НКЦК

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

CYBER DIGEST

Огляд подій в сфері кібербезпеки,
грудень 2022

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

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

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

ЗМІСТ

ОСНОВНІ ТЕНДЕНЦІЇ

Американські урядові агенції (CISA, FBI, NSA) все частіше виходять зі спільними релізами про ворожу кіберактивність чи з рекомендаціями про поліпшення кіберзахисту організацій. Можна констатувати, що США вдалось вибудувати модель ефективної міжвідомчої співпраці принаймі з найбільш критичних питань кібербезпеки – протидія ransomware, попередження активності APT груп, зменшення загроз від атак через ланцюжки постачання. Цій скоординованій діяльності надає активну підтримку NIST, який постійно оновлює стандарти безпеки, запроваджуючи нові практики чи відмовляючись від неефективних. На цьому фоні повідомлення про проблеми окремих державних установ з їх кіберзахистом (наприклад NASA) є швидше винятком з правил.

Кібербезпека об'єктів критичної інфраструктури (OKI) знаходиться в центрі уваги як національних суб'єктів, так і приватного сектору. Країни значно посилюють відповідальність та вимоги до OKI щодо обовязкового інформування про кібератаки (Швейцарія, Великобританія). На фоні прогнозів кібербезпекових компаній про істотне зростання загроз саме OKI у 2023 році, урядові агенції (США, Сінгапуру) намагаються вживати превентивних заходів змінюючи (посилюючи) правила безпеки при одночасному наданні максимальної кількості інформаційних матеріалів, які можуть допомогти індустріальним компаніям краще убезпечити свою OKI компоненту.

Кібернавчання (національні, міжнаціональні) стають все помітнішим інструментом злагодження дій різних стейкхолдерів в умовах кризових ситуацій. Лише за грудень 2022 року відбулось щонайменше три таких навчання (національні у Франції та двічі міжнародні під егідою НАТО), а по загальноєвропейським навчанням Cyber Europe 2022 було підбито підсумки. Можна очікувати, що цей формат буде лише розширюватись, зважаючи на інтернаціоналізацію кіберзагроз, збільшення їх маштабів та географічного охоплення.

Фахівці з кібербезпеки впевнено вказують на те, що ransomware залишиться головним викликом 2023 року. Лише у грудні такі атаки вразили великих IT- та хостинг-провайдерів, державні підрозділи в різних країнах (в т.ч. у США, Новій Зеландії, Франції), ЗМІ (Великобританія). Ситуація погіршується шляхом поступового розвитку бізнес-моделі RaaS, яка охоплює все нові елементи таких видів атак. RaaS настільки спростив поріг входження в цю сферу для злочинців, що парадоксальним чином створює стратегічні виклики від низької кваліфікації злочинців (наприклад – ransomware Cryptonite). Така потужна кіберактивність змішує держави посилювати обов'язковість процесів звітування про кіберінциденти – таким шляхом пішла Великобританія та Швейцарія. Одночасно з цим все більше уваги приділяється і малому та середньому бізнесу. Франція та Австралія публікують окремі настанови для цього сегмента користувачів, розуміючи їх обмежені ресурси на забезпечення власної кібербезпеки.

Критична інфраструктура – все ще найбільш бажана ціль для зловмисників. Кількість атак проти освітніх установ, лікарень, індустріальних гігантів, державних установ лише зростає. Управління безпеки на транспорті США планує розширити використання сторонніх органів сертифікації для регулювання питання кібербезпеки найважливіших операторів трубопроводів і залізниць. Одночасно з цим знову зростає активність кібершпигунських угруповань (переважно іранських та китайських), які спрямовують свою діяльність на широке коло суб'єктів.

Україна продовжує залишатись у фокусі уваги російських хакерів. За попередніми даними вірус DolphinCape уразив низку державних установ та елементів транспортної інфраструктури в Україні. Також продовжуються спроби атак на систему військового зв'язку «Дельта». Компанія Mandiant оприлюднила інформацію про спробу поширити піратську версію Windows із вбудованим вірусом-трояном в надії, що він потрапить до державних установ. Водночас російські хакери продовжують поширювати свої кібердії за межі території України, постійно атакуючи країни чи організації, які підтримують українську державу. У грудні були атаковані інформаційні ресурси Ватикану. Також є вірогідність компрометації інформаційних систем організацій в США та Великобританії та спроби атаки проти нафтопереробного заводу країни НАТО. Як Microsoft, так і NSA очікують інтенсифікації російських кібератак протягом найближчих кількох місяців за межами України. Вірогідною мішенню може стати глобальна енергетична інфраструктура.

