НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

УКРАЇНСЬКА ФУНДАЦІЯ БЕЗПЕКОВИХ СТУДІЙ

CYBER DIGEST

Огляд подій в сфері кібербезпеки,
грудень 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

США оновило керівництво двома важливими кібербезпековими структурами. Ексспівробітник ЦРУ Г. Круккер став Національним кібердиректором, а генерал-лейтенант Тімоті Хо змінив на посаді CYBERCOM і NSA генерала армії США Пола М. Накасоне, який очолював ці два відомства з 2018 року. Ці зміни відображають і зміни в політиці цих структур. В тому числі як офіс Національного кібердиректора все більше зосереджується на імплементації Стратегії кібербезпеки США та Стратегії розвитку трудових кіберресурсів, NSA все частіше виступає із настановами орієнтованими на широке коло організацій в середині США, а також нарощує свої міжнародні контакти – вони є постійними учасниками партнерських проєктів в межах Альянсу п'ять очей.

Європейський Союз після майже річних дискусій розпочав рух щодо прийняття Акту про кіберстійкість (Cyber Resilience Act). Цей документ створює нові рамки функціонування для IT-сектору та виробників IT-обладнання, вимагаючи від них більше уваги до заходів кібербезпеки. Швидше за все імплементація цього документа буде складною та відбуватись з різною швидкістю в європейських країнах. Про це каже і досвід NIS2 Директиви, яка більше ніж рік після свого прийняття все ще слабко імплементована у багатьох європейських країнах. При цьому ЄС чітко розуміє зростання ролі кібербезпеки та готовий залучати до цього кошти (остання ініціатива стосується залучення 214 млн євро на кібербезпеку). Це доповнюється закликом керівництва ЄС до створення європейських кіберсил, що будуть мати наступальні можливості.

Міжнародна співпраця також стає системнішою. Вперше підписано угоду про співпрацю між європейською ENISA та американською CISA – двома ключовими агенціями у сфері кібербезпеки в ЄС та США. Це відображає зростання ролі альянсів та пошуку міжнародних партнерів двома найбільшими економіками світу в інтересах спільної кібербезпеки. Ця тенденція доповнюється зростанням кількості зв'язків між євроатлантичними країнами та їх азійськими партнерами. Наприклад, у навчаннях НАТО з кібербезпеки вперше взяли участь Японія та Південна Корея, а США зі свого боку розпочала з цими двома країнами нову спільну ініціативу спрямовану на протидію деструктивній діяльності Північної Кореї.

Україна продовжує поглиблювати міжнародну співпрацю з приватними та державними акторами. У 2024 році компанія Recorded Future допомагатиме Україні захищати критичну інфраструктуру від військової та кіберагресії росії. До міжнародної кіберкоаліції на підтримку України приєдналася Ісландія, яка стала 8 учасницею. Протидія інформаційним атакам та боротьба з фінансовим фішингом стали предметом обговорення представників НКЦК з компанією Meta. Про співробітництво домовилися Міністерство цифрової трансформації України та Європейська організація кібербезпеки (ECSO). Результатом співпраці стане посилення системи кіберзахисту України відповідно до міжнародних стандартів та доступ українських підприємств та фахівців до ринку кібербезпеки ЄС. Розширюється також двостороння співпраця з Японією та Німеччиною.

російська кіберактивність не зменшується. Активізується також і китайська. В 2024 році відбудуться вибори у низці країн (включаючи США та Великобританію) і вже зараз безпекові органи відзначають, що APT групи з росії та КНР готуються до цих подій, плануючи втрутитись в них. Ця спрямована активність доповнюється дослідженнями сучасного ландшафту кіберзагроз, який каже, що більше ніж 60% DDoS атак наразі мають політичне підґрунтя, а фахівці з кібербезпеки вже прямо кажуть, що групам реагування на кіберінциденти доведеться слідкувати не лише за своїми інформаційними системами, але і геополітичними подіями, які стають каталізатором нових загроз для державного та приватного секторів. Напередодні виборів до Європейського парламенту також було проведено внутрішній огляд кібербезпеки. За його висновками, кібербезпека Європарламенту «ще не відповідає галузевим стандартам» і «не повністю відповідає рівню загрози», створеної спонсорованими державою хакерами.

Критична інфраструктура все частіше піддається атакам зі спробами вплинути на промислові процеси. Хоча ransomware залишається основним джерелом загроз, але атаки сягають все більше небезпечних рівнів. Нещодавні кібератаки проти систем водопостачання на рівні окремих невеликих громад в США (а також щонайменше однієї схожої організації в Ірландії) показали наскільки локальний рівень залишається незахищеним перед кіберзагрозами – там ще більш серйозно відчувається недостача кадрів та фінансових ресурсів для належного кіберзахисту. Можна прогнозувати, що локальні/місцеві об'єкти критичної інфраструктури все частіше будуть ставати мішенню для зловмисників, які планують довести неспроможності центральної влади захистити всіх громадян.

Україна продовжує протистояння з російськими кіберсилами. У грудні 2023 року відбулась серйозна кібератака проти одного з національних операторів мобільного зв'язку «Київстар». Наслідки атаки були руйнівними – щонайменше декілька днів абоненти компанії не мали зв'язку, а процес відновлення розтягнувся на декілька тижнів. російські хакери також скористалися цією ситуацією при розсилці листів зі зловмисним ПЗ. російські хакери все ще активні та синхронізують свої дії з загальною російською військовою стратегією (наприклад, атакуючи паралельно з ракетними ударами сільськогосподарський сектор України), при цьому APT групи, які працюють проти України, майже не змінюються.

Україна зміцнює національну систему кібербезпеки. Під час засідання Національного координаційного центру кібербезпеки (НКЦК) при РНБО України у закритому режимі було ухвалено низку рішень, спрямованих на невідкладне посилення захищеності системи електронних комунікацій України, її об'єктів та інфраструктури. Також учасники обговорили пріоритетні напрями реалізації Талліннського механізму та питання оптимізації міжнародної взаємодії у сфері кібербезпеки. Крім того, сценарій третіх щорічних командно-штабних навчань, які у грудні провів НКЦК, вперше включав завдання щодо відпрацювання наступальних заходів активної кібероборони.

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

ЄВРОПЕЙСЬКА КОМІСІЯ ВІТАЄ ПОЛІТИЧНУ ДОМОВЛЕНІСТЬ ЩОДО CYBER RESILIENCE ACT

1 грудня стало відомо, що Європейським парламентом і Європейська рада досягли політичної домовленості щодо прийняття Cyber Resilience Act – комплексного документа, що на думку Єврокомісії має істотно підвищити рівень кібербезпеки цифрових продуктів на користь споживачів і компаній у всьому ЄС. Ця домовленість відкриває шлях до наступних кроків – офіційного схвалення як Європейським парламентом, так і Європейською радою. Після прийняття Закон набуде чинності на 20-й день після його офіційної публікації.

Пропоновані зміни включають підтримку малих і мікропідприємств під час оцінки відповідності та спрощення процесу класифікації цифрових продуктів відповідно до регламенту. Компанії, які не повідомлять про активно використовувану вразливість, можуть зіштовхнутись зі значними штрафами.

Відтепер очікується, що виробники повідомлятимуть про вразливості Національній групі реагування на інциденти комп'ютерної безпеки (CSIRT) своєї країни замість того, щоб звітувати безпосередньо в ENISA, яка буде керувати платформою для CSIRT для завантаження звітів.

ГАРРІ КРУКЕРА ЗАТВЕРДЖЕНО НОВИМ НАЦІОНАЛЬНИМ КІБЕРДИРЕКТОРОМ США

12 грудня Сенат США, проголосувавши 59 проти 40, затвердив Гаррі Крукера (Harry Coker, Jr) на посаді нового директора Офісу Національного кібердиректора (Office of the National Cyber Director). Г. Крукер починав як офіцер ВМФ, але надалі у більшість своєї кар'єри (17 років) присвятив ЦРУ, а пізніше – NSA. У ЦРУ він займався питанням цифрових інновацій та зовнішніми відносинами Управління. Кокер змінить Кріса Інгліса на цій посаді.

ЄС ІНВЕСТУЄ ПОНАД 760 МІЛЬЙОНІВ ЄВРО В ЦИФРОВУ ТРАНСФОРМАЦІЮ І КІБЕРБЕЗПЕКУ

14 грудня Єврокомісія прийняла поправку до робочої програми «Цифрова Європа» на 2024 рік, виділивши 762,7 мільйона євро на цифрові рішення. З них майже 549 мільйонів євро буде зосереджена на розгортанні проєктів, які використовують цифрові технології, передусім – хмарні сервіси та передові цифрові навички. Решту 214 мільйонів євро виділено на кібербезпеку, щоб посилити колективну стійкість ЄС проти кіберзагроз. Заходи, що фінансуються цією програмою, будуть реалізовані Європейським центром компетенції з кібербезпеки.

ТІМОТІ ХО СТАВ НОВИМ КЕРІВНИКОМ CYBERCOM І NSA

22 грудня Сенат США підтримав призначення генерала Тімоті Хо на посаді керівника CYBERCOM і NSA. Генерал-лейтенанта Тімоті Хо змінить на цій посаді генерала армії США Пола М. Накасоне, який очолював ці два відомства з 2018 року.

ПЕНТАГОН ДЛЯ ОБМІНУ ДАНИМИ З РЕГІОНАЛЬНИМИ ПАРТНЕРАМИ БУДУЄ МЕРЕЖУ MISSION PARTNER ENVIRONMENT НА ЗАСАДАХ «НУЛЬОВОЇ ДОВІРИ»

11 грудня стало відомо, що Пентагон разом з партнерами планує провести в Індійсько-Тихоокеанському регіоні військову гру, частиною якої є тестування Mission Partner Environment – спеціальної мережі, яку будує Пентагон для обміну даними між США та регіональним партнерам, таким як Філіппіни та Тайвань. Мережа будується на принципах «нульової довіри» і мета навчань – перевірити її надійність та функціональність.

КНР РОЗРОБИЛО ПРОЄКТ НАЦІОНАЛЬНОГО ПЛАНУ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

16 грудня було оприлюднено План дій у випадку кіберінцидентів – в ньому описано, як компаніям і владі потрібно реагувати на інциденти безпеки даних. У плані пропонується класифікувати будь-який інцидент за чотирма кольоровими кодами, кожен з яких базується на ступені шкоди, завданої національній безпеці, онлайн-мережі/інформаційній мережі компанії або економіці загалом. Документ визначає порядок дій різних суб'єктів за різних за тяжкістю кіберінцидентів, в тому числі порядок інформування урядових органів про такі інциденти.

ПРЕЗИДЕНТ РАДИ ЄС ПРОПОНУЄ СТВОРИТИ «ЄВРОПЕЙСЬКІ КІБЕРСИЛИ» З «НАСТУПАЛЬНИМИ МОЖЛИВОСТЯМИ»

Таку думку Шарль Мішель озвучив під час виступу на щорічній конференції Європейського оборонного агентства (EDA) 30 листопада. Він не деталізував свою пропозицію, але його заява прозвучала на тлі того, що Міністри оборони ЄС підписали нову програму Союзу щодо оперативної мережі військової комп'ютерної команди реагування на надзвичайні ситуації, але не погодилися розширити загальноєвропейські наступальні можливості.

