бути показником її спроможностей для військових операцій, а форми передача OAC над DI супротивнику (або не дружнім країнам) може стати асиметричним засобом розмивання військової переваги США в довгостроковій перспективі.

ПРОГНОЗ КІБЕРЗАГРОЗ У 2024 ВІД TRELLIX

30 жовтня кібербезпекова компанія Trellix оприлюднила свої оцінки року що минає, а також поділилась своїми прогнозами щодо кіберзагроз у 2024 році. Експерти виділяють три макрогрупи загроз:

- Загроза штучного інтелекту (підпільна розробка шкідливих LLM; відновлення Script Kiddies; голосове шахрайство для соціальної інженерії, створене ШІ).
- Зміна тенденцій у поведінці суб'єктів загрози (атаки ланцюга постачання на рішення для передачі файлів; зростання динаміки застосування програм-вимагачів; загрози виборчому процесу).
- Виникаючі загрози та методи атак (сплеск інсайдерських загроз; зростання кількості фішингових компаній з використанням QR-кодів; приховані атаки на периферійні пристрої; атаки на драйвери).

БРИТАНСЬКА NCSC НАДАЄ РЕКОМЕНДАЦІЇ ДЛЯ ПІДГОТОВКИ КОМПАНІЙ ДО ПОСТКВАНТОВОГО ШИФРУВАННЯ

3 листопада NCSC оприлюднила набір інструкцій, що мають допомогти власникам у комерційному секторі, державних організаціях та постачальникам критичної національної інфраструктури підготуватись до переходу на постквантову криптографію.

RAND ПРОПОНУЄ НОВІ ПІДХОДИ ДО ВИЗНАЧЕННЯ КІ НАЙВИЩИХ РІВНІВ КРИТИЧНОСТІ

20 листопада RAND поширив свою доповідь про системно важливі об'єкти (SIE) – OKI, які мають особливе значення для життєдіяльності країни та її національної безпеки. У звіті, зокрема, сформульовано критерії для визначення пріоритетного списку SIE – списку, який може дозволити CISA посилити управління ризиками, оптимізувати ресурси, відстежувати загрози та небезпеки та визначити пріоритети планування на підтримку ширшу національну стратегію багаторівневого стримування.

CISA ТА NCSC ВЕЛИКОБРИТАНІЇ ВИПУСТИЛИ СПІЛЬНІ РЕКОМЕНДАЦІЇ ЩОДО БЕЗПЕЧНОЇ РОЗРОБКИ СИСТЕМИ ШІ

26 листопада CISA спільно з NCSC Великобританії опублікували «Рекомендації щодо безпечної розробки систем ШІ». Рекомендації мають допомогти розробникам будь-яких систем, які використовують ШІ, приймати обґрунтовані рішення щодо кібербезпеки на кожному етапі процесу розробки. Керівні принципи були розроблені у співпраці з 21 іншою агенцією та міністерством з усього світу, включно з усіма членами Великої Сімки, і є першими такими Рекомендаціями узгодженими в усьому світі. Рекомендації розбиті на чотири ключові сфери: безпечний дизайн, безпечна розробка, безпечне розгортання та безпечна експлуатація та обслуговування. Кожен розділ висвітлює міркування та засоби пом'якшення, які допоможуть зменшити ризики кібербезпеки для процесу розробки.

ПРОГНОЗ КІБЕРЗАГРОЗ У 2024 РОЦІ ВІД PROOFPOINT

28 листопада кібербезпекова компанія Proofpoint оприлюднила свої прогнози щодо ландшафту кіберзагроз у 2024 році. До цих прогнозів увійшли: більший акцент на соціальну інженерію, використання зловмисниками генеративного ШІ, фішингові атаки через мобільні пристрої, атаки на облікові записи користувачів.

КІБЕРВІЙНА: ВЛАДА, ПРЕСТИЖ, МІЖНАРОДНЕ УПРАВЛІННЯ ТА СТРАТЕГІЯ В ЕПОХУ ГЛОБАЛЬНОЇ ПОЛІКРИЗИ

Стаття присвячена еволюції кібервійни, в ній підкреслюється роль кіберскладової у глобальних полікризах і стратегічні міркування для міжнародного управління. Автор підкреслює взаємодію між кіберможливостями, динамікою геополітичної потужності та гонитвою за престижем на глобальній арені. Автор наголошує на необхідності комплексної стратегії, яка б протистояла кіберзагрозам у контексті ширших міжнародних викликів, таких як політичні, економічні та соціальні кризи. У статті йдеться про те, що ефективне кіберуправління потребує багатовимірного підходу, який виходить за рамки технічних аспектів, беручи до уваги геополітичні наслідки та боротьбу за владу, яка формує сучасний світ.

КЕРІВНИК ВІДДІЛУ ШІ ПЕНТАГОНУ ЩОДО МЕРЕЖЕВО-ОРІЄНТОВАНОЇ ВІЙНИ, ВИКЛИКІВ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ

21 листопада видання Security Week розмістила інтерв'ю з головним спеціалістом Пентагону зі штучного інтелекту, Нандом Мульчандані, який обговорює теми, пов'язані з мережево-центричною війною та викликами генеративного штучного інтелекту. Мульчандані підкреслює необхідність мережевого підходу до ведення війни, використовуючи ШІ для покращення процесу прийняття рішень та координації між різноманітними військовими платформами. Він обговорює виклики та можливості, пов'язані із генеративним ШІ, підкреслюючи важливість етичних аспектів та відповідальної розробки штучного інтелекту в військовому контексті. Мульчандані також зачіпає зусилля Пентагону, спрямовані на співпрацю з партнерами з індустрії та академічного середовища для розвитку можливостей ШІ, забезпечуючи при цьому безпеку та стійкість перед еволюцією загроз.

НОВИЙ ПЛАН ЗБЕРЕЖЕННЯ КОНФІДЕНЦІЙНОСТІ ТА БЕЗПЕКИ В ІНТЕРНЕТІ

У статті Брюса Шнайєра та Барата Рагавана в IEEE Spectrum описується новий підхід до безпеки хмари під назвою «відокремлення», який може забезпечити кращу конфіденційність даних, що зберігаються в хмарі.

Шнайер і Рагаван пояснюють: «Що менше хтось знає, то менше він може наражати вас і ваші дані на небезпеку. У сфері безпеки це називається найменшим привілеєм. Принцип відокремлення застосовує цю ідею до хмарних сервісів, гарантуючи, при виконанні своєї роботи системи оперують якомога меншою кількістю інформації. Таким чином ми отримуємо безпеку та конфіденційність, розосереджуючи приватні дані, які сьогодні надмірно сконцентровані в одному місці.

Щоб гарантувати, що хмарні сервіси не вивчатимуть більше, ніж їм необхідно, і щоб порушення з боку одного з них не становило фундаментальної загрози нашим даним, нам потрібні два типи відокремлення. По-перше, це організаційне відокремлення: розподіл приватної інформації між організаціями таким чином, щоб ніхто не знав про все, що відбувається. По-друге, це функціональне відокремлення: розподіл інформації між рівнями програмного забезпечення. Ідентифікатори, які використовуються для автентифікації користувачів, наприклад, слід зберігати окремо від ідентифікаторів, які використовуються для підключення їхніх пристроїв до мережі.

5. КРИТИЧНА ІНФРАСТРУКТУРА

BITSIGHT ІДЕНТИФІКУЄ МАЙЖЕ 100 000 ПРОМИСЛОВИХ СИСТЕМ КЕРУВАННЯ, ВІДКРИТИХ ДЛЯ ПУБЛІЧНОГО ІНТЕРНЕТУ

2 жовтня компанія BitSight повідомила, що виявила майже 100 000 промислових систем керування, з прямим доступом до Інтернету, зокрема в освіті, технологіях, уряді та політиці та бізнес-секторах. Проте дослідники відзначають, що з 2019 року в цілому спостерігається постійне зниження кількості таких систем. Тож у певному сенсі це справді хороша новина.

BitSight додає: «Відкриті системи та пристрої, які обмінюються даними через протоколи Modbus і S7, стали більш поширеними в червні 2023 року, ніж раніше, причому поширеність першого зросла з 2020 року, а другого — з середини 2022 року. Однак, приблизно з 2021 року кількість незахищених промислових систем керування, які спілкуються через Niagara Fox, має тенденцію до зниження. Організації повинні знати про ці зміни в поширеності, щоб інформувати свої стратегії безпеки OT/ICS».

CISA РАЗОМ З ІНШИМИ УРЯДОВИМИ ОРГАНІЗАЦІЯМИ І ПРОМИСЛОВИМИ КОМПАНІЯМИ ОПРИЛЮДНИЛИ РЕКОМЕНДАЦІЇ ЩОДО БЕЗПЕКИ OT З ВІДКРИТИМ КОДОМ

10 жовтня CISA спільно з ФБР, АНБ і Міністерством фінансів США оприлюднили вказівки щодо «Покращення безпеки програмного забезпечення з відкритим кодом (OSS) у для OT та промислових систем управління (ICS)». Документ розроблений в межах ініціативи JCDC. Керівництво сприятиме кращому розумінню та висвітленню найкращих практик щодо безпечного використання OSS у середовищах OT/ICS. Настанови охоплюють:

- підтримку постачальників у розробці й обслуговуванні OSS;
- управління вразливостями;
- управління виправленнями;
- вдосконалення політики автентифікації та авторизації;
- визначення загальної структури, яка включатиме розробку та підтримку офісу програм із відкритим кодом.

ВИЯВЛЕНО 10 ZERO-DAY ВРАЗЛИВОСТЕЙ У ПРОМИСЛОВОМУ МАРШРУТИЗАТОРІ

11 жовтня кібербезпекова компанія Cisco Talos повідомила про виявлення 10 вразливостей нульового дня в промисловому стільниковому маршрутизаторі Yifan YF325. Зловмисники можуть використовувати ці вразливості для здійснення різноманітних атак, у деяких випадках отримуючи можливість виконувати довільні команди оболонки на цільовому пристрої. Yi-fan YF325 – це стільниковий термінальний пристрій, який пропонує можливості підключення до мережі Wi-Fi та Ethernet. Він широко використовується в галузях M2M, таких як індустрія терміналів самообслуговування, інтелектуальний транспорт, розумна мережа, промислова автоматизація, телеметрія, фінанси, POS, водопостачання, захист навколишнього середовища, пошта тощо.