Поступово формується коаліція країн, що підтримують підходи до розвитку технологій, базовані на повазі до прав людини, що відрізнятиме її від авторитарних країн, таких як Китай та рф. Її ядром може стати Рада з торгівлі та технологій між ЄС та США, третя зустріч якої відбулася у грудні 2022. Наслідком цього може стати роз'єднання у сфері технологій та геополітичне роз'єднання загалом, що є відходом від бачення світу, як взаємопов'язаної екосистеми.

Поглиблюється розрив між США та Китаєм у галузі передових технологій. США спрямовує зусилля на те, щоб позбавити Китай можливості використовувати технологічні досягнення США для розвитку своїх озброєнь. Не всі країни ЄС поділяють настороженість США щодо Китаю, особливо це стосується Голландії та Німеччини. Також, традиційним партнером Китаю у сфері технологій є Японія. Разом з тим, події цього місяця вказують на те, що Нідерланди та Японія, швидше за все, погодяться з обмеженнями на експорт обладнання для виробництва високотехнологічних чіпів до Китаю. Така активна політика США у цій сфері, поєднана зі збільшенням інвестицій та релокацією виробництва сучасних чіпів до західних країн, становить значний виклик для Китаю.

Попри заяви компанії TikTok, що вона не працює у Китаї та не ділиться персональними даними американців з китайським урядом, в США розгортається кампанія із заборони використання застосунку TikTok на урядових пристроях, якими користуються держслужбовці. Таку заборону запровадили вже п'ять американських штатів, а також декілька федеральних установ. Законопроєкт, який зробить таку заборону обов'язковою для всього федерального сектору, пройшов перший етап розгляду в Сенаті США.

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

CISA ТА FBI ПРОДОВЖУЮТЬ ЗАХОДИ ІЗ ВИРОБЛЕННЯ СПІЛЬНОГО ПІДХОДУ ДО ПРОТИДІЇ RANSOMWARE

14 грудня за результатами другого засідання спільної робочої групи двох відомств було напрацьовано спільні підходи щодо чотирьох напрямків:

- підтримка потерпілих – стандартизація та синхронізація федеральної взаємодії з жертвами ransomware для надання послуг;
- вимірювання – збір даних і показників для ліпшої протидії;
- залучення партнерів – розширення оперативної співпраці та обміну розвідувальними даними з партнерами;
- постійне вдосконалення – більше аналітичного опрацювання отриманих даних для покращення готовності, інтеграція розвідувальних даних та координація кампаній відомств спрямованих на знищення учасників організаторів ransomware кампаній.

CISA ПРИСТУПИЛА ДО РОЗГОРТАННЯ ДРУГОЇ ФАЗИ ПРОГРАМИ ЩОДО ПОЛІПШЕННЯ NS/EP

9 грудня CISA повідомила, що розпочала роботу над другою фазою реалізації проєкту пов'язаного з розробкою, тестуванням, впровадженням і підтримкою зв'язку національної безпеки та готовності до надзвичайних ситуацій (NS/EP). Відповідне завдання було визначено Указом Президента США (виконавчий наказ 13618). Мета програми – забезпечити ефективне надання мережевих послуг наступного покоління (NGN PS), щоб усі користувачі NS/EP могли спілкуватися з будь-ким і будь-коли.

ANSSI СПІЛЬНО З ПАРТНЕРАМИ З ПРИВАТНОГО СЕКТОРУ ПРОВЕЛИ МАСШТАБНІ КІБЕРНАВЧАННЯ REMPAR22

8 грудня ANSSI спільно з Cyber Campus та Business Continuity Club (CCA) провели спільні кібернавчання. У заході взяли участь понад 100 організацій-учасників. Розроблений для навчань кризовий сценарій мав допомогти учасникам підвищити обізнаність про проблеми безперервності бізнесу та протестувати систему управління кризовими ситуаціями. Крім того, учасники відпрацювали координацію акторів між собою та в межах одного сектору, підготувались до кризового спілкування всередині та ззовні організацій, а також поліпшили інформаційний обмін.