ВІЦЕПРЕМ'ЄР-МІНІСТР ВЕЛИКОЇ БРИТАНІЇ ЗВЕРНУВ УВАГУ БРИТАНСЬКОГО ПАРЛАМЕНТУ НА ПИТАННЯ СТІЙКОСТІ ПІД ЧАС КІБЕРАТАК

Під час щорічного звернення до парламенту, віцепрем'єр-міністр Олівер Доуден наголосив, що стійкість стосується не лише кібербезпеки, але підкреслив важливість того, щоб звичайні люди могли вдатися до «аналогових» технологій у разі кібератаки, яка зупинила роботу енергомережі або комунікаційної інфраструктури. Він порекомендував кожному поглянути на речі, якими вони давно не користувалися, і припустив, що найнеобхідніше може включати, щонайменше, радіо на батарейках, свічки та ліхтарик.

ГОЛОВА БРИТАНСЬКОГО NCSC ЛІНДІ КЕМЕРОН ЗАЛИШИТЬ КІБЕРАГЕНТСТВО ДЛЯ ПЕРЕХОДУ НА ДИПЛОМАТИЧНУ ПОСАДУ

13 грудня стало відомо, що виконавча директорка Національного центру кібербезпеки Сполученого Королівства (NCSC) Лінді Кемерон збирається залишити свою посаду на початку наступного року, щоб перейти на дипломатичну роботу. Кемерон звільняється передчасно, хоча раніше очікувалося, що вона залишатиметься на посаді до 2025 року. Під час роботи в NCSC Кемерон опікувалася численними подіями з кібербезпеки, зокрема надавала оборонну кіберпідтримку Україні під час російського вторгнення, боролася зі зростанням кількості атак програм-вимагачів у Великій Британії та з кіберзагрозами з боку державних угруповань.

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

СПОЛУЧЕНІ ШТАТИ, ПІВДЕННА КОРЕЯ ТА ЯПОНІЯ РОЗПОЧАЛИ НОВУ СПІЛЬНУ ІНІЦІАТИВУ У СФЕРІ КІБЕРБЕЗПЕКИ

9 грудня Сполучені Штати, Південна Корея та Японія домовилися про нові зусилля щодо відповіді на загрози Північної Кореї в кіберпросторі. Для цього було розпочато нову тристоронню ініціативу для протидії загрозам з боку КНДР. Більша частина цієї ініціативи буде спрямована на недопущення використання КНДР криптовалюти для відмивання викрадених нею грошей.

ПІД ЧАС ДИСКУСІЙ ЩОДО ТЕКСТУ ПРОЄКТУ КОНВЕНЦІЇ ООН ПРО КІБЕРЗЛОЧИННІСТЬ НЕ ВРАХОВАНО ЗАСТЕРЕЖЕННЯ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА

19 грудня видання Euroactive опублікувало власний аналіз ситуації навколо можливого ухвалення Конвенції ООН про кіберзлочинність – документа, який багато років послідовно просувають росія та КНР на міжнародному рівні. На думку представників громадянського суспільства в нинішньому вигляді цей документ відображає бажання авторитарних країн повністю контролювати своїх громадян. При цьому частина положень конвенції вже погоджена різними країнами і тривають дискусії щодо найбільш складних елементів пов'язаних з правами людини.

ENISA ТА CISA ПІДПИСАЛИ РОБОЧУ УГОДУ ПРО СПІВПРАЦЮ

7 грудня під час Кібердіалогу між ЄС та США ENISA та CISA оголосили про підписання робочої угоди як важливої віхи в загальній співпраці між Сполученими Штатами та Європейським Союзом у сфері кібербезпеки. Угода охопить такі сфери:

- розвиток кіберобізнаності та потенціалу для підвищення кіберстійкості;
- обмін найкращими практиками імплементації кіберзаконодавства;
- обмін знаннями та інформацією для підвищення загальної ситуаційної обізнаності.

НАТО ПОГЛИБЛЮЄ СПІВПРАЦЮ В РАМКАХ КІБЕРКОАЛІЦІЇ З АЗІЙСЬКИМИ ПАРТНЕРАМИ

На початку грудня країни НАТО завершили одні зі своїх ключових навчань з кібербезпеки в Естонії. Навчання Cyber Coalition 2023 у Таллінні було зосереджено на обміні розвідувальною інформацією про загрози та реагуванні на сценарії атак на віртуальну національну критичну інфраструктуру, а також цілі та структури військового характеру.

У ньому взяли участь 1000 учасників майже з усіх країн НАТО. Новачки Японія та Південна Корея, які попереднього разу були лише спостерігачами, вперше приєдналися як повноправні учасники. Українські чиновники також були присутні після відсутності з 2019 року.

NSA ТА НКЦК ВЕЛИКОБРИТАНІЇ РАЗОМ З ПАРТНЕРАМИ ОПРИЛЮДНИЛИ ОНОВЛЕННЯ ПРО РОСІЙСЬКУ ФІШИНГОВУ КАМПАНІЮ STAR BLIZZARD

7 грудня Агентство національної безпеки (NSA) спільно з Національним центром кібербезпеки Великої Британії (NCSC-UK), за участі CISA, ФБР, Австралійського директорату зв'язку (ASD's ACSC), Канадським центром кібербезпеки (CCCS) та новозеландським національним центром кібербезпеки (NCSC-NZ) поширили аналіз діяльності російського кібератора Star Blizzard (пов'язаного з фсб рф), щоб підвищити обізнаність щодо конкретних методів фішингу, які Star Blizzard використовує для нападу на окремих осіб і організації, включно з урядом США та оборонно-промисловим сектором. Аналіз містить опис основних TTP, а також рекомендації щодо захисту від цієї постійної загрози.

CISA, NSA, ФБР ТА МІЖНАРОДНІ ОРГАНИ З КІБЕРБЕЗПЕКИ ОПУБЛІКУВАЛИ ПОСІБНИК ІЗ ПІДГОТОВКИ ДОРОЖНІХ КАРТ БЕЗПЕКИ ПАМ'ЯТІ

6 грудня CISA, разом з NSA, ФБР та органами кібербезпеки Австралії, Канади, Нової Зеландії та Великої Британії, опублікували спільний посібник, що має заохотити виробників програмного забезпечення усунути вразливості безпеки пам'яті та запровадити безпечні принципи розробки Secure by Design. Посібник має допомогти розробникам програмного забезпечення розробити дорожню карту, яка має детально описувати, як виробник змінюватиме свій життєвий цикл розробки програмного забезпечення (SDLC), щоб скоротити та зрештою усунути небезпечний для пам'яті код у своїх продуктах.

СПІЛЬНА ЗАЯВА ЗА РЕЗУЛЬТАТАМИ ДЕВ'ЯТОГО КІБЕРДІАЛОГУ США-ЄС У БРЮССЕЛІ

8 грудня в Брюсселі відбувся 9-й кібердіалог США-ЄС. Сторони підтвердили свою відданість ідеї відкритого, безпечного та надійного Інтернету. Дискусії стосувалися глобального середовища кіберзагроз, зосереджуючись на агресії росії проти України та занепокоєння щодо зростання зловмисної кібердіяльності. Обидва суб'єкти засудили ці дії та пообіцяли зміцнити кібербезпеку, боротися з кіберзлочинністю, посилювати глобальну кіберстійкість та сприяти відповідальній поведінці держав. Діалог охоплював міжнародну кіберполітику, кіберзахист та співпрацю щодо побудови кіберпотенціалу. Зусилля щодо підвищення кібербезпеки та стійкості, включаючи спільний план дій, були окреслені, а також співпраця над новими технологіями та запуску кіберстипендії США-ЄС.

Наступний діалог запланований на 2024 рік у Вашингтоні.

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

ІРАНСЬКІ КІБЕРШПИГУНИ АТАКУЮТЬ ОБОРОННІ ОРГАНІЗАЦІЇ США ЗА ДОПОМОГОЮ НОВОГО БЕКДОРА

23 грудня Microsoft повідомило, що іранські кібершпигуни атакують організації оборонної промисловості за допомогою нового бекдора під назвою FalseFont. Цю активність кіберфахівці пов'язують із підтримувану Іраном групою Peach Sandstrom. Mandiant, який відстежує це угрупування як APT33, підкреслює, що він націлений на організації в США, Саудівській Аравії та Південній Кореї для «стратегічного кібершпигунства», при цьому особливий інтерес приділяється як комерційним, так і військовим авіаційним компаніям, а також компаніям в енергетичному секторі.

ФБР РОЗРОБИЛО ДЕШИФРАТОР ДЛЯ ПРОГРАМИ-ВИМАГАЧА BLACKCAT

19 грудня Міністерство юстиції США повідомило, що завдяки тому, що правоохоронні органи отримали доступ до мережі BlackCat Ransomware Group, ФБР вдалось створити дешифратор для програми-вимагача BlackCat. ФБР запропонувало цей інструмент понад 500 організаціям і вважає, що в результаті вдалося уникнути виплати викупу на суму 68 мільйонів доларів.

АВСТРАЛІЙСЬКА КОМПАНІЯ EAGERS AUTOMOTIVE ЗІШТОВХНУЛАСЬ З ПРОБЛЕМАМИ В РОБОТІ ПІСЛЯ ІНЦИДЕНТУ З КІБЕРБЕЗПЕКОЮ

29 грудня австралійська компанія Eagers Automotive заявила, що зазнала впливу в своїй діяльності від кіберінциденту. Він вплинув на деякі її IT-системи, а також на здатність компанії завершувати транзакції для деяких нових автомобілів, які вже продані та готові до доставлення. Технічні деталі атаки невідомі.

APT ГРУПА TA4557 НАМАГАЄТЬСЯ ІНФІКУВАТИ ОРГАНІЗАЦІЇ ЧЕРЕЗ HR СЛУЖБИ

12 грудня фахівці компанії Proofpoint повідомили, що виявили чітку зміну поведінки APT групи TA4557 у початковому інфікуванні організацій. Тепер зловмисники створюють фальшиві вебсторінки кандидатів на посади в IT-компанії. Зловмисники ініціативно надсилають електронні листи HR-службам чи рекрутерам (які відповідають за найм), а як тільки одержувач відповів на початковий електронний лист, актор відповідає на нього URL-адресою, яка посилається на контрольований актором вебсайт, який видається за резюме кандидата.

CISA ЗАПУСТИЛА НОВИЙ СЕРВІС THREAT INTELLIGENCE ENTERPRISE SERVICES

18 грудня CISA оприлюднила свою нову ініціативу у сфері обміну інформацією про кіберзагрози – Threat Intelligence Enterprise Services. Це платформа обміну інформацією про загрози, яка об'єднає наявні можливості CISA для подальшого обміну інформацією з федеральними відомствами та визначеними спільнотами користувачів. Платформа має полегшити комунікацію та забезпечить взаємодію щодо конкретних загроз із різноманітними клієнтами CISA.