NSA ОПРИЛЮДНИЛО РЕПОЗИТОРІЙ ОТ INTRUSION DETECTION SIGNATURE AND ANALYTICS

12 жовтня NSA опублікувало на GitHub репозиторій для ОТ – Intrusion Detection Signature and Analytics. Він має дозволити власникам критичної інфраструктури, організаціям оборонно-промислового сектору та організаціям систем національної безпеки ідентифікувати та виявляти потенційно зловмисну кіберактивність у своїх ОТ-середовищах.

У РОБОТІ ВЕЛИКИХ АВСТРАЛІЙСЬКИХ ПОРТІВ ВИНИКЛИ СУТТЄВІ ПЕРЕБОЇ ЧЕРЕЗ КІБЕРАТАКУ

13 листопада найбільший в Австралії контейнерний термінал і оператор ланцюга постачання DP World постраждав від кібератаки. У відповідь DP World відключила свої системи від Інтернету та припинила наземні операції в портах Сіднея, Мельбурна, Фрімантла та Брісбена. Роботу компанії було відновлено у той же день. Ні сама компанія, ні уряд Австралії не повідомили деталей атаки, але розслідування стосовно можливого виконавця триває. Компанія повідомила, що не отримувала вимоги викупу.

ЕЛЕКТРОМЕРЕЖА ЄВРОПИ ПЕРЕБУВАЄ ПІД ЗЛИВОЮ КІБЕРАТАК

Стаття у Politico від 23 листопада розглядає зростаючу загрозу у секторі енергетики, оскільки європейська енергетична мережа зіштовхується зі зростаючою кількістю кібератак. У нещодавньому звіті Міжнародного енергетичного агентства було виявлено, що середня щотижнева кількість кібератак на підприємства, що надають комунальні послуги, зросла більш ніж удвічі між 2020 і 2022 роками по всьому світу – минулого року було зареєстровано 1101 таку атаку. Ці атаки походять «зі сходу, від російської федерації та недемократичних країн». Атаки спрямовані на різні елементи енергетичного ланцюга, включаючи електростанції, системи розподілу електроенергії та інші критичні компоненти інфраструктури. Ситуація сигналізує про вразливість енергетичного сектору перед кіберзагрозами та підкреслює необхідність посилення заходів кібербезпеки для забезпечення цілісності та надійності європейської енергетичної мережі.

ЗЛОВМИСНИКАМ ВДАЛОСЬ АТАКУВАТИ НАСОСНЕ ОБЛАДНАННЯ ВОДООЧИСНОЇ СТАНЦІЇ

25 листопада спеціалізоване видання WaterWorld повідомило, що зловмисники вивели з ладу програмований логічний контролер (PLC) на одній зі станцій муніципального управління водопостачання в Аліквіппі, штат Пенсильванія. Зловмисники отримали доступ лише до насосів, які регулюють тиск на підвищених ділянках його покриття, і небезпеки для водопостачання не було. Постраждала підвищувальна станція управління контролює та регулює тиск, а також надає послуги водопостачання та водовідведення понад 6600 споживачам.

Атаку нібито здійснила підтримувана Іраном група Cyber Av3ngers у відповідь на триваючу війну між Ізраїлем і ХАМАС. Вважається, що зловмисники на муніципальне управління водопостачання Аліквіппи отримали доступ до закладу через Інтернет, використовуючи типові або слабкі паролі.

6. АНАЛІТИЧНІ ОЦІНКИ

СЕКТОР ОХОРОНИ ЗДОРОВ'Я ДЕМОНСТРУЄ СЛАБКИЙ ПРОГРЕС У ПОЛІПШЕННІ КІБЕРБЕЗПЕКИ – ДАНІ НОВОГО ЗВІТУ PONEMON

10 жовтня Інститут Ponemon оприлюднив свій звіт з оцінками впливу кіберзагроз на медичний сектор США. Згідно з його результатами, 88% медичних компаній зазнали в середньому 40 атак за останні 12 місяців. При цьому 66% сказали, що кібератаки, спрямовані на їхній бізнес, порушили лікування пацієнтів, а 23% помітили підвищення рівня смертності. Попри це автори звіту підкреслюють, що сектор охорони здоров'я дуже повільно реагує на зміни ландшафту кіберзагроз, хоча є помітна позитивна тенденція.

ЗАКОН ЄС ПРО КІБЕРСОЛІДАРНІСТЬ МАЄ ПОТЕНЦІАЛ, АЛЕ ПРОБЛЕМИ ПОТРІБНО ВИРІШУВАТИ

У статті, опублікованій виданням OODA Loop 16 жовтня, обговорюється Закон про кіберсолідарність Європейського Союзу (ЄС) та його потенційні наслідки. Закон про кіберсолідарність спрямований на посилення колективної реакції держав-членів ЄС на кіберінциденти шляхом сприяння обміну інформацією та співпраці. Стаття вказує на потенційні проблеми із законодавством, такі як проблеми, пов'язані з суверенітетом, довірою та координацією між державами-членами. У ньому підкреслюється необхідність ясності щодо ролі Агентства ЄС з кібербезпеки (ENISA) і створення основи для скоординованої відповіді на кіберзагрози. Попри потенційні переваги, у статті йдеться про те, що розв'язання цих проблем має вирішальне значення для Акту про кіберсолідарність для ефективного посилення стійкості кібербезпеки ЄС.

CISA ОПРИЛЮДНИЛА РЕКОМЕНДАЦІЇ ДЛЯ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ ЩОДО ЗМЕНШЕННЯ ЗАГРОЗ ВІД АТАК ЧЕРЕЗ ЛАНЦЮЖКИ ПОСТАЧАННЯ

23 жовтня CISA випустила посібник «Розширення можливостей малого та середнього бізнесу (SMB): ресурсний посібник для розробки стійкого плану управління ризиками в ланцюзі постачання». Цей невеликий 9-сторіноквий документ пропонує організаціям МСБ вісім простих кроків, які допоможуть їм ідентифікувати свої ланцюжки постачання мінімізувати можливі ризики пов'язані з ними.

CSIS ОПРИЛЮДНИЛА ЗВІТ З КОМПЛЕКСНИМ АНАЛІЗОМ СИТУАЦІЇ ІЗ ЗАХИСТОМ ФЕДЕРАЛЬНИХ МЕРЕЖ США

23 жовтня фахівці аналітичного центру CSIS оприлюднили майже 100-сторінкову доповідь про проблеми та перспективи захисту федеральних мереж уряду США. Документ охоплює оцінку наявної ситуації з розвитком сенсорної інфраструктури (проєкт EINSTAIN), обміну інформацією про інциденти, реагування на кіберінциденти, розвиток стійкості та навчання персоналу. Загальні виклики, з якими стикаються суб'єкти кібербезпеки включають:

- спроби розв'язати наявні проблеми шляхом механічного застосування нових рішень;
- не завжди ефективне використання наявних ресурсів;
- не завжди очевидні зони відповідальності урядових кіберсуб'єктів та інші.

ЗВІТИ ПРО МОЖЛИВІ БАГАТОМІЛЬЯРДНІ ВТРАТИ В НАСЛІДОК КІБЕРАТАК МОЖУТЬ БУТИ ШКІДЛИВИМИ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ – CISCO TALOS

26 жовтня експерт CIsco Talos Джонатан Маншоу порушив питання про те, чи справляють позитивний ефект різноманітні звіти, в яких оприлюднюються оцінки можливих світових втрат внаслідок кібератак. Він звертає увагу, що такі дані можуть мати навіть негативний ефект на сферу кібербезпеки, адже змушують людей почуватися переможеними – ніби немає сенсу намагатися змінити ситуацію, оскільки проблема настільки величезна, що один індивідуальний внесок все одно не матиме значення, тож тоді ми всі сидимо й нічого не робимо. Відповідно немає сенсу впроваджувати нові практики, якщо загроза наскільки катастрофічна.

КІЛЬКІСТЬ КІБЕРАТАК НА ІЗРАЇЛЬСЬКІ ЦІЛІ ЗРОСЛА НА 18% З ПОЧАТКУ ВІЙНИ

У матеріалі від 31 жовтня Гіл Мессінг, керівник штабу Check Point Software Technologies, підкреслив, що відповідно до наявних даних кількість кібератак на ізраїльські цілі зросла на 18% з початку війни й експерти очікують, що ця ситуація залишиться незмінною довгий час. Водночас більшість атак, які здійснюються хактивістами, що симпатизують ХАМАС, становлять DDoS атаки.

НІМЕЦЬКІ БЕЗПЕКОВІ ОРГАНІЗАЦІЇ ПОВІДОМЛЯЮТЬ ПРО ВИСОКИЙ РІВЕНЬ КІБЕРЗАГРОЗ

2 листопада Управління інформаційної безпеки Німеччини (BSI) представило свій звіт про стан IT та кібербезпеки в країні, який охоплює період з червня 2022 року по червень 2023 року. У звіті зазначено, що рівень загрози «вищий, ніж будь-коли раніше», зафіксувавши найвищий середній приріст типів зловмисного програмного забезпечення, а кількість жертв програм-вимагачів у Німеччині (чиї імена та отримані дані були опубліковані на сайтах витоку) також досягла історичного максимуму у другому кварталі – 65. Протягом звітного періоду BSI також зафіксував збільшення DDoS-атак з боку проросійських хактивістів.

ЗА РІК АМЕРИКАНСЬКІ ОРГАНІЗАЦІЇ ЗАПЛАТИЛИ 1,3 МЛРД ДОЛАРІВ ВИКУПУ ВНАСЛІДОК АТАК RANSOMWARE

3 листопада аналітичний центр CSIS провів експертну дискусію присвячену ransomware та Ініціативі Білого Дому щодо протидії ransomware. Під час свого виступу Енн Нойбергер, заступник помічника секретаря президента та заступник радника з національної безпеки з питань кібербезпеки та нових технологій, підкреслила, що проблема все ще залишається складною і американські компанії продовжують потерпати від ransomware. За її даними з середини 2022 року та середину 2023 року компанії заплатили 1,3 млрд доларів викупу внаслідок атак ransomware. На думку учасників дискусії виплати викупів підживлюють цей ринок, тому значна кількість зусиль має бути спрямована на ефективні інструменти стійкості та припинення виплати викупів зловмисникам.