ФРАНЦІЯ АНОНСУЄ СИСТЕМУ ПІДТРИМКИ ДЛЯ СТАРТАПІВ, А ТАКОЖ МАЛОГО І СЕРЕДНЬОГО БІЗНЕСУ В ПИТАННЯХ ДОТРИМАННЯ СЕРТИФІКАЦІЇ БЕЗПЕКИ ХМАРНИХ ПОСЛУГ

22 грудня французький уряд оголосив про створення програми підтримки для МСБ та стартапів, що хочуть пройти сертифікацію SecNumCloud Security Visa. Цей фреймворк був розроблений ANSSI для ідентифікації «довірених» пропозицій хмарних послуг. Оператори критичної інфраструктури можуть використовувати лише послуги тих хмарних операторів, що мають підтверджену відповідність щодо SecNumCloud Security Visa.

Розуміючи високу вартість проведення сертифікації за цими вимогами для МСБ та стартапів, Франція створює систему підтримки для таких організацій з бюджетом 3,5 мільйона євро. Підтримка охопить заходи, які містять в собі початковий аудит для визначення рівня зрілості компанії-кандидата, консультаційні послуги (план розвитку процесу кваліфікації та план підготовки до кваліфікації) і саму фінансову допомогу для кваліфікації.

ENISA ТА EEAS ПУБЛІКУЮТЬ СПІЛЬНИЙ ЗВІТ ПРО ЗВ'ЯЗОК ІНОЗЕМНОГО ВТРУЧЕННЯ ТА ПРОБЛЕМ КІБЕРБЕЗПЕКИ

8 грудня ENISA та EEAS (Європейська служба зовнішніх справ) оприлюднили спільний звіт про зв'язок між кіберзагрозами та іноземним втручанням (Foreign Information Manipulation and Interference, FIMI). У звіті аналізуються численні взаємозв'язки двох сфер і вказується на необхідність нарощування спільних дій у таких сферах:

- посилення кіберспроможностей у встановленні джерел операцій FIMI/дезінформації;
- обміну інформацією між спільнотами кібербезпеки та FIMI/дезінформації;
- важливість обміну передовим досвідом між двома спільнотами;
- підвищення обізнаності та підтримка розвитку потенціалу держав-членів та міжнародних партнерів.

МІНІСТЕРСТВО ОБОРОНИ США ПІДПИСАЛО КОНТРАКТ З PALO ALTO NETWORKS ДЛЯ МАСШТАБНОГО ВИКОРИСТАННЯ РІШЕННЯ ДЛЯ КЕРУВАННЯ ПОВЕРХНЕЮ АТАК CORTEX XPANSE

23 грудня компанія Palo Alto Networks повідомила, що підписала довгострокову угоду з Міністерством оборони США на використання платформи Cortex Xpanse для захисту критично важливих цифрових мереж та активів Міністерства оборони. Платформа надає можливість виявляти, вивчати та усувати ризики та передумови для реалізації атак. Xpanse працює, постійно виявляючи та оцінюючи ризики кібератак (cyber attack surface risks) на активи, які підключені до мережі Інтернет.

CISA ТА FBI ВИПУСТИЛИ СПІЛЬНЕ ПОПЕРЕДЖЕННЯ ПРО ДІЯЛЬНІСТЬ ГРУПИ CUBA RANSOMWARE

5 грудня CISA та FBI випустили спеціальне попередження щодо діяльності групи Cuba Ransomware, яка вже атакувала понад 100 організацій по всьому світу та отримала понад 60 мільйонів доларів у вигляді викупу. Їх атаки спрямовані на критичну інфраструктуру, фінансові послуги, охорону здоров'я, інформаційні технології та державні установи. Група бере участь у подвійних атаках з вимаганням не тільки за розшифрування даних, але й погрожуючи оприлюднити дані, викрадені у жертви, якщо викуп, який вимагають у біткойнах, не буде сплачено.

СИНГАПУР ПОСИЛЮЄ УВАГУ ДО КІБЕРБЕЗПЕКИ ОТ

13 грудня видання ZDnet у своїй редакційній статті описує еволюцію підходу Сінгапуру до пріоритетів кібербезпеки в країні. Зокрема вказується на те, що влада суттєво корегує свою Стратегію кібербезпеки на користь більшої уваги до OKI. А саме рішень, що включають промислове управління, управління будівлями та системи керування світлофорами, які контролюють або змінюють фізичний стан системи, наприклад залізничних. Ці системи все частіше стають жертвами атак ransomware, а також тих зловмисників, які здійснюють свою діяльність в інтересах урядів.

Ще один важливий елемент безпеки OKI – захист ланцюгів постачання. Для цього CSA програму CII Supply Chain, яка окреслює п'ять основоположних ініціатив, щоб допомогти цим секторам розв'язувати проблеми ланцюжка кіберпостачання на різних рівнях, включаючи організаційний, галузевий, національний і міжнародний.