БРИТАНСЬКИЙ НКЦК ВИЗНАЧИВ НАДІЙНИХ ПОСТАЧАЛЬНИКІВ ПОСЛУГ ДЛЯ ПРОВЕДЕННЯ ТТХ

5 грудня Британський НКЦК повідомив, що визначив перелік надійних (довірених) постачальників послуг для організації командно-штабних навчань (ТТХ). Організації, які відчувають потребу у проведенні настільних або «живих» (в режимі реального часу) навчань можуть скористатись цим переліком для того, щоб отримати послугу належної якості.

БРИТАНСЬКИЙ НКЦК ДОПОМАГАЄ СЕКТОРУ КУЛЬТУРИ ПІДГОТУВАТИСЬ ДО ЗАГРОЗ ВІД RANSOMWARE

18 грудня відбувся спільний захід представників британського НКЦК, Департаменту культури, медіа та спорту та представниками культурного сектору Великобританії, щоб обговорити, що можна зробити для захисту цифрових колекцій установ. Наразі значна кількість надбання музеїв, архівів та інших аналогічних установ вже оцифрована і це робить їх мішенню для ransomware (останнім часом сталось вже декілька таких випадків). НКЦК сформулювало низку ключових порад для організацій сектору культури, що мають допомогти їм вберегтися від ransomware атак.

ANSSI ДОДАВ НОВИЙ СЦЕНАРІЙ ДО СВОГО НАБОРУ З ОРГАНІЗАЦІЇ ТТХ

1 грудня французька ANSSI додала ще один сценарій до свого безкоштовного комплексного набору інструментів для організації ТТХ. Новий сценарій присвячено Олімпійським та Паралімпійським іграм. Його мета – допомогти організаціям підготуватись до кіберінцидентів. Основні потенційні користувачі сценарію: організації, що відповідають за місця проведення змагань; приймаючі громади; громадські та правоохоронні органи; постачальники послуг.

РОСІЙСЬКІ КІБЕРАКТОРИ ВИКОРИСТОВУЮТЬ ВІДОМУ ВРАЗЛИВІСТЬ TEAMCITY ДЛЯ СВОЇХ ОПЕРАЦІЙ ПО ВСЬОМУ СВІТУ

13 грудня NSA спільно з ФБР та кібербезпековими агенціями Польщі і Великобританії, підготували спільне попередження про кіберакторів Служби зовнішньої розвідки росії (СЗР), які використовують загальновідому вразливість у TeamCity для компрометації жертв у всьому світі, включно з в США. Документ детально описує TTP, які застосовують суб'єкти, технічні деталі їх роботи, індикатори компромісу (IOC) і рекомендації щодо пом'якшення наслідків для захисників мережі.

РОСІЙСЬКІ ТА КИТАЙСЬКІ МЕРЕЖІ ДЛЯ ВТРУЧАННЯ «БУДУЮТЬ АУДИТОРІЮ» ПІД ВИБОРИ 2024 РОКУ – META

Як повідомило видання The Record, іноземні групи втручання готуються до майбутніх виборів. Компанія Meta попередила, що ці групи прагнуть створити й охопити онлайн-аудиторію під час підготовки до великих виборів у 2022 році. Вибори відбудуться в кількох країнах, таких як Сполучені Штати, Великобританія та Індія, а також Тайвань і Молдова, які й раніше були об'єктами іноземного втручання.

Meta продовжує протидіяти операціям впливу: у своєму останньому звіті про ворожі загрози Meta оприлюднила висновки щодо трьох окремих кампаній впливу – дві з Китаю та одна з росії. Усі ці операції мали на меті вплинути на сприйняття та обговорення в соціальних мережах ключових політичних питань і подій у цільових країнах. Зусилля Meta, спрямовані на боротьбу з цими кампаніями, включають виявлення та усунення «скоординованої неавтентичної поведінки».

P2PINFECT – НОВИЙ ВАРІАНТ ШПЗ НАЦІЛЕНИЙ НА ПРИСТРОЇ MIPS

4 грудня Cado Security попередила, що новий варіант зловмисного ПЗ ботнету P2Pinfect почав таргетувати архітектуру MIPS (мікропроцесор без зблокованих конвеєрних етапів). Дослідники кажуть, що це «демонструє посилення атак на маршрутизатори, Інтернет речей (IoT) та інші вбудовані пристрої з боку тих, хто стоїть за P2Pinfect».

НОВОГО ЗАГРОЗЛИВОГО АКТОРА AEROBLADE ПОМІЧЕНО У ШПИГУНСЬКІЙ АТАЦІ НА АЕРОКОСМІЧНУ КОМПАНІЮ США

5 грудня видання The Hacker News повідомило, що BlackBerry виявила раніше невідомого загрозливого суб'єкта, націленого на аерокосмічну організацію в США. Його очевидною метою є комерційне та конкурентне кібершпигунство. Команда BlackBerry Threat Research and Intelligence відстежує цю загрозу як AeroBlade. Актор використовував спеціальний фішинг як механізм доставлення: документ, надісланий як вкладення до електронної пошти, містить вбудовану техніку віддаленого впровадження шаблону та шкідливий макрокод VBA, щоб доставити наступну порцію для остаточного застосування корисного навантаження.

Мережева інфраструктура та інструменти зловмисника запрацювали приблизно у вересні 2022 року. BlackBerry оцінює із середньою або високою впевненістю, що наступальна фаза атаки відбулася в липні 2023 року. За цей час зловмисник покращив свій набір інструментів, зробивши його більш прихованим, а мережа інфраструктура залишилася такою ж.

КІБЕРАТАКА ПОРУШИЛА РОБОТУ FIRST AMERICAN ТА ЇЇ ДОЧІРНІХ КОМПАНІЙ

Перша американська фінансова корпорація та її дочірні компанії зазнали значних збоїв у роботі своїх систем та операціях через кібератаку, про яку стало відомо 21 грудня. Компанія, що є головним постачальником послуг зі страхування прав власності у Сполучених Штатах, вимкнула деякі системи, а пізніше повідомила, що також постраждали системи електронної пошти. First American повідомила Комісію з цінних паперів і бірж, що 20 грудня 2023 року вона ізолювала деякі системи для усунення інциденту та працює над відновленням нормальної роботи, хоча тривалість і ступінь збою залишаються невизначеними.

Попри те, що минув тиждень після порушення, основний вебсайт і допоміжні сайти все ще не відновили повністю свою роботу. Хоча природа атаки не розголошується, вона схожа на інцидент з програмами-вимагачами, хоча жодна конкретна група програм-вимагачів не взяла на себе відповідальність. Клієнти висловлювали занепокоєння в соціальних мережах щодо фінансових втрат і комунікації компанії та врегулювання ситуації.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

GOOGLE ВІДКРИВ НОВИЙ ЦЕНТР КІБЕРБЕЗПЕКИ В ІСПАНІЇ

4 грудня видання Euroactive пише про подію кінця листопада 2023 року - відкриття нового центру кібербезпеки Google в Іспанії. Google Safety Engineering Center (GSEC) у Малазі є третім таким центром у Європі. У 2019 році Google запустив центр у Мюнхені, який зосереджується на розробці конфіденційності та безпеки, а у 2020 році ще один у Дубліні, щоб розв'язати питання відповідальності за контент. Із запуском GSEC Màlaga Google також оголосила про виділення 10 мільйонів доларів США на розвиток навичок кібербезпеки та навчання в європейських університетах і допомогу місцевим громадським організаціям які займаються питаннями цифрової грамотності.

МАЙБУТНЄ КІБЕРБЕЗПЕКИ 2030: НОВІ ОСНОВИ

5 грудня Центр довгострокової кібербезпеки Каліфорнійського університету в Берклі (CLTC), Центр кібербезпеки Всесвітнього економічного форуму та Інститут громадських досліджень CNA опублікували звіт про те, «як цифрова безпека може розвиватися протягом наступних 5-7 років». Серед іншого, дослідники зазначають, що для країн, що розвиваються існує вікно можливостей, щоб запровадити принцип «безпека за дизайном», які здебільшого не змогли впровадити країни з першої хвилі цифровізації. «Особи, які приймають рішення, повинні стежити за темпами цифровізації та здатністю населення безпечно і надійно інтегрувати нові технології,» – вважають автори звіту.

ЯК КОМАНДАМ З КІБЕРБЕЗПЕКИ ПІДГОТУВАТИСЯ ДО ПОБІЧНИХ ЕФЕКТІВ ГЕОПОЛІТИЧНОЇ КРИЗИ

У статті Крістофера Вайта (Christopher Whyte), опублікованій 5 грудня виданням CSOonline, обговорюється, як команди з кібербезпеки можуть підготуватися до кібератак під час геополітичних криз, на прикладі таких конфліктів, як війна між росією та Україною чи Ізраїлем та ХАМАС. Геополітичні кризи призводять до різноманітних викликів кібербезпеці, цілями атак стають компанії приватного сектора. У статті представлено класифікацію атак на деградацію, перформативність, сигналізацію та роїння. Автор підкреслює потребу для команд з кібербезпеки розуміти мотиви, що стоять за кібератаками, і пропонує проактивний підхід до ефективного управління ризиками. Основна увага зосереджена на зв'язку кризового хакерства з профілем ризику організації та врахуванні геополітичних аспектів у плануванні кібербезпеки.

ПРОГНОЗИ ЩОДО КІБЕРБЕЗПЕКИ TRUSTWAVE 2024

19 грудня фахівців Trustwave оприлюднили низку своїх прогнозів для сфери кібербезпеки на 2024 рік. Серед них:

- генеративний штучний інтелект буде відігравати більшу роль у сфері кібербезпеки, а компанії повинні почати серйозно розглядати етичні наслідки ШІ та конфіденційність, а також його організаційне прийняття та визначити, чи використовуватимуть вони генеративний ШІ для внутрішнього чи зовнішнього використання;
- у зв'язку з майбутніми виборами в США існує підвищений ризик кібератак на виборчі системи, бази даних виборців та виборчу інфраструктуру.
- дефіцит талантів у сфері кібербезпеки буде зростати, а потреба в талановитих збережеться. Організації можуть допомогти усунути розрив, підвищивши кваліфікацію своєї поточної робочої сили;
- системи державного сектору (США) мають багато застарілих платформ, які потребують інновацій або додаткового захисту, щоб залишатися безпечними;
- широкомасштабні атаки ranasomware продовжуватимуть зростати, оскільки вони забезпечують дуже високу віддачу від інвестицій для суб'єктів загрози.

ПІВНІЧНОКОРЕЙСЬКА ГРУПА APT LAZARUS GROUP ВИКОРИСТОВУЄ МОЖЛИВОСТІ TELEGRAM ДЛЯ КІБЕРАТАК

11 грудня Cisco Talos повідомило про виявлення нової масштабної операції північнокорейської групи APT Lazarus Group яку експерти назвали Operation Blacksmith. Операція Blacksmith передбачає використання CVE-2021-44228, також відомого як Log4Shell, і використання раніше невідомого RAT на основі DLang, що використовує Telegram як канал C2 (для приймання команд, передачі їхніх результатів і навіть для вхідної та вихідної передачі файлів.). Ця кампанія спрямована на підприємства в усьому світі, з акцентом на виробничі організації, сільськогосподарські та компанії з фізичної охорони.