ХМАРНІ ВРАЗЛИВОСТІ: СУЧАСНІ ТЕНДЕНЦІЇ ТА РИЗИКИ

14 листопада компанія Illumio опублікувала результати опитування щодо безпеки хмари, проведене Вансоном Борном, яке виявило, що «47% зломів за останній рік в досліджуваних організаціях виникли в хмарі».
Опитування виявило наступні недоліки як проблеми безпеки хмари, які найчастіше використовують:

- складність програм і робочих навантажень, а також величезне перекриття хмарних і локальних середовищ;
- різноманітність і величезна кількість послуг, які пропонують хмарні постачальники, наприклад IaaS, PaaS, контейнери та безсерверні обчислення;
- погана видимість усього вищезазначеного, включаючи нездатність визначити слабкі місця та проактивно забезпечити захист, а не просто реактивне блокування скомпрометованих систем.

БРИТАНСЬКА NCSC ОПРИЛЮДНИЛА РІЧНИЙ ЗВІТ ПРО ЛАНДШАФТ КІБЕРЗАГРОЗ. ОСНОВНИЙ ФОКУС – APT ЗАГРОЗИ ОКІ

14 листопада британський NCSC оприлюднив свій щорічний звіт з оглядом стану кібербезпеки країни та основними тенденціями щодо кіберзагроз британським організаціям. Ключовий висновок – OKI зіштовхуються із «тривалою та значною загрозою» на тлі зростання сил державних угруповань, зростання загальної агресивної кіберактивності та нових геополітичних викликів. Основні сектори, які знаходяться під атакою, – водного забезпечення, електроенергетика, зв'язок, транспорт, фінансова система, а також доступ до Інтернету. Також підкреслюється, що протягом останніх 12 місяців NCSC спостерігав за появою нового класу кіберсупротивників у формі державних акторів, які часто симпатизують подальшому вторгненню росії в Україну, та мають ідеологічну, а не фінансову мотивацію.

ЛАНДШАФТ ЗАГРОЗ У СЕКТОРІ РОЗДРІБНИХ ПОСЛУГ У 2023 РОЦІ ВІД TRUSTWAVE THREAT INTELLIGENCE

15 листопада Trustwave Threat Intelligence опублікувала власну оцінку ландшафту загроз у секторі роздрібних послуг у 2023 році. Експерти виділяють шість елементів, притаманних електронній роздрібній торгівлі які є і сильними сторонами, і одночасно загрозами:

- електронна комерція: електронна комерція зберігає велику кількість конфіденційних даних клієнтів, таких як номери кредитних карток і адреси доставлення;
- вразливості ланцюга постачань: складна мережа постачальників, партнерів з логістики та дистриб'юторів може створювати численні точки вразливості;
- сезонність: Сезонність може ускладнити підтримку стандартів безпеки та відповідності;
- багатоканальність: багатоканальний підхід забезпечує зручність для клієнтів, але ускладнює безпеку;
- поширеність подарункових карток: зловмисники використовують подарункові картки для збереження анонімності своїх транзакцій і для відмивання коштів, отриманих зі зламаних кредитних карток та інших платіжних платформ;
- модель франшизи: порушення безпеки в одній франшизі може завдати шкоди репутації всього бренду.

КОМПАНІЯ KROLL ОПУБЛІКУВАЛА ЗВІТ ПРО ЛАНДШАФТ ЗАГРОЗ ЗА ТРЕТІЙ КВАРТАЛ 2023 РОКУ

15 листопада опублікувала звіт, в якому розповіла, що у третьому кварталі 2023 року соціальна інженерія у багатьох її формах посідала центральне місце. У цьому кварталі «злом людей» перетворився з давньої проблеми безпеки на обраний метод загрозливих акторів. «Про це свідчать наші спостереження за драматичною ескалацією тактик соціальної інженерії зі значним збільшенням фішингу, смішингу, дійсних облікових записів, голосового фішингу та інших тактик, що додало найбільшої кількості інцидентів, які ми бачили у 2023 році,» – йдеться у звіті.

ІНВЕСТИЦІЇ В КІБЕРБЕЗПЕКУ ОКІ В ЄС ЗРОСТАЮТЬ ДУЖЕ НЕЗНАЧНИМИ ТЕМПАМИ – ЗВІТ ENISA

16 листопада ENISA оприлюднила новий звіт, в якому досліджується динаміка інвестицій в кібербезпеку з боку операторів критичної інфраструктури відповідно до вимог NIS Директиви. Серед ключових висновків – хоча кіберчастка IT-бюджету OKI досягла 7,1% у 2022 році, однак це лише на 0,4% більше ніж у 2021. Крім того, 47% OKI не планують наймати фахівців з кібербезпеки протягом наступних двох років, при цьому 83% організацій стверджують, що мають труднощі з наймом принаймні в одній сфері інформаційної безпеки. Дослідження охопило 1080 операторів основних послуг (OES) і постачальників цифрових послуг (DSP) з усіх 27 держав-членів ЄС. Всі дані стосуються 2022 року.

ВІДНОВЛЕННЯ ROYAL MAIL ПІСЛЯ АТАКИ ПРОГРАМ-ВИМАГАЧІВ КОШТУВАТИМЕ ЩОНАЙМЕНШЕ 12 МІЛЬЙОНІВ ДОЛАРІВ

16 листопада стало відомо, що International Distributions Services (материнська компанія Royal Mail) витратить на відновлення компанії після атаки ransomware LockBit 12,4 мільйона доларів США. Орієнтовні втрати, яких зазнала компанія через саму кібератаку склала 27 мільйонів доларів. Зловмисники вимагали викупу у 80 млн доларів, які компанія відмовилась виплачувати.

АРГУМЕНТИ У ПІДТРИМКУ СТВОРЕННЯ КІБЕРСИЛ

У статті, опублікованій 17 листопада, начальник відділу оборонних інформаційно-комунікаційних технологій Генерал-майор Мюррей Томпсон обговорює важливість і необхідність створення спеціальних кіберсил у складі Австралійських сил оборони (ADF). У ньому наголошується на зростаючих кіберзагрозах, з якими стикаються країни в усьому світі, і на необхідності створення спеціалізованого військового підрозділу для ефективного вирішення цих викликів. Запропоновані Cyber Force будуть відповідати за проведення кібероперацій, захист від кіберзагроз і підтримку інших військових підрозділів. У статті підкреслюється важливість інтеграції кіберспроможності в більш широку оборонну стратегію для забезпечення національної безпеки в умовах розвитку кіберзагроз. Він також підкреслює потенційну співпрацю з міжнародними союзниками для зміцнення колективних зусиль у сфері кібербезпеки.

КІЛЬКІСТЬ КІБЕРАТАК НА ЕНЕРГЕТИЧНИЙ СЕКТОР ЄС СТРІМКО ЗРОСТАЄ

У статті «Електромережа Європи перебуває під потопом кібератак» від 27 листопада вказується на стрімке зростання кількості атак на енергетичну мережу ЄС. У звіті Міжнародного енергетичного агентства було виявлено, що середня кількість кібератак на комунальні послуги щотижня зросла більш ніж удвічі між 2020 і 2022 роками в усьому світі – минулого року було зареєстровано 1101 щотижневу атаку. Проблема полягає в тому, що деякі операційні системи, які використовуються в європейських мережах, використовуються близько 40 років. Відповідно їх «дуже важко виправити», якщо виникне проблема.

КУЛЬТУРА ТА ФОРМУВАННЯ КІБЕРМОЖЛИВОСТЕЙ ІЗРАЇЛЮ

27 листопада було оприлюднено рецензію на книгу «Ізраїль та кіберзагрози» Ч.Фрейліча (Charles D. Freilich), М.Коена (Matthew S. Cohen) та Г.Сібоні (Gabi Siboni). У книзі обстоюється думка, що Ізраїль став провідною кібердержавою завдяки поєднанню необхідності та стратегічної культури. Наголошується на політичних факторах і процесах прийняття рішень, які сформували підхід Ізраїлю до можливостей і проблем, пов'язаних із технологічними змінами. Автори надають поглиблений аналіз кіберстратегії та можливостей Ізраїлю, досліджуючи його роль у кіберконфлікті та відповідь на нього в історичному та регіональному контекстах.

9-Й ЩОРІЧНИЙ ЗВІТ SONATYPE ПРО СТАН ЛАНЦЮГА ПОСТАЧАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ РОЗКРИВАЄ ШЛЯХИ ПОКРАЩЕННЯ ЕФЕКТИВНОСТІ РОЗРОБНИКІВ І DEVSECOPS

9-й щорічний звіт про стан ланцюга постачання програмного забезпечення від Sonatype, опублікований 3 жовтня, зокрема, містить інформацію, що у 2023 році було вдвічі більше таких атак, ніж у 2019-2022 роках разом узятих. Sonatype виявила 245 032 шкідливих пакетів у 2023 році.

Майже всіх (96%) вразливостей можна уникнути, адже на 2,1 мільярда завантажень відкритого програмного забезпечення (OSS) із відомими вразливими місцями у 2023 році була доступна краща виправлена версія – такий же відсоток, як у 2022 році. На кожне неоптимальне оновлення компонента припадає зазвичай 10 доступних виправлених версій.

Лише 11% проєктів з відкритим кодом «активно обслуговуються».
У звіті обговорюється широке використання контейнерів і вплив безпеки ланцюга постачання на організації і наголошується на необхідності постійного моніторингу, оцінки ризиків та усунення вразливостей у ланцюжку постачання програмного забезпечення. Крім того, звіт надає рекомендації для організацій щодо покращення практики розробки програмного забезпечення та забезпечення безпеки перед обличчям нових викликів.

БЕЗПЕКА В ЕПІЦЕНТРІ ІННОВАЦІЙ: ЦЕ НЕ ТОЙ СВІТ, У ЯКОМУ МИ ЖИВЕМО СЬОГОДНІ, АЛЕ ЩО, ЯКБИ ЦЕ БУЛО?

Компанія PwC опублікувала опитування Global Digital Trust Insights Survey за 2024 рік, яке виявило, що, попри те, що хмарні атаки є головною проблемою в кібернетичному просторі, близько третини організацій не мають плану управління ризиками для розв'язання проблем постачальників хмарних послуг». Крім того, «понад 30% компаній не дотримуються стандартних практик кіберзахисту».

В опитуванні також йдеться: «Близько третини цьогорічних респондентів погоджуються, що чотири типи регулювання будуть найважливішими для забезпечення майбутнього зростання їхньої організації – регулювання штучного інтелекту (37%), гармонізація законів про кібернетифікацію та захист даних (36%), обов'язкове звітування про управління кіберризиками, стратегію та управління (35%) і вимоги до операційної стійкості (32%)».

СТАН ПРОГРАМ-ВИМАГАЧІВ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я

Компанія Sophos опублікувала звіт, присвячений програмам-вимагачам в галузі охорони здоров'я, виявивши, що зловмисникам вдалося зашифрувати дані під час майже трьох чвертей атак: «Це найвищий рівень шифрування за останні три роки, і він становить значне зростання порівняно з 61% організацій охорони здоров'я, які повідомили минулого року, що їхні дані зашифровані». У 37% успішних атак злочинці також викрали дані. Зламані облікові дані були найпоширенішою причиною атак програм-вимагачів у секторі.

Дослідники також виявили, що «організаціям охорони здоров'я тепер потрібно більше часу, щоб відновитися: 47% відновлюються за тиждень, порівняно з 54% минулого року». Крім того, у звіті зазначається: «Кількість опитаних медичних організацій, які сплатили викуп, зменшилася з 61% минулого року до 42% цього року. Це нижче середньогалузевого показника (46%).

ЗВІТ ПРО ГЛОБАЛЬНІ ЗАГРОЗИ У ТРЕТЬОМУ КВАРТАЛІ ВІД BLACKBERRY

BlackBerry опублікувала звіт про глобальну розвідку загроз за третій квартал 2023 року, зазначивши збільшення кількості унікальних зразків зловмисного програмного забезпечення на 70% порівняно з попереднім кварталом. Галузь фінансових послуг залишається найбільш атакованим сектором.

Країни, які найбільше піддаються кібератакам: Сполучені Штати, Канада, Японія, Перу, Індія.

Індустрія охорони здоров'я також стикнулася зі зростанням кількості унікальних атак зловмисного програмного забезпечення на 181%.

СТАН СЕГМЕНТАЦІЇ 2023 – ЗВІТ AKAMAI

У звіті Akamai «2023 State of Segmentation» досліджується поточний стан сегментації мережі та її вплив на кібербезпеку. Отримані результати показують, що організації зіштовхуються з труднощами при впровадженні ефективних стратегій сегментації, пов'язаними зі складністю, недостатньою видимістю та використанням застарілих інструментів. У звіті підкреслюється важливість динамічної сегментації на основі ідентичності для підвищення безпеки. Він підкреслює потребу організацій у переоцінці та модернізації своїх підходів до сегментації, щоб адаптуватися до нових кіберзагроз і ефективно захистити конфіденційні дані.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

УКРАЇНА ТА ENISA ПІДПИСАЛИ РОБОЧУ УГОДУ ПРО СПІВПРАЦЮ

13 листопада ENISA та Україна (в особі НКЦК при РНБО України та Держспецзв'язку) уклали Робочу угоду. Угода передбачає співпрацю по низці напрямків: підвищення обізнаності та розбудова потенціалу для посилення кіберстійкості; обмін найкращими практиками для забезпечення гармонізації законодавства та імплементації (серед іншого – NIS2 у кіберсфері, а також у таких секторах, як телекомунікації та енергетика); обмін знаннями та інформацією щодо ландшафту загроз кібербезпеці для підвищення загальної обізнаності про ситуації тощо. Це перша для ENISA робоча домовленість з партнером з-поза меж ЄС.

НКЦК ПРОВІВ МІЖНАРОДНЕ ЗАСІДАННЯ НАЦІОНАЛЬНОГО КЛАСТЕРА КІБЕРБЕЗПЕКИ У ПРАЗІ

Національний координаційний центр кібербезпеки при РНБО України спільно з CRDF Global в Україні та за підтримки Державного департаменту США 26 жовтня 2023 року у Празі провів міжнародне засідання Національного кластера кібербезпеки «Державно-приватне партнерство на міжнародному рівні та запровадження кібердипломатії».

Під час дискусійних панелей учасники заходу обговорили кілька тем. Серед них – досвід України та провідних країн світу у кібервійні; розвиток кібердипломатії в Україні та світі; державно-приватне партнерство для забезпечення глобальної стійкості у кіберпросторі.

УКРАЇНА ПІДПИСАЛА ДЕКЛАРАЦІЮ БЛЕТЧЛІ З БЕЗПЕКИ ШТУЧНОГО ІНТЕЛЕКТУ

2 листопада Україна під час AI Safety Summit, у якому взяли участь представники 29 урядів, зокрема США, Австралії та ЄС, підписала декларацію Блетчлі з безпеки штучного інтелекту. Одна з головних цілей декларації – колективна домовленість країн щодо розробки та імплементації ризикоорієнтованих політик регулювання ШІ, які б унеможливлювали негативні наслідки. Водночас на саміті наголосили, що штучний інтелект є корисною технологією для економічного зростання та сталого розвитку.

УКРАЇНСЬКА ВІЙСЬКОВА РОЗВІДКА ПРОВЕЛА ПЕРШУ НАСТУПАЛЬНУ КІБЕРОПЕРАЦІЮ

23 листопада Головне управління розвідки Міністерства оборони України повідомило про проведення успішної спеціальної операції у кіберпросторі проти «федерального аґєнтства воздушного транспорта» («росавіація»). Внаслідок операції вдалось здобути великий обсяг закритих службових документів росавіації. Серед отриманих внаслідок зламу даних — перелік щодобових звітів «росавіації» у масштабах всієї рф за понад півторарічний період. Це перший випадок, коли українська безпекова структура повідомляє про проведення наступальної операції в кіберпросторі.

НКЦК ЗА ПІДТРИМКИ JICA ПРОВІВ ЧОТИРИДЕННІ ІНТЕГРОВАНІ КІБЕРНАВЧАННЯ HACKWAVE 2023

Національний координаційний центр кібербезпеки при РНБО України за підтримки Японського агентства міжнародного співробітництва (JICA) та CRDF Global в Україні провів 26-29 вересня чотириденні інтегровані кібернавчання Hackwave 2023 для представників держсектору та об'єктів критичної інфраструктури. Головною метою Hackwave 2023 було комплексне вдосконалення фахівцями своїх знань та навичок у виявленні та реагуванні на кібератаки, а також оцінка готовності до кібератак.

Це перші кібернавчання в Україні, де одночасно змагались команди фахівців у сфері кібербезпеки, менеджменту та комунікаційників.

НА IGF 2023 УКРАЇНА ЗАКЛИКАЛА ДО СИСТЕМАТИЧНОГО ДОКУМЕНТУВАННЯ РОСІЙСЬКИХ ВОЄННИХ ЗЛОЧИНІВ ІЗ ВИКОРИСТАННЯМ ЕЛЕКТРОННИХ ДОКАЗІВ

У жовтні 2023 року Секретар НКЦК Наталія Ткачук під час участі у Міжнародному форумі з управління Інтернетом (IGF 2023) наголосила на тому, що окрім перемоги над ворогом та відбудови України важливою задачею є притягнення до відповідальності всіх воєнних злочинців рф, винних у злодіяннях, що відбуваються в Україні: «З початку агресії російської федерації правоохоронними органами України зареєстровано понад 100 тисяч воєнних злочинів. Це безпрецедентна цифра, що потребує залучення до процесу їх документування всього громадянського суспільства та світової спільноти, і методи OSINT та використання електронних доказів є важливим інструментом».

IGF проводиться під егідою ООН. Цього року він об'єднав понад 5000 учасників зі 175 країн.

У КИЄВІ ВІДБУЛАСЯ ЗУСТРІЧ КЕРІВНИЦТВА МІНОБОРОНИ З ВІЙСЬКОВИМИ АТАШЕ В РАМКАХ ІТ-КОАЛІЦІЇ

Під головуванням Міністра оборони Рустема Умєрова у Києві відбулася зустріч з військовими аташе в рамках ІТ-коаліції. Участь у заході взяли представники понад 30 країн-учасниць Контактної групи з питань оборони України. Міністр оборони України наголосив на тому, що війну виграють технології. Також учасникам зустрічі обґрунтували першочергові потреби, які Україна розраховує отримати від учасників ІТ-коаліції.

ЗАСТУПНИК СЕКРЕТАРЯ РНБОУ СЕРГІЙ ДЕМЕДЮК: НАМ ПОТРІБНО СТВОРИТИ ЄДИНУ СИСТЕМУ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ

31 жовтня заступник Секретаря Ради національної безпеки і оборони України Сергій Демедюк під час заходу на базі Академії СБУ зазначив, що Україна гостро потребує єдиної системи розслідування кіберінцидентів. Це обумовлено тим, що хоча Україна навчилась ефективно проводити експертизу цифрових доказів, однак процес їх збору та документування залишається проблемою. Це, своєю чергою, ускладнює процес розслідування зловмисної діяльності російських хакерів, а також військових злочинів російської федерації.

УКРАЇНА ПОТРЕБУЄ СТВОРЕННЯ КІБЕРСИЛ ТА УХВАЛЕННЯ ВІДПОВІДНОЇ КОНЦЕПЦІЇ СТВОРЕННЯ КІБЕРСИЛ УКРАЇНИ – НАТАЛІЯ ТКАЧУК (НКЦК)

10 листопада секретар НКЦК при РНБО України Н. Ткачук під час міжвідомчого заходу щодо «Забезпечення кібероборони держави» підкреслила необхідність якнайшвидшого створення українських кіберсил на основі досвіду України та успішних міжнародних кейсів. Першим кроком на цьому шляху має стати розробка та затвердження Концепції створення кіберсил України.