NSA ОПУБЛІКУВАЛО РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ ПРОГРАМНО-ВИЗНАЧЕНИХ МЕРЕЖЕВИХ КОНТРОЛЕРІВ

12 грудня NSA на своєму сайті поширило рекомендації «Управління ризиками від програмно визначених мережевих контролерів» (Software Defined Networking Controllers). У документів містяться рекомендації, які допоможуть мережевим адміністраторам Систем національної безпеки (NSS), Міністерства оборони (DoD) і Defense Industrial Base (DIB) зменшити ризики, пов'язані з програмними рішеннями для керування та налаштування програмно визначених мережевих контролерів (SDNC). SDNC дозволяють підприємствам налаштовувати мережеві політики та політику безпеки, а також контролювати доступ до програм із централізованого місця. Це зменшує кількість окремих пристроїв, до яких адміністратор має отримати доступ, щоб підтримувати їх оновлення. SDNC забезпечують вигідне централізоване керування корпоративною мережею, але таке централізоване керування робить їх пріоритетною ціллю для зловмисників.

КІБЕРЗЛОЧИНЦІ ВИКОРИСТОВУЮТЬ ОСОБЛИВОСТІ ЗАКОНОДАВСТВА ШТАТУ ВАЙОМІНГ ДЛЯ ГЛОБАЛЬНИХ ЗЛОЧИННИХ ОПЕРАЦІЙ

13 грудня Reuters опублікувала велике дослідження щодо активності кіберзлочинців із використанням особливостей законодавства штату Вайомінг, що дозволяє їм швидко та анонімно створювати легальні компанії, захищені високим рівнем анонімності для самих злочинців. Також трафік компаній, які зареєстровані в цьому штаті, захищено американським законодавством, що призвело до росту кібератак типу DDoS саме тими групами, які мають зареєстровані підставні компанії в цьому штаті. Ця ситуація викликає занепокоєння у кіберекспертів щодо перетворення Вайомінгу на «Віртуальний Дикий Захід». Вони закликають до перегляду законодавства у цій сфері.

ЗРОСТАЄ ЗАГРОЗА ДЛЯ МОБІЛЬНОГО БАНКІНГУ – ЗВІТ ZIMPERIUM ЗА 2023 РІК

У звіті кібербезпекової компанії Zimperium, опублікованому на початку грудня, зазначено, що 2013 року 29 сімейств шкідливих програм використовувалися для ураження 1800 банківських додатків у 61 країні. Для порівняння: у 2022 році 10 сімейств зловмисного програмного забезпечення були націлені на 600 банківських програм. Це підкреслює зростання загрози в цьому секторі. Звіт містить основні результати дослідження, топ таргетованих фінансових програм, нові можливості шахрайства, крадіжки та захоплення облікових записів, найкращі методи боротьби зі зловмисним програмним забезпеченням.

НОВА АТАКА 5GHOUL ВПЛИВАЄ НА ТЕЛЕФОНИ 5G ІЗ ЧІПАМИ QUALCOMM І MEDIATEK

8 лютого видання BleepingComputer повідомило, що дослідники з Сінгапурського університету технологій і дизайну виявили низку вразливостей, що впливають на реалізацію прошивки модемів мобільної мережі 5G від Qualcomm і MediaTek. Недоліки під загальною назвою 5Ghoul можуть бути використані, щоб спричинити збої або зниження рівня мережі. Дослідники виявили, що це стосується понад 710 моделей смартфонів, які зараз є на ринку. Разом з тим, вони підкреслюють, що фактична кількість постраждалих моделей може бути більшою, оскільки код мікропрограми часто використовується для різних версій модемів.

СІМ ОСНОВНИХ ТЕНДЕНЦІЙ, ЯКІ ФОРМУВАТИМУТЬ БЕЗПЕКУ SAAS У 2024 РОЦІ

У статті, опублікованій The Hacker News 18 грудня, обговорюються ключові тенденції, що впливатимуть на безпеку SaaS у 2024 році. Також надається уявлення про те, як організації можуть вирішити ці виклики. Тенденції включають:

- Демократизація SaaS: перехід до децентралізованого впровадження SaaS розширює можливості бізнес-підрозділів, але вимагає від команд безпеки пошуку нових способів співпраці та надання вказівок щодо різноманітних програм SaaS.
- ITDR (Identity Threat Detection & Response): визнаючи ідентифікацію основним периметром для додатків SaaS, очікується, що організації запровадять підходи ITDR для виявлення загроз і ефективного реагування на них.
- Транскордонна відповідність: дедалі складніші нормативні вимоги в різних країнах призведуть до більшої географічної специфіки орендарів, вимагаючи незалежної конфігурації та безпеки для кожного.
- Неправильно налаштовані параметри: нещодавні випадки неправильних конфігурацій, що спричинили витік даних, підкреслюють важливість захисту програм SaaS від неправильних конфігурацій, які можуть призвести до значної шкоди.
- Програми сторонніх розробників: використання програм сторонніх розробників створює ризики, оскільки командам безпеки потрібне бачення інтегрованих програм, розуміння дозволів і оцінка цінності та ризику, пов'язаного з кожною програмою.
- Кілька пристроїв і віддалена робота. Через те, що значна частина співробітників працює віддалено, організації зіштовхуються з проблемами забезпечення доступу SaaS з різних пристроїв, особливо некерованих або незахищених.
- Прийняття SSPM (SaaS Security Posture Management): організації звертаються до інструментів SSPM у поєднанні з можливостями ITDR, щоб автоматично відстежувати конфігурації, виявляти загрози та реагувати на них, а також покращувати загальну безпеку програм SaaS.

5. КРИТИЧНА ІНФРАСТРУКТУРА

КОМПАНІЯ DRAGOS ПРОПОНУЄ БЕЗКОШТОВНУ ТЕХНОЛОГІЮ КІБЕРБЕЗПЕКИ ОТ ДЛЯ НЕВЕЛИКИХ КОМУНАЛЬНИХ ПІДПРИЄМСТВ США

6 грудня компанія Dragos оголосила, що пропонує безкоштовне програмне забезпечення безпеки операційних технологій (ОТ) та інші ресурси невеликим компаніям з електроенергії, водопостачання та природного газу в Сполучених Штатах через свою Програму захисту громади (Community Defense Program). Програма дозволяє американським комунальним підприємствам, які мають річний дохід менше ніж 100 мільйонів доларів США, безкоштовно користуватися перевагами технології Dragos. Учасники отримають необмежений доступ до платформи Dragos, яка забезпечує видимість мережі ОТ і можливості моніторингу, дозволяючи організаціям інвентаризувати свої активи, виявляти загрози, керувати вразливими місцями та проводити пошук загроз.

ПРОІРАНСЬКІ ХАКЕРИ СПРИЧИНИЛИ ДВОДЕННЕ ВІДКЛЮЧЕННЯ ВОДИ У ВІДДАЛЕНОМУ РЕГІОНІ ІРЛАНДІЇ

На початку грудня проіранське хакерське угруповання Cyber Av3ngers атакувала систему водопостачання в сільській місцевості Ерріс графства Мейо (Ірландія), що позбавило водопостачання близько 160 домогосподарств протягом двох днів.

Інцидент став результатом використання вразливості в програмованих логічних контролерах (PLC) Unitronics. Цей тип обладнання широко використовується у водному секторі та інших галузях, таких як енергетика, виробництво харчових продуктів та напоїв, а також охорона здоров'я.

Національний центр кібербезпеки Ірландії (NCSC) виявив і повідомив всіх власників обладнання, уразливого до цього типу кібератак у країні. CISA додало помилку Unitronics до свого каталогу відомих використаних вразливостей під назвою CVE-2023-6448.

США ПОПЕРЕДИЛИ, ЩО УГРУПОВАННЯ ІРАНСЬКИХ ТЕРОРИСТІВ ЗЛАМАЛО «КІЛЬКА» ВОДНИХ ОБ'ЄКТІВ США

Згідно з повідомленням видання The Register від 4 грудня, щонайменше три групи, афілійовані з іранським Корпусом вартових ісламської революції (КВІР), заявили про кібератаки на водопровідні компанії: Haghjoyan, CyberToufan Group і YareGomnam Team.

Видання з розчаруванням підкреслює, що банда не потребувала складної тактики, щоб здійснити цю атаку: Cyberav3ngers, ймовірно, зламали водопровідні об'єкти в США, використовуючи стандартні паролі для доступних через Інтернет ПЛК.

На фоні цих загроз Microsoft спільно з деякими партнерами розпочали пілотну програму кібербезпеки, щоб надати персоналізоване навчання кіберготовності для підприємств водопостачання та навчання їх працівників.

FORESCOUT VEDERE LABS РОЗКРИВАЄ 21 НОВУ ВРАЗЛИВІСТЬ, ЩО ВПЛИВАЄ НА МАРШРУТИЗАТОРИ OT/IOT

5 грудня компанія Forescout Vedere Labs повідомила, що виявила загалом 21 нову вразливість, що впливає на стільникові маршрутизатори Sierra Wireless AirLink і деякі компоненти з відкритим кодом, такі як TinyXML і OpenNDS, які використовуються в багатьох інших продуктах. У звіті йдеться про такі тенденції:

- кількість вразливостей маршрутизаторів та мережевої інфраструктури зростає. Принаймні з 2020 року вразливості в мережевій інфраструктурі постійно входять до числа найбільш використовуваних;
- спонсоровані державою суб'єкти розробляють спеціальні шкідливі програми для використання маршрутизаторів для довгострокових атак та шпигунства, тоді як кіберзлочинці використовують їх для домашніх проксі-серверів і для створення ботнетів;
- уразливості в пристроях OT/IoT часто виникають через недоліки конструкції, такі як використання жорстко закодованих облікових даних і сертифікатів. Ці вразливості легше використовувати в пристроях OT/IoT через відсутність ефективних засобів захисту від експлойтів;
- компоненти ланцюга постачання, такі як програмне забезпечення з відкритим кодом, що надається третіми сторонами, можуть бути дуже ризикованими та збільшувати поверхню атаки критично важливих пристроїв, що призводить до вразливостей, які власникам активів може бути важко відстежити та пом'якшити.