ЗАСТУПНИК МІНІСТРА ОБОРОНИ КАТЕРИНА ЧЕРНОГОРЕНКО ПРОВЕЛА ЗУСТРІЧ З ДЕЛЕГАЦІЄЮ ІНСТИТУТУ МИРУ США

Заступник Міністра оборони України з питань цифрового розвитку, цифрових трансформацій і цифровізації Катерина Черногоренко зустрілася з делегацією американського Інституту миру (USIP) на чолі з Віцепрезидентом, Послом США в Україні (2006-2009) паном Вільямом Тейлором. Сторони обговорили питання ефективності військової допомоги Україні від країн-партнерів, налагодження співробітництва в технологічній сфері, перспективи створення коаліції співпраці в інженерній сфері, а також цифровізації процесів послуг для ветеранів війни.

ФАХІВЦІ НКЦК ПРОВЕЛИ РОБОЧУ ЗУСТРІЧ З ПРЕДСТАВНИКАМИ ПОСОЛЬСТВА КОРОЛІВСТВА ДАНІЯ В УКРАЇНІ

Керівник управління забезпечення діяльності НКЦК Апарату РНБО України Сергій Прокопенко 3 листопада 2023 року зустрівся із представниками Посольства Королівства Данія в Україні. Обговорили шляхи поглиблення практичного співробітництва у сфері протидії кібератакам, обміну інформацією, а також подальше партнерство в освітніх проєктах.

МІНЦИФРА ТА IFES ПІДПИСАЛИ МЕМОРАНДУМ ПРО СПІВПРАЦЮ

Міністерство цифрової трансформації та Міжнародна фундація виборчих систем України (IFES) уклали меморандум про співробітництво. Це допоможе посилити кібербезпеку, сприятиме цифровому розвитку нашої держави, а також дасть змогу впровадити інноваційні технології для покращення виборчих процесів України та приведення їх у відповідність до міжнародних стандартів.

ДЕРЖСПЕЦЗВ'ЯЗКУ РОЗПОЧАЛА СПІВПРАЦЮ ЗІ СЛУЖБОЮ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА КІБЕРБЕЗПЕКИ РЕСПУБЛІКИ МОЛДОВА

Адміністрація Державної служби спеціального зв'язку та захисту інформації України та Служба інформаційних технологій та кібербезпеки Республіки Молдова уклали Меморандум про взаєморозуміння у сфері кіберзахисту. Серед напрямів співпраці, передбачених Меморандумом:

- сприяння створенню двосторонніх каналів інформування між CERT-UA та Центром кібербезпеки CERT-GOV-MD для виявлення загроз у кіберпросторі та реагування на них;
- обмін інформацією про кіберінциденти, кібератаки та кіберзагрози;
- обмін досвідом і передовими практиками у сфері кіберзахисту тощо.

НКЦК ПРОВІВ ДВОДЕННІ ЗМАГАННЯ З КІБЕРБЕЗПЕКИ INCIDENT RESPONSE DAYS 2.0

16 та 17 жовтня 2023 року НКЦК спільно з CRDF Global в Україні провели дводенні кіберзмагання INCIDENT RESPONSE DAYS 2.0, у яких взяли участь понад сто профільних фахівців державного сектору, об'єднаних у 22 команди. Захід поєднав у собі змагання з кібербезпеки та тренінги щодо кібероперацій, реагування на кіберінциденти та форензіки. Протягом 6 годин учасники працювали за унікальним сценарієм, розслідували інциденти, збирали артефакти та аналізували шкідливе програмне забезпечення. Всього у навчаннях взяли участь 100 фахівців. Також учасники відпрацьовували питання комунікацій між представниками суб'єктів забезпечення кібербезпеки та державними органами.

В УКРАЇНІ ВІДБУЛИСЬ СЕКТОРАЛЬНІ КІБЕРНАВЧАННЯ ДЛЯ ТРАНСПОРТНОГО СЕКТОРУ CIREX.COBRIDGE

20 жовтня Держспецзв'язку та Проєкт USAID «Кібербезпека критично важливої інфраструктури України» провели навчання CIREX.CoBridge у форматі TTX (tabletop exercises), присвячені захисту об'єктів критичної інфраструктури від фізичних та кібератак. У заході взяли участь представники центральних органів влади та об'єктів критичної інфраструктури у сфері транспорту, органів цивільного захисту, правоохоронних органів. Навчання розроблені на базі методичних рекомендацій Агентства США з питань кібербезпеки та захисту інфраструктури (CISA).

СЕКРЕТАР НКЦК НАТАЛІЯ ТКАЧУК: ДЛЯ ВДОСКОНАЛЕННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ ПОТРІБНО ІМПЛЕМЕНТУВАТИ СТАНДАРТИ НАТО ТА ЄС

23 листопада 2023 року під час заходу для представників основних суб'єктів забезпечення кібербезпеки в Україні на тему: «Забезпечення кібербезпеки та стійкості шляхом покращення міжвідомчої взаємодії» секретар НКЦК при РНБО України Н. Ткачук наголосила на необхідності вивчення та імплементації в Україні стандартів та політик НАТО та Євросоюзу.

Під час семінару профільні фахівці держсектору ознайомились з найважливішими нормами із забезпечення безпеки та кіберстійкості на європейському та євроатлантичному рівнях. Розглянуто механізми, за допомогою яких відповідні правові норми та технічні рішення можна перенести в український контекст для забезпечення кіберстійкості України.

ПОНАД 20 ТИСЯЧ ГЛЯДАЧІВ ДОЛУЧИЛИСЯ ДО ВСЕУКРАЇНСЬКОГО ОНЛАЙН-УРОКУ З КІБЕРБЕЗПЕКИ

31 жовтня, Держспецзв'язку за підтримки Інституту спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського провели всеукраїнський онлайн-урок «Я. Безпека. Кіберпростір». Серед основних тематик – як убезпечитися від хакерів, інтернет-шахраїв, кібербулінгу та кібергрумінгу, розрізняти шкідливий і неетичний контент тощо.

ПРЕДСТАВНИК НКЦК ВЗЯВ УЧАСТЬ У НАВЧАННЯХ З КІБЕРДИПЛОМАТІЇ GCMC

Керівник управління забезпечення діяльності НКЦК профільної служби Апарату РНБО України Сергій Прокопенко 25-29 вересня 2023 року взяв участь у навчаннях з кібердипломатії George C. Marshall European Center for Security Studies, які проводились спільно з Держдепартаментом США. У заході взяли участь майже 30 учасників з країн Європи та США. В ході навчань обговорювалися ключові аспекти розвитку спроможностей у сфері кібербезпеки, роль кібердипломатії в міжнародній безпеці та національні підходи до реагування на кібератаки.

ДЕРЖСПЕЦЗВ'ЯЗКУ СПІЛЬНО З НКЦК ПРОВЕЛИ СЕМІНАР-ПРАКТИКУМ, ПРИСВЯЧЕНИЙ РЕАЛІЗАЦІЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ

9-10 жовтня Держспецзв'язку спільно з Національним координаційним центром кібербезпеки при РНБО України провели семінар-практикум, присвячений реалізації Стратегії кібербезпеки України. Відповідно до цілей та завдань заходу обговорили механізми, аспекти, роль та особливості щорічного планування заходів із реалізації Стратегії та зосередилися на важливості підготовки звітності за результатами їх виконання.

МІНЦИФРА РАЗОМ З ПРОЄКТОМ USAID «КІБЕРБЕЗПЕКА КРИТИЧНО ВАЖЛИВОЇ ІНФРАСТРУКТУРИ УКРАЇНИ» ЗАПУСТИЛИ НОВИЙ НАВЧАЛЬНИЙ СЕРІАЛ ПРО КІБЕРБЕЗПЕКУ НА ДІЯ.ОСВІТА

Мінцифра разом з Проєктом USAID «Кібербезпека критично важливої інфраструктури України» та за участі фахівців Києво-Могилянської академії створила освітній серіал, який допоможе навчитися кібергігієни та вберегти себе від кіберзагроз. У серіалі йдеться про мотиви кіберзлочинців, відповідальність громадян за власні гаджети, паролі, безпеку програмного забезпечення, психологію кібершахрайства та віруси.

GOOGLE РАЗОМ З ПАРТНЕРАМИ ЗАПУСТИВ НАВЧАЛЬНИЙ КУРС «ОСНОВИ КІБЕРБЕЗПЕКИ ДЛЯ ПІДПРИЄМЦІВ»

Навчальний курс корисний для власників, керівників і співробітників малого та середнього бізнесу, які хочуть захистити свій бізнес від кіберзагроз. Він складається із 5 навчальних тренінгів і охоплюють такі теми:

- розпізнавання кібератак;
- створення системи захисту свого бізнесу від кіберзагроз;
- методи дотримання співробітниками кібергігієни;
- розробка стратегії й тактики підвищення безпеки бізнесу;
- досвід українського підприємця у побудові ефективної системи кібербезпеки.

ЗРОСЛА КІЛЬКІСТЬ РОСІЙСЬКИХ КІБЕРАТАК З ВИКОРИСТАННЯМ SMOKELOADER – ДОСЛІДЖЕННЯ НКЦК

24 жовтня НКЦК оприлюднило своє дослідження російської кіберактивності із використанням шкідливого програмного забезпечення Smokeloader. За даними НКЦК з травня 2023 року українські фінансові та державні організації були атаковані російськими зловмисниками з використанням Smokeloader - програмного забезпечення, функціонал якого включає методи протидії аналізу, викрадення даних та віддаленого керування комп'ютером жертви. Зловмисники використовують фінансову тематику при формуванні кампаній для заманювання та обману жертв.

ДЕРЖСПЕЦЗВ'ЯЗКУ ПЕРЕДБАЧАЄ ЗРОСТАННЯ КІЛЬКОСТІ СКЛАДНИХ АТАК НА ЛАНЦЮЖКИ ПОСТАЧАННЯ

30 жовтня Держспецзв'язку оприлюднила новий аналітичний звіт про російські кібероперації. Фахівці Держспецзв'язку передбачають зростання кількості складних атак на ланцюжки постачання. Компанії, які розробляють програмне забезпечення для критичної інфраструктури та військових, зазнаватимуть активних цілеспрямованих кібернападів у довгостроковій перспективі. Зловмисники, ймовірно, використовуватиме більш комплексні атаки та інструменти, включно з розробкою і розгортанням дуже складного шкідливого програмного забезпечення, яке має ширше розповсюдження, здатне атакувати різні операційні системи. Також підкреслено, що росія залучає дедалі більшу кількість нових людей для нападів у кіберпросторі, зокрема, молодь. Ще один важливий висновок – хакери, пов'язані із військовою розвідкою рф, роблять акцент на складності атак, а не на кількості.

APT29 АТАКУВАЛИ ПОСОЛЬСТВА ПО ВСІЙ ЄВРОПІ – ЗВІТ НКЦК

14 листопада НКЦК оприлюднив звіт про активність кібершпигунського угруповання APT29. Досліджувана операція APT29 стосується їх операції проти посольств по всій Європі, включаючи Італію, Грецію, Румунію, Азербайджан. Основний інструмент угрупування – нещодавно виявлена вразливість з індикатором CVE-2023-38831, що стосується програмного забезпечення WinRAR. APT29 використовує нешкідливі, на перший погляд, приманки, які надають зловмисникам доступ до систем жертв.

КІЛЬКІСТЬ ЗАРЕЄСТРОВАНИХ КІБЕРІНЦИДЕНТІВ У ПЕРШОМУ ПІВРІЧЧІ 2023 РОКУ ЗРОСЛА БІЛЬШЕ НІЖ УДВІЧІ – ДЕРЖСПЕЦЗВ'ЯЗКУ

13 жовтня Держспецзв'язку оновила статистичну інформацію щодо динаміки кіберінцидентів. У першому півріччі 2023 року CERT-UA, яка діє при Держспецзв'язку, зареєструвала 762 кіберінциденти (без урахування інцидентів SOC). Тобто у середньому ворожі хакери намагалися атакувати українські інформаційно-комунікаційні системи чотири-п'ять разів на добу. Для порівняння – протягом другого півріччя 2022 року були зареєстровані 342 (без урахування інцидентів SOC), у середньому – один-два на добу.

БІЛЬШІСТЬ ВОРОЖИХ КІБЕРАТАК СПРЯМОВАНІ НА ДОСТУП ДО ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ДЕРЖУСТАНОВ І ТЕХНОЛОГІЧНИХ СИСТЕМ ІНФРАСТРУКТУРИ – ДАНІ СБУ

3 жовтня працівники СБУ провели практичний семінар для 70 представників різних державних установ. Під час заходу вони оприлюднили результати власного аналізу зловмисної поведінки російських хакерських груп. Так, за їх даними більшість ворожих кібератак спрямована на пошук несанкціонованого доступу до електронного документообігу держустанов і технологічних систем інфраструктури. Зазвичай такими «точками входу» для російських хакерів є публічно доступні сервіси, насамперед – електронна пошта.

СБУ ТА ДЕРЖСПЕЦЗВ'ЯЗКУ ЗАКЛИКАЛИ ЕНЕРГЕТИЧНІ КОМПАНІЇ ПОСИЛИТИ ЗАХОДИ КІБЕРБЕЗПЕКИ НА ЧАС ЗИМОВОГО ПЕРІОДУ

10 листопада СБУ та Держспецзв'язку звергнули увагу енергетичних компаній на підвищені загрози кібербезпеці з боку росії у зимовий період. Базуючись на досвіді минулих років спеціальні служби вказують на вірогідність активних спроб російських хакерів вплинути на роботу об'єктів критичної інформаційної інфраструктури енергетичної сфери та надання ними життєво важливих сервісів. З метою кращої підготовки до складного періоду пропонується використовувати матеріали звіту компанії Mandiant щодо деструктивної кібератаки, скерованої на одне з українських регіональних енергетичних підприємств у 2022 році, а також рекомендації CERT-UA, яка діє при Держспецзв'язку.

UAC-0165 ВТРУЧАЄТЬСЯ В РОБОТУ 11 УКРАЇНСЬКИХ ПРОВАЙДЕРІВ –ДОСЛІДЖЕННЯ CERT-UA

16 листопада CERT-UA оприлюднив результати свого нового дослідження активності російських зловмисників. Цього разу це аналіз діяльності організованої групи кіберзловмисників, що відстежується за ідентифікатором UAC-0165. За період від 11 травня до 29 вересня 2023 року ця група втрутилася в інформаційно-комунікаційні системи не менше ніж 11 провайдерів. Внаслідок чого, зокрема, виникали перебої в наданні послуг споживачам.

CERT-UA НА ПОЧАТКУ ЖОВТНЯ ЗАФІКСУВАЛА ЩОНАЙМЕНШЕ ЧОТИРИ ХВИЛІ КІБЕРАТАК ПРОТИ БУХГАЛТЕРІВ

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA за період від 2 по 6 жовтня 2023 зафіксувала щонайменше чотири хвилі кібератак, здійснених угрупуванням UAC-0006 із застосуванням шкідливої програми SmokeLoader. Типовий зловмисний задум угрупування UAC-0006 полягає в ураженні бухгалтерських комп'ютерів, за допомогою яких здійснюється забезпечення фінансової діяльності, а також викраденні автентифікаційних даних та створенні несанкціонованих платежів.

ЧЕРГОВЕ РОЗСИЛАННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ: ХАКЕРИ МАСКУЮТЬСЯ ПІД СБУ

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA виявила масове розповсюдження електронних листів начебто від імені Служби безпеки України. Повідомлення містили вкладений RAR-файл «Електронна вимога СБУ України.rar». Активність відстежується за ідентифікатором UAC-0050. Раніше схожі небезпечні листи від групи UAC-0050 надходили нібито від імені Печерського суду та Укртелекому.

З ПОЧАТКУ ПОВНОМАСШТАБНОЇ ВІЙНИ СБУ ЗАБЛОКУВАЛА 76 БОТОФЕРМ З АУДИТОРІЄЮ 3 МЛН ФЕЙКОВИХ АКАУНТІВ

У листопаді начальник Департаменту кібербезпеки СБУ Ілля Вітюк у коментарі для UNITED24 Media розповів, що упродовж 2022-2023 років Служба безпеки України заблокувала діяльність 76 ботоферм, які діяли на території нашої держави та відпрацьовували проросійські наративи. Також за 10 місяців 2023 року СБУ нейтралізувала майже 4 тисячі кібератак.

КІБЕРПОЛІЦІЯ ТА СЛІДЧІ НАЦПОЛУ ВИКРИЛИ ХАКЕРІВ, ЯКІ АТАКУВАЛИ ПРОВІДНІ СВІТОВІ КОМПАНІЇ

Починаючи з 2018 року фігуранти, використовуючи розроблені ними віруси-шифрувальники, здійснювали атаки на сервери провідних світових компаній. У ході міжнародної поліцейської операції правоохоронці провели понад 30 обшуків та припинили діяльність угруповання. Встановлено, що за кілька років злочинної діяльності зловмисники зашифрували понад 1000 серверів світових підприємств та спричинили збитків на суму у понад 3 мільярди гривень в перерахунку на національну валюту.

КІБЕРПОЛІЦІЯ СПІЛЬНО З ПРАВООХОРОНЦЯМИ 10 КРАЇН ПРИПИНИЛИ ДІЯЛЬНІСТЬ RANSOMWARE ГРУПИ

20 жовтня оприлюднено інформацію про припинення діяльності великої транснаціональної злочинної групи яка використовуючи ransomware починаючи з 2020 року атакувала 168 компаній міжнародних компаній у країнах Європи та Америки. Наразі невідомо про масштаби завданої групою шкоди, але частина членів групування знаходилась в Україні, в тому числі як розробник ransomware та частина групи функціонувала у Франції.

КІБЕРПОЛІЦІЯ ПРИКАРПАТТЯ ВИКРИЛА ГРУПУ ШАХРАЇВ, ЩО ДІЯЛИ ЗА СХЕМОЮ «ДРУГ ПРОСИТЬ У БОРГ»

Шляхом підбору паролів фігуранти зламували електронні поштові скриньки громадян, до яких були «прив'язані» акаунти соціальних мереж. У такий спосіб вони отримували доступ до сторінок та від імені власників надсилали повідомлення друзям останніх із проханням позичити гроші. Наразі встановлено два десятки потерпілих, яких встигли ошукали шахраї. Загальна сума збитків становить близько 150 тисяч гривень.

MICROSOFT ЩЕ РІК НАДАВАТИМЕ БЕЗОПЛАТНІ ХМАРНІ ПОСЛУГИ УКРАЇНСЬКИМ ДЕРЖУСТАНОВАМ

29 листопада Міністерство цифрової трансформації повідомило, що державні установи України зможуть безоплатно користуватися хмарними продуктами від Microsoft ще рік – до 31 грудня 2024-го. Це є частиною політики підтримки України з боку корпорації Microsoft.

МІНЦИФРА ЗАПУСТИЛА ТЕСТ НА ЗНАННЯ ПРАВИЛ БЕЗПЕКИ В МЕРЕЖІ «КІБЕРГРАМ»

15 листопада Мінцифра за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України» запустила «Кіберграм» – тест, який перевіряє п'ять основних компетенцій користувача:

- захист пристроїв та безпечне підключення до інтернету;
- захист персональних даних і приватності, безпека в інтернеті;
- захист особистих прав споживача від шахрайства та зловживань;
- захист здоров'я і добробуту;
- захист навколишнього середовища.

Тест доступний всім користувачам платформи Дія.Освіта.