МАЙЖЕ ВСЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ЩО ВИКОРИСТОВУЄТЬСЯ ЕНЕРГЕТИЧНИМИ КОМПАНІЯМИ США, МІСТИТЬ КОД ВІД РОСІЙСЬКИХ І КИТАЙСЬКИХ РОЗРОБНИКІВ – FORTRESS INFORMATION SECURITY

4 грудня Fortress Information Security оприлюднила наступні висновки дослідження Специфікації програмного забезпечення (SBOM) для програмного забезпечення, яке зазвичай використовується енергетичними компаніями США:

- 90 відсотків із понад 200 програмних продуктів, які перевірила Fortress, містили компоненти від розробників, які вказали, що вони з росії та Китаю. З 7918 розглянутих компонентів 13 відсотків були внесені російськими та китайськими розробниками;
- кількість часток коду з росії та Китаю значно більша, ніж з інших країн з підвищеним ризиком, таких як Куба, Іран та Північна Корея;
- програмне забезпечення з російським або китайським кодом, перевірене дослідженнями Fortress, має у 2,25 рази більше шансів мати вразливості. Ще більше занепокоєння викликає те, що програмне забезпечення має втричі більше шансів мати критичні вразливості;
- приблизно 7% усіх вразливостей були критичними. Мікропрограмне забезпечення мало найбільше вразливостей (в середньому 620 вразливостей на продукт), але операційні системи мали стільки ж критичних вразливостей – 12%;
- аналіз SBOM, проведений дослідниками Fortress, показав, що вразливості, вбудовані в програмне забезпечення, яке виконує критичні операції та компоненти, чекають понад чотири роки, не привертаючи уваги постачальників, продавців або надавачів комунальних послуг. Середній вік критичних вразливостей склав майже три роки – 952 дні.

ЧЕРЕЗ КІБЕРАТАКУ НА ЯДЕРНУ ДОСЛІДНИЦЬКУ СТАНЦІЮ В АЙДАХО ХАКЕРИ ОТРИМАЛИ ДОСТУП ДО ДАНИХ ПОНАД 45000 ОСІБ

Видання The Record повідомило 14 грудня, що інформацію про понад 45 000 людей було викрадено через кібератаку на федеральну лабораторію ядерних досліджень наприкінці листопада.

Національна лабораторія Айдахо (INL) подала до регуляторних органів повідомлення що 45 047 співробітників, колишніх співробітників, подружжя та їхніх утриманців мали конфіденційну інформацію, що зберігалася у «дистанційному центрі обробки даних», до якого 20 листопада отримали доступ хакери.

Відома ядерна дослідницька лабораторія Міністерства енергетики США, яка розташована поблизу Айдахо-Фоллз, відома новаторськими дослідженнями ядерних реакторів і наразі налічує понад 5700 співробітників.

ХАКЕРИ ВИВЕЛИ З ЛАДУ 60% АВТОЗАПРАВОК В ІРАНІ

18 грудня невідомі зловмисники (Іран звинувачує в цьому ізраїльських та американських хакерів) змогли відключити на АЗС онлайн-системи, що спричинило довгі автомобільні черги біля деяких станцій Тегерану, а ще частина були повністю закриті.

6. АНАЛІТИЧНІ ОЦІНКИ

ІНФОРМАЦІЙНІ СИСТЕМИ БРИТАНСЬКОГО ЯДЕРНОГО ОБ'ЄКТА SELLAFIELD МОЖЛИВО БУЛИ ЗЛАМАНІ КИТАЙСЬКИМИ ТА РОСІЙСЬКИМИ ХАКЕРАМИ

4 грудня газета The Guardian оприлюднило результати свого розслідування щодо ядерного об'єкта Sellafield. Sellafield – це місце поводження з ядерними відходами, яке, згідно з Управлінням ядерного регулювання Великобританії (ONR), обробляє більше радіоактивних відходів в одному місці, ніж будь-який інший ядерний об'єкт у світі. В розслідуванні вказується, що перші злами були виявлені ще в 2015 році, і що зловмисне програмне забезпечення було «вбудовано в комп'ютерні мережі Sellafield». ONR та Sellafield Ltd загалом заперечують наявність проблеми і вказують, що не мають жодних доказів того, що системи Sellafield були зламані державними суб'єктами у спосіб, описаний у звіті.

Тіньовий секретар з енергетичної безпеки опозиційної Лейбористської партії Е. Д. МІЛІБЕНД сказав, що «уряд зобов'язаний сказати, коли він вперше дізнався про ці звинувачення, які заходи вжив він і регулятор, і надати гарантії щодо захисту нашої національної безпеки».

Представник Департаменту енергетичної безпеки та Net Zero відповів на критику в The Guardian: «Багато порушених питань є історичними, і регулятор деякий час працював із Sellafield, щоб забезпечити впровадження необхідних покращень. Ми очікуємо регулярних повідомлень про розвиток ситуації».

УГОРЩИНА Є ЛІДЕРОМ В ІМПЛЕМЕНТАЦІЇ NIS2 ДИРЕКТИВИ – ЕКСПЕРТИ PWC

12 грудня експерти з кібербезпеки PwC оприлюднили оцінки успіху європейських країн на шляху імплементації NIS2 Директиви – загальноєвропейської рамки кібербезпеки прийнятої на початку 2023 року. Наразі лідерами з впровадження цього документу є Угорщина, Чехія та Німеччина. Найменший прогрес – Польща, Норвегія та Великобританія.

5 КЛЮЧОВИХ РІШЕНЬ УРЯДУ США У СФЕРІ КІБЕРБЕЗПЕКИ У 2023 РОЦІ

28 грудня Марк Стоун з Security Intelligence опублікував свій огляд найбільш важливих рішень уряду США у 2023 році, що стосується питань кібербезпеки. До них відносяться: нова Стратегія кібербезпеки США, Імплементаційний план до Стратегії кібербезпеки США; оприлюднення NIST Cybersecurity Framework 2.0 (CSF); публікацію найкращих практик захисту домашніх мереж від NSA; поява Указу президента Байдена щодо штучного інтелекту.

ОГЛЯД КІБЕРБЕЗПЕКОВИХ ТЕНДЕНЦІЙ ВІД TRENDMICRO

7 грудня кібербезпекова компанія Trendmicro опублікувала власну оцінку ключових тенденцій кібербезпеки у 2023 році. Серед ключових висновків:

- вплив штучного інтелекту (зокрема, ChatGPT) на кібербезпекову ситуацію був перебільшеним (помітним був лише вплив у сфері фішингу);
- технології блокчейну зайняли свою скромну нішу виключно у фінансовому секторі і перестали сприйматись як проривна технологія у сфері кібербезпеки;
- збільшення кількості різних інструментів кібербезпеки в одній установі часто веде до більших проблем ніж до більшої безпеки, адже ускладнює їх адміністрування фахівцями організацій;
- люди залишаються слабкою ланкою у сфері кібербезпеки – цьому сприяє загальна негативна культура в організаціях, яка не заохочує людей сповіщати про кібербезпекові проблеми;
- організації нереалістично формують запити на фахівців з кібербезпеки, що ускладнює їх пошук і формує брак робочої сили.

НАЙПОШИРЕНІШИМ RANSOMWARE ДЛЯ АТАКИ НА ВИРОБНИЧИЙ СЕКТОР Є LOCKBIT 3.0 – ДАНІ TRUSTWAVE

6 грудня Trustwave опублікувало своє дослідження «Ландшафт загроз: дані розвідки загроз від Trustwave та стратегії пом'якшення» (Threat Landscape: Trustwave Threat Intelligence Briefing and Mitigation Strategies). В ньому робиться акцент на загрози промисловому сектору, який продовжує свою цифрову трансформацію та чиї операційні технології (OT), промислові системи управління (ICS) і диспетчерський контроль і збір даних (SCADA) стають все більш схильними до кібератак. Звіт вказує на те, що Lockbit 3.0 є основним ransomware, яке використовується для атак на виробників – 36% усіх таких атак. Також звіт вказує, що географія атак на промисловий сектор досить обмежена – 63% жертв є компаніями зі Сполучених Штатів, за ними йдуть Великобританія з 14% і Франція 9%.

КІБЕРАТАКИ МОЖУТЬ МАТИ ОСОБЛИВО РУЙНІВНИЙ ХАРАКТЕР ДЛЯ ЛАНЦЮЖКІВ ПОСТАЧАННЯ – RAND CORPORATION

19 грудня RAND Corporation опублікував результати дослідження проведеного на запит Науково-дослідної лабораторії ВПС (AFRL) щодо того, як кіберризики можуть бути порівняні (з точки зору наслідків) з іншими ризиками для ланцюгів постачання оборонно-промислового комплексу (мова йшла про стандартні, а не програмні ланцюги постачання). Серед основних висновків:

- кіберподії можуть представляти більшу загрозу (ніж фізичні загрози ланцюжку постачання) з точки зору характеру їх початку, тривалості, видимості та охоплення;
- деякі звичайні способи реагування на ризики ланцюга постачання можуть не перешкоджати, а навіть підвищувати ризики від кібератак;
- зусилля приватного сектора щодо управління ризиками можуть не відповідати потребам національної безпеки.

66% DDOS-АТАК Є ПОЛІТИЧНО МОТИВОВАНИМИ – ДОСЛІДЖЕННЯ ENISA

У новому звіті Агентства Європейського Союзу з кібербезпеки (ENISA) оприлюдненого 6 грудня, підкреслюється, що для 66% атак типу DDoS основним мотивом є політичні погляди їх ініціаторів. Аналіз базується на 310 підтверджених DDoS-атаках за період з січня 2022 року по серпень 2023 року. Серед інших важливих висновків: найбільше від таких атак страждає сектор державного управління, на який припало 46% атак, а близько 50% всіх глобальних інцидентів виявилися пов'язаними з російсько-українською війною.

В 2023 РОЦІ КИТАЙ ТА РОСІЯ ЗАЛИШАЛИСЬ ГОЛОВНИМИ ДЖЕРЕЛАМИ ЗАГРОЗ ДЛЯ США – ЗВІТ NSA ЗА 2023 РІК

19 грудня NSA опублікувало річний звіт про свою діяльність та оцінки 2023 року. В документі підкреслюється, що спонсоровані Китаєм та росією хакерські групи були ключовою загрозою у 2023 році, якій протистояло NSA. Звіт відмічає операцію китайських хакерів щодо проникнення у мережі об'єктів критичної інфраструктури США, а також кібершпигунську операцію Snake, яка була реалізована 16 центром фсб і яка вплинула на 50 країн.

CISA КОНСТАТУЄ ПОЗИТИВНИЙ ВПЛИВ ВІД ЗАПРОВАДЖЕННЯ ФЕДЕРАЛЬНИМИ ОРГАНАМИ CYBERSECURITY PERFORMANCE GOALS (CPG)

5 грудня CISA повідомила, що виявила чіткі позитивні тенденції щодо двох вимог CPG (CPG Goal 1.E та CPG Goal 2.W) у майже 3500 організаціях, які брали участь у дослідженні. CPG (Cybersecurity Performance Goals) є набором базових практик/рекомендацій кібербезпеки (побудованих на основі NIST CSF) який розроблено CISA та рекомендовано до впровадження у федеральних відомствах.

За результатами дослідження відзначається стала тенденція до зменшення середньої кількості відомих вразливостей (known exploited vulnerabilities, KEVs) в мережах федеральних організацій (відмічається через службу сканування вразливостей CISA) та видаленні шкідливих інтернет-сервісів.

ГРУПА КІБЕРШПИГУНСТВА SANDMAN ПОВ'ЯЗАНА З КИТАЄМ

У спільному звіті, опублікованому 12 грудня, компанії SentinelOne, Microsoft та PwC демонструють зв'язок нещодавно викритого APT Sandman з ймовірно розташованими в Китаї кластерами загроз, які використовують бекдор KEYPLUG. «За нашою оцінкою, існують значні збіги в операційній інфраструктурі, націлюванні та TTP, які пов'язують Sandman APT із супротивниками з Китаю, які використовують бекдор KEYPLUG, зокрема STORM-0866/ Red Dev 40. Це підкреслює складний характер ландшафту китайських загроз», – зазначає SentinelOne.

КИТАЙСЬКІ ХАКЕРИ РОЗШИРЮЮТЬ СВОЇ СТРАТЕГІЧНІ ЦІЛІ

У статті на Lawfare Blog, опублікованій 5 грудня, Аліза Себеніус досліджує загрозу, що розвивається у кіберсфері з боку Китаю, зосереджуючись на нещодавній зміні стратегії, спрямованої на критичну інфраструктуру на додаток до традиційного економічного шпигунства. Агентство з кібербезпеки та безпеки інфраструктури США (CISA) і Міністерство оборони США попереджають про намір Китаю зруйнувати та пошкодити критично важливу оборонну інфраструктуру, особливо під час конфлікту, що потенційно може спричинити серйозні наслідки.

Хоча економічне шпигунство залишається проблемою, кібердіяльність Китаю тепер також поширюється на вплив на операції з використанням штучного інтелекту та дезінформації. У статті наголошується на необхідності для США впоратися з цими багатогранними кіберзагрозами з боку Китаю, що потребує комплексної стратегії, яка включає співпрацю з технологічними компаніями, стимули для протидії економічному шпигунству та постійні інвестиції в оборону для забезпечення критичної інфраструктури. Попри інші невідкладні геополітичні кризи, довгострокові стратегічні виклики Китаю в кіберпросторі вимагають першочергової уваги.

ЗВІТ BLACKFOG ПРО СТАН ПРОГРАМ-ВИМАГАЧІВ

Згідно з звітом компанії BlackFrog, у листопаді було зафіксовано вісімдесят дев'ять публічно оприлюднених атак програм-вимагачів, що є найбільшою кількістю, з моменту створення блогу компанії State of Ransomware у 2020 році. Ця цифра на 112% перевищує кількість зареєстрованих атак у 2022 році. LockBit і BlackCat залишаються двома найпопулярнішими варіантами, які здійснили 20 і 15 атак відповідно. Охорона здоров'я була найбільш постраждалою галуззю: зареєстровано 21 інцидент.

ДОСЛІДЖЕННЯ ПРОМИСЛОВОЇ КІБЕРБЕЗПЕКИ РОЗКРИВАЄ ПРОБЛЕМИ ТА ПРІОРИТЕТИ НА ТЛІ ПОСТІЙНИХ ЗАГРОЗ ВИМАГАЧІВ

6 грудня Claroty опублікувала результати опитування щодо атак програм-вимагачів на промислові організації, виявивши, що 75% організацій у промисловому секторі зазнали атаки програм-вимагачів минулого року: «З цих 75% респондентів 69% заплатили викуп, а більша частина (54%) тих, хто заплатив викуп, зазнали фінансових наслідків у 100 000 доларів США або більше».

Крім того, «45% респондентів кажуть, що Директиви безпеки TSA мали найбільший вплив на пріоритети безпеки та інвестиції їхньої організації, за ними йдуть CDM DEFEND (39%) та ISA/IEC-62443 (37%)».

ЗЛОМ МОЗКУ ЛЮДИНИ: ВИКОРИСТАННЯ ВРАЗЛИВОСТЕЙ НА «ПЕРШІЙ ЛІНІЇ КІБЕРЗАХИСТУ»

7 грудня видання The Hacker News розмістило статтю, яка аналізує якості людини, які експлуатують хакери, з метою контролю за її поведінкою. В статті наводяться конкретні приклади та механізми використання емоцій та реакції людини, щоб змусити її робити бажані для зловмисників дії. Стаття також містить підказки, як можна протидіяти таким маніпуляціям за допомогою аналітичних питань.

МАЙЖЕ 90% IT-СПЕЦІАЛІСТІВ ВІДЧУВАЛИ ГОТОВНІСТЬ ДО КІБЕРАТАКИ НА ОСНОВІ ПАРОЛЯ, АЛЕ БІЛЬША ЧАСТИНА СТАЛИ ЖЕРТВАМИ ТАКИХ АТАК

Опубліковане 12 грудня опитування, проведеного постачальником безпарольного оркестрування для всієї організації Axiad щодо стану автентифікації за 2023 рік, яке охопило понад 200 американських IT-фахівців із різних галузей, продемонструвало такі ключові результати:

- 39% фахівців найбільше бояться фішингових атак, тоді як 49% вважають, що це найімовірніша атака;
- 88% вважають, що їхня компанія готова захищатися від кібератак на основі пароля, але 52% стали жертвами кібератак за останній рік;
- попри проблеми з паролями, 93% все ще використовують паролі, посилаючись на страх перед змінами (64%), потенційну заміну технології (54%), обмеження часу (51%) і брак персоналу (25%) як причини;
- відповідаючи на питання про використання паролів, респонденти звинуватили IT-персоналу (35%), кінцевих користувачів (32%), служби безпеки (25%) і керівництво (8%);
- для майбутніх технологій 45% планують використовувати технологію без пароля, а 27% обирають стійку до фішингу багатофакторну автентифікацію (MFA);
- рекомендації Агентства з кібербезпеки та безпеки інфраструктури (CISA) найбільше вплинули на стратегію автентифікації респондентів (41%), за нею йдуть Національний інститут стандартів і технологій (NIST) (26%) і Адміністративно-бюджетне управління Білого дому (OMB)) (13%).

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

НА ЗАСІДАННІ НКЦК УХВАЛИЛИ РІШЕННЯ ПРО ПОСИЛЕННЯ ЗАХИЩЕНОСТІ СИСТЕМИ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ УКРАЇНИ, ЇЇ ОБ'ЄКТІВ ТА ІНФРАСТРУКТУРИ

21 грудня 2023 року відбулося засідання Національного координаційного центру кібербезпеки при РНБО України. У ході засідання учасники обговорили важливі питання щодо створення системи оброблення великих даних за технологіями Big Data в інтересах безпеки і оборони держави, за результатами чого були надані відповідні доручення. Також було розглянуто низку законодавчих ініціатив у сфері кібербезпеки, запропонованих СБ України, зокрема спрямованих на забезпечення ефективної протидії посяганням на основи національної безпеки України, що здійснюються з використанням кіберпростору.

У закритому режимі було ухвалено низку рішень, спрямованих на невідкладне посилення захищеності системи електронних комунікацій України, її об'єктів та інфраструктури. Також під час засідання учасники обговорили пріоритетні напрями реалізації Талліннського механізму та питання оптимізації міжнародної взаємодії у сфері кібербезпеки.

НКЦК ПРОВІВ КОМАНДНО-ШТАБНІ НАВЧАННЯ СТРАТЕГІЧНОГО РІВНЯ

Національний координаційний центр кібербезпеки при РНБО України втретє провів щорічні командно-штабні навчання (ТТХ) стратегічного рівня «Національна кіберготовність – 2023», які спрямовані на зміцнення національної системи кібербезпеки. У ході навчань експерти відпрацювали механізми та навички ухвалення стратегічних рішень під час реагування на масштабні кібератаки та спеціальні інформаційні операції, що супроводжують подібні атаки. Вперше сценарій включав завдання щодо відпрацювання наступальних заходів активної кібероборони.

RECORDED FUTURE ПРОДОВЖУЄ НАДАВАТИ КРИТИЧНО ВАЖЛИВІ РОЗВІДДАНІ ДЛЯ ЗАХИСТУ УКРАЇНИ ВІД КІБЕР- ТА ФІЗИЧНИХ ЗАГРОЗ

Найбільша у світі приватна розвідувально-аналітична компанія Recorded Future продовжить допомагати Україні захищати критичну інфраструктуру від військової та кіберагресії росії у 2024 році. Загальна сума інвестицій підтримку України у цьому році становитиме понад 23 млн $.

Від початку повномасштабного вторгнення компанія надавала розвідувальні дані для захисту критичної інфраструктури України, допомагала розслідувати воєнні злочини росіян, відкрила доступ до програмної платформи Intelligence Cloud на понад 10 млн $.

ІСЛАНДІЯ ПРИЄДНАЛАСЬ ДО ІТ-КОАЛІЦІЇ

Ісландія приєднується до ІТ-коаліції. З початку повномасштабного вторгнення росії в Україну Ісландія надавала гуманітарну, економічну та безпекову підтримку Україні здебільшого через міжнародні організації – ООН, Світовий банк, НАТО та інші багатонаціональні форуми.

Міністр оборони України Рустем Умєров подякував уряду та народу Ісландії за потужну підтримку, завдяки якій Україна зможе посилити сфери інформаційних технологій, зв'язку та кібербезпеки. Наразі до складу ІТ-коаліції входять вісім країн: Естонія, Люксембург, Бельгія, Данія, Ісландія, Латвія, Литва, Японія. Велика Британія та Італія також оголосили про свій намір приєднатися.

НКЦК ПОГЛИБЛЮЄ СПІВПРАЦЮ З КОМПАНІЄЮ META ДЛЯ ПОСИЛЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРСТІЙКОСТІ УКРАЇНИ

Керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Наталія Ткачук провела робочу зустріч з керівницею регіональної державної політики Meta в Центральній і Східній Європі Катериною Крук. Обговорено питання стратегічної співпраці у сфері протидії інформаційним атакам, а також боротьби з фінансовим фішингом. Також під час зустрічі з-поміж іншого було обговорено питання співпраці щодо системи фільтрації фішингових доменів Protective DNS і протидії поширенню фішингових кампаній в соціальних мережах.

МІНЦИФРА ТА ECSO ПІДПИСАЛИ МЕМОРАНДУМ ПРО СПІВПРАЦЮ

Міністерство цифрової трансформації України та Європейська організація кібербезпеки (ECSO) уклали меморандум про співробітництво. Це дасть змогу посилити систему кіберзахисту України відповідно до міжнародних стандартів. А також забезпечити доступ українських підприємств та фахівців до ринку кібербезпеки ЄС. Крім цього, співпраця з ECSO дасть змогу:

- забезпечити українським фахівцям доступ до навчальних ресурсів з підвищення кваліфікації й професійного розвитку;
- організувати промоцію українських стартапів у сфері кіберзахисту та залучити інвесторів;
- забезпечити підтримку науково-технічних проєктів.

ДЕРЖСПЕЦЗВ'ЯЗКУ НАЛАГОДЖУЄ СПІВПРАЦЮ З JICA

До Державної служби спеціального зв'язку та захисту інформації завітав постійний представник офісу Японського агентства міжнародного співробітництва (JICA) в Україні Сатоші Сугімото. Японський гість мав можливість ознайомитися з роботою Служби та обговорити потенційні напрями співробітництва, зокрема, кіберзахист державних інформаційних систем, захист критичної інфраструктури, Армія дронів, забезпечення трансляції українського телебачення та радіо тощо.