GOOGLE В УКРАЇНІ ЗАПУСТИВ МЕДІАКАМПАНІЮ «ПОРАДИ З ОНЛАЙН-БЕЗПЕКИ»

Google спільно з Мінцифрою та за підтримки Держспецзв'язку запустили в соціальних мережах медіакампанію «Поради з онлайн-безпеки». Мета – допомогти українцям бути кіберсвідомими й уникати онлайн-загроз. Медіакампанія передбачає чотири відеоролики, які розповідають про інструменти для підтримки кібербезпеки. Серед них: багатофакторна автентифікація, програмне забезпечення, фішинг та менеджер паролів.

УКРАЇНА ПОКИ НЕ ОБМЕЖУВАЛА ОБЛАДНАННЯ HUAWEI У ДОСТУПІ ДО ІНФРАСТРУКТУРНИХ ПРОЄКТІВ

За словами заступника Міністра цифрової трансформації Єгора Дубинського Україна не виключила китайських телекомунікаційних постачальників Huawei і ZTE з проєктів постачання обладнання для відновлення інфраструктури, пошкодженої внаслідок нападів росії на її територію. Це обумовлено тим, що наразі Україна не має надійних доказів щодо можливих ризиків безпеці, пов'язаних з китайським постачальником.

8. ПЕРША СВІТОВА КІБЕРВІЙНА

МІЖНАРОДНИЙ КОМІТЕТ ЧЕРВОНОГО ХРЕСТА ОПУБЛІКУВАВ 8 ПРАВИЛ ДЛЯ ХАКТИВІСТІВ, ЯКІ ВЕДУТЬ ГІБРИДНУ ВІЙНУ

На початку жовтня двоє представників Міжнародного комітету Червоного Хреста (МКЧХ) випустили рекомендації для хактивістів, опубліковані у вигляді есе в Європейському журналі міжнародного права. Вони являють собою розширення існуючих міжнародних норм збройних конфліктів на кіберпростір з метою збереження норм, які захищатимуть некомбатантів не лише від атак на інфраструктуру, але й від онлайн-підбурювання до жорстокості. Деякі конкретні класи цілей прямо заборонені, зокрема медичні та гуманітарні об'єкти.

Деякі групи хактивістів відповіли насмішками. IT-армія України повідомила BBC, що не впевнена, чи буде дотримуватися цих правил. Зокрема, IT-армія, схоже, розглядає правила як абсолютну заборону супутніх руйнувань, яких не завжди можливо уникнути. Група вже уникає атак на лікарні та подібні заклади, але вона проводила DDoS-атаки на цивільну інфраструктуру, як-от банки та служби бронювання подорожей.

Хактивісти з іншого боку війни відкинули МКЧХ як неактуальний. російська мережа KillNet запитала: «Чому ми повинні слухати Червоний Хрест?» Anonymous Sudan, яка, попри свою назву, є допоміжною групою російських хактивістів, категорично відкинула правила МКЧХ, заявивши, що обмеження «нежиттєздатні і що їх порушення заради справи групи неминуче».

У 2023 РОЦІ АВТОРИТАРНІ УРЯДИ СКОНЦЕНТРУВАЛИСЬ НА КІБЕРШПИГУНСЬКИХ ОПЕРАЦІЯХ – НОВИЙ ЗВІТ MICROSOFT

5 жовтня корпорація Microsoft оприлюднила свій звіт про зловмисну кібератівність у 2023 році з оцінкою дій державних суб'єктів та їх пріоритетів. Основний фокус зосереджено на діях росії, КНР, Ірану та Північної Кореї. Автори звіту роблять висновок, що у 2023 році всі авторитарні уряди сконцентрувались на операціях кібершпигунства, намагаючись отримати більше інформації щодо важливих для них зовнішньополітичних ініціатив. російські спецслужби переорієнтували свої кібератаки на шпигунську діяльність на підтримку війни проти України, одночасно з цим продовжуючи руйнівні кібератаки в Україні та ширші шпигунські зусилля.

УКРАЇНА, ІЗРАЇЛЬ, ПІВДЕННА КОРЕЯ ОЧОЛИЛИ СПИСОК КРАЇН, ЯКІ НАЙЧАСТІШЕ ПІДДАЮТЬСЯ КІБЕРАТАКАМ

Згідно з новим звітом Microsoft, опублікованим 6 жовтня, понад 120 країн зазнали кібератак протягом останнього року, причому Україна, Ізраїль, Південна Корея та Тайвань очолили список країн, які найбільше піддалися нападам.

Ці атаки були в основному здійснені чотирма державами: росією, Китаєм, Іраном і Північною Кореєю. У деяких атаках також були залучені хакери з Палестинських територій та інші хакери-найманці, найняті різними країнами.
Звіт Microsoft про цифровий захист за 2023 рік виявив зміни в стратегіях атак, зазначивши перехід від деструктивних і фінансово вмотивованих кампаній (наприклад, програм-вимагачів) до кампаній, які переважно стосуються крадіжки інформації, прихованого моніторингу зв'язку або маніпулювання інформацією. Хоча росія продовжує здійснювати кібератаки на Україну, вона також активізувала шпигунську діяльність, тоді як Китай продовжує неперевершені кампанії зі шпигунства та крадіжки даних і розширює арсенал для потенційно деструктивних атак.

2023 СТАН ЗАГРОЗИ: ОГЛЯД РОКУ ВІД SECUREWORKS

На початку жовтня компанія Secureworks опублікувала звіт про стан загроз за 2023 рік, у якому виявила, що програми-вимагачі залишаються головною загрозою, з якою стикаються організації: «Кількість атак повернулася до історичної норми, а потім і перевищила її після торішнього короткого уповільнення після вторгнення в Україну. Середній час очікування між отриманням початкового доступу і доставлення корисного навантаження програми-вимагача значно скоротився до середнього показника, який становить лише 24 годин».

У звіті також розглядаються мотиви фінансованих державою кібероперацій: «росія зосереджується на війні в Україні, Північна Корея — на крадіжці валюти, Іран — на придушенні опозиції, а Китай — на кібершпигунстві. Однак регіональні фокуси в деяких випадках починають зміщуватися, особливо з боку Китаю, який уважно стежить за впливом війни в Україні на інші європейські країни».

КІБЕРЗЛОЧИНЦІ ВИКОРИСТОВУЮТЬ РОСІЙСЬКИЙ СЕРВІС КОРЕЕСНКА ДЛЯ МАСОВОЇ РОБОТИ З ОБЛІКОВИМИ ЗАПИСАМИ В СОЦІАЛЬНИХ МЕРЕЖАХ

27 жовтня кібербезпекова компанія Trustwave оприлюднила своє дослідження про те, як кіберзлочинці користуються послугами російського сервісу Kopeechka для масового створення облікових записів в популярних соціальних мережах. Такі облікові записи використовуються для соціальної інженерії, реклами фішингових сайтів тощо.

США ЗАПРОВАДИЛИ САНКЦІЇ ПРОТИ РОСІЯНКИ, ЗВИНУВАЧЕНОЇ У ВІДМИВАННІ ВІРТУАЛЬНОЇ ВАЛЮТИ ДЛЯ АФІЛІЙОВАНОЇ ПРОГРАМИ-ВИМАГАЧА

3 листопада, громадянка рф Катерина Жданова потрапила під санкції Міністерства фінансів США за ймовірне відмивання віртуальної валюти від імені російської еліти та кіберзлочинців, включаючи філію вимагача Ryuk.

Жданову звинувачують у відмиванні понад 2,3 мільйона доларів у 2021 році для філії програми-вимагача Ryuk через криптовалютну біржу Garantex, яка також була включена до списку OFAC у 2022 році. OFAC заявляє, що до запровадження санкції на ній було проведено транзакції на понад 100 мільйонів доларів, пов'язані з ринками даркнету та злочинцями.

РОСІЙСЬКІ ФІРМИ «ВПЛИВУ ЗА НАЙМОМ» ПОШИРЮЮТЬ ПРОПАГАНДУ В ЛАТИНСЬКІЙ АМЕРИЦІ – ДЕРЖДЕПАРТАМЕНТ США

8 листопада Державний департамент США викрив фінансовану росією кампанію дезінформації в Латинській Америці, спрямовану на підрив підтримки України та дискредитацію США та НАТО. Кампанія проводиться трьома місцевими компаніями: Агентством соціального дизайну (SDA), Інститутом розвитку Інтернету та Structura, які ДержДеп описує як фірми, що надають послуги «впливу за наймом» із глибокими технічними можливостями.

росія керує значною екосистемою проксі-сайтів, окремих осіб і організацій, які, здається, є незалежними джерелами новин для просування своєї пропаганди в Латинській Америці. Розпорошена мережа іспаномовних і португаломовних журналістів і засобів масової інформації дозволяє росії інтегрувати проросійський контент у латиноамериканські медіа, приховуючи свою приналежність до рф. Також росія втручається у вибори в Африці, щоб зберегти при владі дружні до москви режими.

SANDWORM ПЕРЕРВАВ ПОСТАЧАННЯ ЕЛЕКТРОЕНЕРГІЇ В УКРАЇНІ ЗА ДОПОМОГОЮ НОВОЇ АТАКИ НА ОПЕРАЦІЙНУ ТЕХНОЛОГІЮ

9 листопада компанія Mandiant опублікувала результати дослідження кібератаки угруповання SandWorm на системи операційних технологій (OT) української енергокомпанії наприкінці 2022 року. Mandiant Threat Intelligence виявила, що цей інцидент являв собою кібератаку з кількома подіями, із застосуванням нової техніки впливу на промислові системи управління (ICS) / операційні технології (OT). Актор вперше використав методи OT-level liveing off the land (LotL), щоб, ймовірно, спрацювали автоматичні вимикачі підстанції жертви, спричинивши незаплановане відключення електроенергії, яке збіглося з масовими ракетними ударами по критичній інфраструктурі по всій Україні.

«Ця атака демонструє найновіший розвиток можливостей росії щодо кіберфізичних атак, яка стає все більш помітною після вторгнення рф в Україну. Методи, застосовані під час інциденту, свідчать про зростаючу зрілість російського наступального арсеналу OT, включаючи здатність розпізнавати нові вектори загроз OT, розвивати нові можливості та використовувати різні типи інфраструктури OT для здійснення атак,» – йдеться у звіті.