КАБМІН ЗАТВЕРДИВ ПЛАН ЗАХОДІВ ЩОДО ПОДАЛЬШОЇ РЕАЛІЗАЦІЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ

Уряд ухвалив розпорядження «Про затвердження плану заходів на 2023 – 2024 роки з реалізації Стратегії кібербезпеки України». Документ визначає завдання та заходи, спрямовані на досягнення цілей Стратегії, а також встановлює індикатори та строки їх виконання. Ключовими напрямами роботи відповідно до зазначеного плану стануть: нормативно-правове забезпечення діяльності у сферах кібербезпеки, кіберзахисту та кібероборони, налагодження більш тісного співробітництва з міжнародними партнерами тощо.

КОМАНДА CERT-UA ЗДОБУЛА ПЕРШЕ МІСЦЕ НА КІБЕРНАВЧАННЯХ КОРПУСУ МОРСЬКОЇ ПІХОТИ США

Фахівці урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA вибороли перше місце на міжнародних змаганнях із кібербезпеки «Cyber Gators 2023», які відбулися на полігоні CYBER RANGES technology у місті Орландо, штат Флорида (США) та були організовані Корпусом морської піхоти США.

У змаганнях взяли участь сім команд – кіберзахисники України, США, Канади та інших країн. Навчання полягали у реалізації сценаріїв оборони від численних складних загроз. На виконання 109 завдань було виділено десять годин. Українські кіберзахисники – вклалися у шість.

МІНЦИФРА ЗАПУСТИЛА ОСВІТНІ КУРСИ ВІД CISCO НА ДІЯ.ОСВІТА

Академія Cisco переклала 9 власних освітніх курсів українською мовою, щоб допомогти українцям розширити знання в цих галузях. Серед них: вступ до кібербезпеки, мережеві пристрої та початкова конфігурація, безпека кінцевих пристроїв, захист мережі, управління кіберзагрозами тощо. Переглянути курси можна за посиланням – https://osvita.diia.gov.ua/korysni-posylannya?category=cisco-courses

ФАХІВЦІ ДЕРЖСПЕЦЗВ'ЯЗКУ ПРОЙШЛИ ПІДГОТОВКУ ДЛЯ ФАСИЛІТАТОРІВ ЗА АМЕРИКАНСЬКИМИ СТАНДАРТАМИ

Наприкінці листопада в Кракові (Польща) відбувся тренінг для фасилітаторів командно-штабних навчань. Це перший захід у рамках обміну передовими практиками та участі у забезпеченні кібербезпеки шляхом проведення курсів, тренінгів, спільних навчань та реалізації спільних кібербезпекових проєктів відповідно до Меморандуму про співробітництво щодо співпраці у сфері кібербезпеки між Держспецзв'язку і CISA.

ДЕРЖСПЕЦЗВ'ЯЗКУ ТА НІМЕЦЬКІ ПАРТНЕРИ ЗМІЦНЮЮТЬ СПІВПРАЦЮ У СФЕРІ КІБЕРБЕЗПЕКИ

За ініціативи Держспецзв'язку та за підтримки уряду Німеччини в особі Німецького товариства міжнародного співробітництва (GIZ) розробляється тренінгова програма з кібербезпеки національного рівня для фахівців, які працюють у державному секторі. ЇЇ метою є підтримка України в питанні розвитку фахівців відповідно до європейських стандартів і вимог кібербезпеки, щоб підвищити світову кіберстійкість.

Уже відбулися три пілотні навчання для держслужбовців різних категорій, які проходили онлайн і впроваджувались компанією Deloitte. Наступна фаза проєкту має розпочатись у 2024 році. У довгостроковій перспективі проєкт допоможе побудувати стійке, відкрите та безпечне кіберсередовище між європейськими партнерами та Україною, обмінюватися досвідом європейської кіберполітики та законодавства з огляду на шлях нашої країни до членства в ЄС і підвищити кадровий потенціал у сфері кібербезпеки.

ПРЕДСТАВНИКИ ДЕРЖСПЕЦЗВ'ЯЗКУ ВЗЯЛИ УЧАСТЬ У МІЖНАРОДНИХ НАВЧАННЯХ МІЖНАРОДНОГО СОЮЗУ ЕЛЕКТРОЗВ'ЯЗКУ

Представники Держспецзв'язку взяли участь у міжрегіональних навчаннях країн Європи та Азійсько-Тихоокеанського регіону, організованих Міжнародним союзом електрозв'язку (ITU). У ході відпрацювання практичних вправ у об'єднаній команді з делегацією Іспанського національного інституту кібербезпеки (INCIBE) українські кіберзахисники двічі посіли перше місце, і у ще двох вправах – друге та сьоме місце відповідно.

Окрім того, українські кіберзахисники взяли участь у панельних дискусіях про стан кібербезпеки в Європі та Азійсько-Тихоокеанському регіоні, стратегії захисту критичної інформаційної інфраструктури, національні плани реагування на кіберкризи та роль партнерства у кібердипломатії. Загалом у навчаннях взяли участь понад 70 команд та більш як 200 учасників з 40 країн світу.

ФРАНЦУЗЬКІ ПРАВООХОРОНЦІ ПРОВЕЛИ ТРЕНІНГ ДЛЯ УКРАЇНСЬКИХ ПОЛІЦЕЙСЬКИХ

Упродовж тижня правоохоронці різних відомств, зокрема співробітники Департаменту кримінального аналізу Нацполіції та Департаменту кіберполіції, удосконалювали навички у сфері кримінального аналізу. Іноземні колеги поділилися досвідом щодо використання в роботі новітніх методик і інструментів у сфері збору, оброблення, систематизації та аналізу інформації щодо запобігання і протидії злочинності. Окрема увага приділена практичним аспектам стратегічного аналізу, а також протидії кіберзлочинів.

ЗА ДОБУ СБУ ТА НАЦПОЛІЦІЯ ЛІКВІДУВАЛИ ПОНАД 100 ШАХРАЙСЬКИХ КОЛ-ЦЕНТРІВ, ЯКІ ВИКРАДАЛИ ПЕРСОНАЛЬНІ ДАНІ ТА ГРОШІ УКРАЇНЦІВ

Кіберфахівці Служби безпеки та співробітники Національної поліції провели багатоетапну спецоперацію по всій території України. У результаті комплексних заходів за одну добу було припинено діяльність понад 100 кол-центрів, які викрадали персональні дані, у тому числі паспортні відомості, номери телефонів тощо, й заощадження українців та іноземних громадян. Надалі ця інформація могла потрапляти до російських спецслужб, які використовують її для дистанційного вербування нових агентів.

РОСІЙСЬКІ ХАКЕРИ ЗА ДОПОМОГОЮ ЕЛЕКТРОННИХ ЛИСТІВ З ПОСИЛАННЯМИ НА «ДОКУМЕНТИ» АТАКУВАЛИ КОРИСТУВАЧІВ УКРАЇНИ ТА ПОЛЬЩІ

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA виявила факт розсилання протягом 15-25 грудня групою APT28 електронних листів з посиланнями на «документи», відвідування яких призводило до зараження комп'ютера шкідливими програмами. Об'єктом атаки, окрім користувачів з України, стали організації з Польщі. Більше деталей про інцидент – на сайті CERT-UA: https://cert.gov.ua/article/6276894

УРЯД ПРИЗНАЧИВ НОВОГО ГОЛОВУ ДЕРЖСПЕЦЗВ'ЯЗКУ – ЮРІЯ МИРОНЕНКА

Кабінет Міністрів призначив військовослужбовця, командира ударної роти БпЛА Юрія Мироненка на посаду Голови Державної служби спеціального зв'язку та захисту інформації України. Новий Голова анонсував, що найближчим часом представить план розвитку ДССЗЗІ.

Юрій Мироненко має досвід корпоративного управління, глибоко розуміється на тематиці БпЛА. До призначення був командиром ударної роти БпЛА, яка працює на Запорізькому напрямку.

ТЕЛЕКОМОПЕРАТОР «КИЇВСТАР» ЗАЗНАВ ПОТУЖНОЇ КІБЕРАТАКИ З БОКУ УГРУПОВАННЯ РОСІЙСЬКОГО ГРУ SANDWORM

Зранку 12 грудня у мережі Kyivstar стався масштабний технічний збій, що спричинив недоступність послуг зв'язку та інтернет у частини абонентів. У мобільному операторі підтвердили, що причиною масштабного збою в роботі зранку 12 грудня стала потужна хакерська атака, але запевнили, що персональні дані клієнтів у безпеці. Збій у мережі оператора вплинув на національний роумінг, що завадило користувачам у переході на іншого оператора. В декількох містах не працювала система оповіщення про повітряну тривогу.

Відповідальність за атаку взяло на себе одне з російських хакерських угруповань, яке російські ЗМІ називають «Солнцепек». За інформацією СБУ, воно є хакерським підрозділом головного управління генштабу Збройних сил РФ, яке таким чином публічно легалізує результати своєї злочинної діяльності. СБУ відкрила кримінальне провадження за вісьмома статтями ККУ.

Як повідомив гендиректор компанії, хакери зламали захист «Київстару» через обліковий запис одного зі співробітників.

РОСІЙСЬКІ ХАКЕРИ ВИКОРИСТОВУВАЛИ СИТУАЦІЮ З КИЇВСТАРОМ ПРИ РОЗСИЛАННІ ЛИСТІВ ЗІ ШКІДЛИВИМ ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ

Фахівці Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA зафіксували масове розсилання електронних листів з тематикою «заборгованості за договором Київстар» і вкладенням у вигляді архіву «Заборгованість абонента.zip». На електронні пошти українців приходили листи щодо «Заборгованості за договором Київстар», які містили вкладення у вигляді архіву «Заборгованість абонента.zip» з додатками у вигляді вкладених захищених паролем RAR-архівів.

Фахівці урядової команди реагування вкотре рекомендують фільтрувати на рівні поштових шлюзів електронні листи з додатками, що захищені паролями (як архіви, так і документи). Більше деталей про інцидент: https://cert.gov.ua/article/6276824

КІБЕРФАХІВЦІ ЗСУ АТАКУВАЛИ 15 САЙТІВ РОСІЙСЬКИХ ПІДПРИЄМСТВ

Кіберфахівці ЗСУ до дня російських ракетних військ стратегічного призначення, 17 грудня, атакували 15 сайтів підприємств, які беруть участь в інженерному забезпеченні військ рф. На сайтах 15 російських компаній з'явився напис «Целятся в НАТО, а попадут в москву». Так українські військові нагадали росіянам про невдалі випробування ракет «Ярс» і «Булава», які збилися з курсу під час випробувань.

8. ПЕРША СВІТОВА КІБЕРВІЙНА

РОСІЙСЬКІ ХАКЕРИ ВИКОРИСТОВУЮТЬ ВІЙНУ ІЗРАЇЛЮ ТА ХАМАС ДЛЯ ПРОВЕДЕННЯ КІБЕРШПИГУНСЬКИХ АКЦІЙ – ДАНІ IBM X-FORCE

8 грудня IBM X-Force заявила, що виявила численні документи-приманки (стосуються війни Ізраїлю та ХАМАС), які використовуються зловмисниками з ITG05, щоб полегшити доставлення ексклюзивного бекдору ITG05 Headlace.
Ця кампанія спрямована проти цілей щонайменше в 13 країнах світу (включаючи Україну, Німеччину, Угорщину, Італію, Польщу та інші) та використовує автентичні документи, створені академічними, фінансовими та дипломатичними центрами. Кампанія має високий цільовий характер. X-Force відстежує ITG05 як групу, яка, ймовірно, спонсорується російською державою, діяльність якої перетинається з такими групами постійних загроз як APT28, UAC-028, Fancy Bear і Forest Blizzard.

APT GAMAREDON ЗАЛИШАЄТЬСЯ ГОЛОВНОЮ РОСІЙСЬКОЮ КІБЕРЗАГРОЗОЮ СПРЯМОВАНОЮ НА УКРАЇНУ – ДАНІ ЗВІТУ CISCO TALOS

5 грудня кібербезпекова компанія Cisco Talos оприлюднила свій річний звіт про кібербезпекові тренди 2023 року. Окремий розділ присвячено Україні. В ньому підкреслено, що російська державна компанія APT Gamaredon залишається головним гравцем у загрозах проти України. Майже ¼ їх атак спрямована на транспортний сектор України.

ВЛІТКУ 2023 РОКУ РОСІЯ НАМАГАЛАСЬ ПРОВЕСТИ КІБЕРАТАКИ ПРОТИ ПІДПРИЄМСТВ СІЛЬСЬКОГОСПОДАРСЬКОГО СЕКТОРУ УКРАЇНИ – ЗВІТ MICROSOFT

12 компанія Microsoft оприлюднила результати свого чергового дослідження щодо ворожої активності росії в інформаційному та кіберпросторі. Серед висновків про скоординованість кібер, інформаційних та кінетичних зусиль росії щодо України згадано помітний тренд літа 2023 року, коли росія змістила фокус своїх зусиль на сільськогосподарський сектор. Це проявлялось не лише у кібератаках на системи зберігання продуктів, але кібератаках на агробізнес з метою викрадення даних, розгортання зловмисного програмного забезпечення. Серед таких прикладів згадується успішна кібератака на неназвану українську організацію з виробництва сільгосптехніки.

КІБЕРШПИГУНИ З XDSPY АТАКУЮТЬ РОСІЙСЬКИХ МЕТАЛУРГІВ ТА ПІДПРИЄМСТВА ВПК

4 грудня з посиланням на російську компанію F.A.C.C.T., The Cyber Wire повідомила, що були виявлені шкідливі розсилки, націлені на пошту одного з російських металургійних підприємств, а також НДІ, що займається розробкою та виробництвом керованої ракетної зброї. Технічні подробиці було наведено у блозі на Хабрі.

РОСІЙСЬКА APT28 ВИКОРИСТОВУВАВ ЕКСПЛОЙТ OUTLOOK ZERO-CLICK

8 грудня видання Security Week повідомило з посиланням на Palo Alto Networks, що російська державна група загроз APT28, використовувала вразливість Outlook (CVE-2023-23397) для атак, націлених на майже 30 організацій в 14 країнах, включаючи країни НАТО. Ця критична вразливість, яку можна активувати через створені повідомлення електронної пошти, не вимагаючи від одержувача відкривати електронний лист, була вперше виявлена в березні 2023 року та використовувалася APT28 приблизно 20 місяців.

Цілями атаки переважно були організації в країнах-членах НАТО, серед яких оборонні, енергетичні, транспортні та урядові організації. Попри поінформованість громадськості про експлойт, APT28 продовжувала використовувати цю вразливість, що свідчить про значну цінність отриманих розвідувальних даних для російських військових інтересів.

Це викриття сталося після нещодавнього оновлення Microsoft, яке приписує використання CVE-2023-23397 APT28, також відомому як Fancy Bear, яка сумно відома різними кібератаками, включаючи хакерські атаки під час виборів у США 2016 року.

СЕРЕД ПРОСУНУТИХ УГРУПОВАНЬ НАЙАКТИВНІШИМИ Є ХАКЕРИ З АЗІЇ – РОСІЙСЬКА ДЕРЖАВНА КОМПАНІЯ «СОЛАР» ПРЕДСТАВИЛА ТРЕНДИ КІБЕРЗАГРОЗ

У звіт російської державної компанії з кібербезпеки «Солар» зазначено, що Китай і Північна Корея є ключовими джерелами наступальних кіберкампаній проти росії у 2023 році. У звіті діяльність, пов'язана з Китаєм, визначається як агресивні кампанії кібершпигунства, націлені на російські організації, тоді як північнокорейські актори зосереджуються на зборі інформації про розробки у галузі ракетних технологій. Коментатори відзначають, що і дії викликають питання про дипломатичні відносини між рф та цими країнами, враховуючи зусилля росії зміцнити зв'язки з Китаєм і Північною Кореєю. Попри їхню ймовірну кіберактивність, москва, схоже, терпить ці дії, вірогідно, через допомогу, що її ці країни надають рф в її війні проти України. У звіті йдеться про те, що дипломатичні відносини не обов'язково поширюються на кіберпростір, підкреслюючи складну динаміку в геополітичному ландшафті.

ЛІДЕР РОСІЙСЬКОЇ ХАКТИВІСТСЬКОЇ ГРУПИ KILLNET «ЙДЕ НА ПЕНСІЮ» ТА ПРИЗНАЧИВ НОВОГО КЕРІВНИКА

Killmilk, лідер проросійської хактивістської групи Killnet, на початку грудня оголосив про свою «відставку». Новим «власником» Killnet, згідно з окремою публікацією в офіційному каналі групи в Telegram, став керівник групи Deanon Club. Він заявив, що вони з Killmilk були друзями протягом тривалого часу, і що це «людина, яка привела мене в маси».

Дві групи справді співпрацювали в минулому. У лютому цього року вони створили форум і ринок під назвою Infinity, який пропонує низку хакерських послуг і навіть платні навчальні посібники для потенційних злочинців.

У ГУР ПОВІДОМИЛИ, ЩО АТАКУВАЛИ ПОДАТКОВУ СИСТЕМУ РОСІЇ

Під час атаки спецоперації воєнним розвідникам вдалось проникнути в один із добре захищених ключових центральних серверів Федеральної податкової служби рф, а далі — у понад 2300 її регіональних серверів по всій росії, а також на території тимчасово окупованого Криму. Паралельно у такий же спосіб була атакована російська IT-компанія Office.ed-it.ru, яка обслуговувала фсп рф.

У ГУР повідомляють, що у результаті двох кібератак повністю ліквідовані конфігураційні файли, які роками забезпечували функціонування розгалуженої податкової системи рф — знищена вся база даних та її резервні копії. Зв'язок між центральним офісом у москві та 2300 російськими територіальними управліннями — паралізований, як і між фсп рф та Office.ed-it.ru, що була для податкової дата-центром (банком даних).

РОСІЙСЬКУ ЗОВНІШНЮ РОЗВІДКУ ПОМІТИЛИ У ВИКОРИСТАННІ ВРАЗЛИВОСТІ JETBRAINS

13 грудня урядові установи США, Польщі та Великобританії заявили, що російська Служба зовнішньої розвідки (СВР) використовувала вразливість у продукті чеської програмної компанії JetBrains, яка була викрита на початку цього року. Атаки, приписувані APT29, також відомій як CozyBear або Midnight Blizzard, почалися у вересні.

Численні компанії по всьому світу були скомпрометовані, що вплинуло на такі сектори, як енергетика, програмне забезпечення, обслуговування клієнтів, управління фінансами та IT. JetBrains випустила патч для цієї вразливості у вересні, але невиправлені сервери призвели до її експлуатації різними групами програм-вимагачів.

9. РІЗНЕ

ХАКЕР SOLANA DEFI ВИЗНАВ СЕБЕ ВИННИМ У ПЕРШОМУ В ІСТОРІЇ ШАХРАЙСТВІ ЗІ СМАРТ-КОНТРАКТАМИ

У справі, що стане прецедентом, Шакіб Ахмед 14 грудня визнав себе винним за звинуваченнями, пов'язаними зі зломом двох децентралізованих бірж криптовалют, включаючи липневу атаку на децентралізовану біржу Solana Nirvana Finance.

IBM CONSULTING І PALO ALTO NETWORKS ОГОЛОСИЛИ ПРО РОЗШИРЕННЯ СТРАТЕГІЧНОГО ПАРТНЕРСТВА З КІБЕРБЕЗПЕКИ

У рамках цих відносин компанії спільно пропонуватимуть розширені рішення безпеки, надані IBM Consulting Cybersecurity Services, які інтегрують технології безпеки Palo Alto Networks. Розширене партнерство спочатку буде зосереджено на двох ключових сферах: допомога компаніям у модернізації їхніх операцій безпеки та захист хмарних перетворень.

В ЄВРОПАРЛАМЕНТІ Є ПРОБЛЕМИ З КІБЕРБЕЗПЕКОЮ ВИБОРІВ

Як пише видання Politico, Європейський парламент стикається з проблемами кібербезпеки напередодні виборів у червні 2024 року. У внутрішньому огляді кібербезпеки зазначено, що його кібербезпека «ще не відповідає галузевим стандартам» і «не повністю відповідає рівню загрози», створеної спонсорованими державою хакерами. Огляд попереджає, що державні атаки на парламент стали більш численними та витонченими. Парламент став вразливим через перехід на дистанційну роботу під час пандемії. У відповідь на цей виклик, Європейський парламент планує найняти 40 нових експертів з кібербезпеки та збільшити бюджет директорату з кібербезпеки до 7 мільйонів євро у 2024 році, а у 2025 році – до 8,5 мільйонів євро.

ЯК ДІЗНАТИСЯ, ЩО ЕТИЧНИМ ХАКЕРАМ МОЖНА ДОВІРЯТИ

Згідно з опитуванням HackerOne, половина фахівців із безпеки (52%) радше погодяться з наявністю невиявлених уразливостей, ніж працюватимуть із хакерами. Компанія представила оновлення своїх продуктів Clear і Gateway, щоб усунути проблеми щодо довіри та контролю під час роботи з етичними хакерами. HackerOne Clear пропонує гнучкі рівні перевірки хакерів для забезпечення відповідності вимогам, дозволяючи організаціям адаптувати доступ до конкретних вимог перевірки. HackerOne Gateway, заснований на глобальній мережі Cloudflare, – це рішення Zero Trust Network Access (ZTNA), яке забезпечує видимість хакерської діяльності та моніторинг етичного хакерського трафіку. Оновлення спрямовані на те, щоб зробити програму безпеки HackerOne, що працює на базі людини, найбільшою довірою в галузі.