ПРОТИ ЕНЕРГОКОМПАНІЙ ДАНІЇ БУЛО ПРОВЕДЕНО СКООРДИНОВАНУ КІБЕРАТАКУ З РОСІЙСЬКИМ СЛІДОМ

14 листопада було поширено інформацію про велику скоординовану атаку на енергетичні об'єкти в Данії яка відбулась у травні цього року. Під час атаки хакерам вдалось скомпрометували 22 енергетичні організації. У рамках атак хакери використовували численні вразливості в брандмауерах Zyxel для початкового доступу, виконання коду та отримання повного контролю над ураженими системами. Перша хвиля атак відбулась 11 травня, друга 22 травня, а третя – 24 травня. Принаймні в одній з атак спостерігалась активність, пов'язана із Sandworm (APT28).

NETFLIX ПОСТРАЖДАВ ВІД DDOS-АТАКИ ANONYMOUS SUDAN

DDoS атаки залишаються характерною технікою російських хактивістів. Нещодавно Anonymous Sudan, філія KillNet, створила перешкоди для Netflix у низці країн, номінально з метою блокування вмісту ЛГБТК, але, ймовірно, насправді просто для привернення уваги. Річард Уоллес, аналітик із розвідки кіберзагроз у Vercara, пояснив: «Крім атаки на Netflix, Anonymous Sudan також взяв на себе відповідальність за атаки на Hulu того самого дня (29 вересня 2013 року).

Раніше цього року Anonymous Sudan погрожував атакувати організації, розташовані в США, у відповідь на триваючу військову та фінансову допомогу Україні. Веркара не вперше спостерігає, як Killnet атакує сайти, які вони вважають аморальними: у минулому вони атакували OnlyFans, а також дарк-вебсайти, що продають наркотики. Anonymous Sudan використовує будь-який привід, щоб легітимізувати свої DDoS-атаки проти західних і європейських країн, щоб отримати безкоштовну рекламу, продовжити вербування та отримати фінансування для подальшої діяльності».

УКРАЇНА РОЗСЛІДУЄ ВОЄННІ ЗЛОЧИНИ У КІБЕРПРОСТОРІ

18 листопада Генеральний прокурор України Андрій Костін повідомив виданню Politico, що український уряд зібрав докази близько 109 000 вірогідних воєнних злочинів росії. Серед них чотири справи відкрито за звинуваченнями у кібервійні. Костін сказав, що включення кіберзлочинів і злочинів проти довкілля до доказів МКС є новою ініціативою України під час цієї війни, підкресливши, що «у кожного злочину є жертви».

РОСІЙСЬКІ ХАКЕРИ ЗАЯВИЛИ ПРО АТАКУ НА КОМПАНІЮ, ЩО ПОСТАЧАЄ УКРАЇНІ ВИНИЩУВАЧІ

19 листопада британське видання The Telegraph повідомило, що відома група програм-вимагачів LockBit, яка діє з дозволу росії та фактично як російський приватна компанія, стверджує, що зламала мережі бельгійської компанії Sabena Engineering, яка займається постачанням F-16 для України. The Telegraph повідомляє, що LockBit погрожував оприлюднити конфіденційні дані, отримані під час атаки, якщо викуп не буде сплачено до 26 листопада. Sabena каже, що розслідує інцидент і впевнена, що, будь-які результати розслідування не вплинуть на безпеку польотів.

NONAME057(16) ЗАЙМАЄТЬСЯ ВЕРБУВАННЯМ АРМІЇ ОНЛАЙН-ХАКТИВІСТІВ

30 листопада Australian Cyber Security Magazine повідомив, що проросійська хактивістська група NoName057(16) активно вербує онлайн-армію для посилення своїх кібератак на вебсайти приватних організацій і державних установ у країнах, які, на її думку, демонструють упередженість проти росії.

Називаючи майбутніх онлайн-рекрутів «патріотами та борцями за справедливість», NoName057(16) обіцяє, що так само, як і у звичайних арміях, члени матимуть звання та нагороди за заслуги залежно від часу служби та досягнень. 25 листопада група заявила, що новобранцям будуть платити в електронній валюті під назвою dCoin «відповідно до їх внеску в атаки», додавши, що чим вищий ранг добровольця та чим більше кібератак новобранець здійснив, тим більше їм будуть платити.

ХАКЕРИ MUSTANG PANDA АТАКУЮТЬ УРЯД ФІЛІППІН НА ТЛІ НАПРУЖЕНОСТІ В ПІВДЕННОКИТАЙСЬКОМУ МОРІ

Зловмисне угрупування Mustang Panda (має зв'язок з Китаєм) пов'язали з кібератакою на урядову установу Філіппін на тлі зростання напруженості між двома країнами через суперечку у Південнокитайському морі. Підрозділ 42 Palo Alto Networks пов'язав зловмисне угруповання з трьома кампаніями в серпні 2023 року, головним чином виділивши організації в південній частині Тихого океану. «Кампанії використовували законне програмне забезпечення, включаючи Solid PDF Creator і SmadavProtect (індонезійське антивірусне рішення) для стороннього завантаження шкідливих файлів», — повідомили в компанії.

9. РІЗНЕ

ФЕДЕРАЛЬНИЙ АПЕЛЯЦІЙНИЙ СУД ПОШИРЮЄ ОБМЕЖЕННЯ НА СПІЛКУВАННЯ АДМІНІСТРАЦІЇ БАЙДЕНА З КОМПАНІЯМИ СОЦІАЛЬНИХ МЕДІА НА ПРОВІДНЕ АГЕНТСТВО З КІБЕРБЕЗПЕКИ США

CNN повідомила 3 жовтня, що агенція CISA зіткнулася з позовом, який оскаржує її повноваження збирати дані соціальних мереж для моніторингу онлайн-загроз. Група захисту конфіденційності, Electronic Privacy Information Center (EPIC), подала позов, вимагаючи судової заборони програми моніторингу соціальних медіа CISA, стверджуючи, що ця програма виходить за рамки законодавчо визначених повноважень агенції та викликає занепокоєння щодо порушень конфіденційності. CISA, яка відповідає за захист критичної інфраструктури від кіберзагроз, ініціювала програму моніторингу онлайн-платформ на наявність потенційних загроз і вразливостей. Ця ситуація підкреслює триваючі дебати щодо балансу між заходами національної безпеки та правами особи на конфіденційність у контексті ініціатив з кібербезпеки.

SEC ЗВИНУВАЧУЄ SOLARWINDS ТА ЙОГО CISO У ШАХРАЙСТВІ ТА ПОРУШЕННЯХ КІБЕРБЕЗПЕКИ

31 жовтня Комісія з цінних паперів і бірж США (SEC) висунула звинувачення проти SolarWinds та її CISO у шахрайстві та неналежному забезпеченні кібербезпеки. SEC стверджує, що CISO SolarWinds не зміг підтримувати адекватний внутрішній контроль, що сприяло порушенню кібербезпеки, яке призвело до вразливості програмного забезпечення компанії та вплинуло на тисячі клієнтів. Компанію SolarWinds також звинувачують в оманливих заявах щодо стану її кібербезпеки в публічних документах. Комісія з цінних паперів і бірж стверджує, що SolarWinds не мала достатніх гарантій для захисту своїх систем, а її неспроможність своєчасно розкрити інформацію про злам є порушенням федерального законодавства про цінні папери.

Цей випадок підкреслює дедалі більшу увагу та правові наслідки, з якими стикаються компанії через порушення кібербезпеки, а також важливість прозорого розкриття інформації в таких інцидентах.

НОВИЙ СВІТ БЕЗПЕКИ: ІНІЦІАТИВА БЕЗПЕЧНОГО МАЙБУТНЬОГО ВІД MICROSOFT

2 листопада корпорація Майкрософт запустила ініціативу Secure Future Initiative, яка включає зобов'язання компанії покращити безпеку ключів підпису особи. Ініціатива базується на «трьох стовпах: фокус на кіберзахисті на основі штучного інтелекту, досягнення у фундаментальній інженерії програмного забезпечення та пропаганді більш жорсткого застосування міжнародних норм для захисту цивільних осіб від кіберзагроз».

ІЗРАЇЛЬСЬКА КОМПАНІЯ NSO ЗАСТОСОВУЄ СУПЕРЕЧЛИВЕ ШПИГУНСЬКЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ PEGASUS ПІД ЧАС КОНФЛІКТУ В ГАЗІ

14 листопада видання Axios повідомило, що ізраїльська влада використовує інструмент перехоплення з нульовим натисканням Pegasus від компанії NSO для відстеження мобільних телефонів заручників, вбитих мирних жителів і терористів ХАМАС, щоб знайти вцілілих заручників. Кажуть, що NSO Group звертається до офіційних осіб США з проханням пом'якшити обмеження щодо її інструментів, які, на її думку, стали життєво важливими для збору інформації щодо терористичних організацій. Поки що мало ознак, що США готові до такого пом'якшення, запровадженого після багатьох повідомлень, що Pegasus сприяло масовим зловживанням з боку репресивних урядів, але, схоже, були деякі прохання з боку європейських урядів, які виступали за відновлення довіри до NSO Group з боку американського уряду.

ФБР ЗАКЛИКАЄ КОМПАНІЇ АКТИВНІШЕ ДІЛИТИСЯ ІНФОРМАЦІЄЮ ПІСЛЯ КІБЕРАТАК НА ТЛІ РОЗСЛІДУВАННЯ ЗЛОМУ MGM

16 листопада видання Axios повідомило, що Федеральне бюро розслідувань просить компанії поділитися більш детальною інформацією про кібератаки, з якими вони стикаються, оскільки Бюро продовжує розслідувати хакерську групу Scattered Spider. Заклик прозвучав на тлі критики на адресу ФБР, що воно так і не заарештувало осіб, дотичних до хакерської діяльності, хоча їх імена відомі та вони знаходяться на території США. Серед причин цього той факт, що інші компанії, які стали жертвами атак угруповання, не повідомили про це слідчих, через що вони не можуть зібрати достатню доказову базу.