АВСТРАЛІЙСЬКИЙ ЦЕНТР КІБЕРБЕЗПЕКИ ОПРИЛЮДНИВ ПОСІБНИКИ ДЛЯ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ ЩОДО ЗАХИСТУ ЇХ ХМАРНОЇ ІНФРАСТРУКТУРИ

16 грудня Австралійський центр кібербезпеки (ACSC) заявив, що розробив Посібники з хмарної безпеки для малого бізнесу. Це стало визнанням того, що малий і середній бізнес може не мати ресурсів, щоб ефективно захистити себе від нових загроз. Посібники мають допомогти підприємствам зрозуміти можливі ризики, як працювати з постачальниками послуг, щоб забезпечити надійну кібергігієну. Посібники містять технічні приклади багатофакторної автентифікації, керування виправленнями (patch) та керування програмами.

ВПЕРШЕ КОМАНДУВАННЯ США ЗАСТОСУЄ КІБЕРКОМПОНЕНТ ПІД ЧАС НАВЧАНЬ У АФРИЦІ

21 грудня Командування США оголосило, що вони планують додати кіберкомпонент під час навчань Justified Accord 23, які відбудуться спільно між американським та африканськими військовим (серед учасників Кенія та Уганда). Це стало наслідком зростання кількості кібератак як на американські цифрові ресурси, так і зростання кіберактивності в Африці.

ФРАНЦУЗЬКИЙ УРЯД ОГОЛОСИВ ПРО ВЕЛИКУ НАВЧАЛЬНУ ПРОГРАМУ З КІБЕРБЕЗПЕКИ ДЛЯ ПЕРСОНАЛУ ЛІКАРЕНЬ

21 грудня міністри внутрішніх справ, охорони здоров'я та цифрових послуг Франції оголосили про запуск навчальної програми для французьких лікарень. «Мета полягає в тому, щоб 100 відсотків найважливіших закладів охорони здоров'я пройшли ці навчання до травня 2023 року», – сказано у спільній заяві.

Ця програма запроваджена як відповідь на хвилю кібератак проти французьких лікарень під час яких кіберзлочинці блокували критично важливі IT-мережі та дані закладу, перш ніж вимагати викуп за їх звільнення. Державні лікарні не можуть платити викуп згідно із чинним законодавством.

УРЯД ШВЕЙЦАРІЇ ПЛАНУЄ ВВЕСТИ ПРАКТИКУ ОБОВ'ЯЗКОВОГО ЗВІТУВАННЯ ПРО КІБЕРАТАКИ НА КРИТИЧНУ ІНФРАСТРУКТУРУ

2 грудня стало відомо, що уряд Швейцарії планує ухвалити законодавство, яке встановлює обов'язковість звітування про кібератаки, які впливають на критичну інфраструктуру країни. Оновлене законодавство також чіткіше визначить роль Національного центру кібербезпеки (NCSC) як центрального органу у відстежуванні кібератак.

ЄС СТВОРИВ САЙТ ДЛЯ ВІДСЛІДКОВУВАННЯ РОЗГОРТАННЯ КЛЮЧОВИХ СТАНДАРТІВ ІНТЕРНЕТУ

Інформаційні панелі візуалізують індикатори розгортання 18 ключових стандартів Інтернету, які допомагають захистити Інтернет і підтримують його постійний технологічний розвиток. Вони згруповані в п'ять категорій відповідно до їх функції:

- перегляд – стандарти веб-зв'язку
- маршрутизація – взаємоузгоджені норми безпеки маршрутизації (MANRS)
- надсилання електронною поштою – стандарти безпеки електронної пошти
- найменування – розширення безпеки системи доменних імен (DNSSEC)
- адресація – Інтернет-протокол версії 6 (IPv6)

ВЕЛИКОБРИТАНІЯ ЗАПРОВАДЖУЄ ОБОВ'ЯЗКОВЕ ЗВІТУВАННЯ ПРО КІБЕРІНЦИДЕНТИ ДЛЯ ПОСТАЧАЛЬНИКІВ КЕРОВАНИХ ПОСЛУГ

Британський уряд запроваджує нову обов'язкову вимогу щодо звітності провайдерів керованих послуг (MSP) щодо розкриття кіберінцидентів, а також мінімальні вимоги безпеки, за невиконання яких MSP можуть бути оштрафовані на суму до 17 мільйонів фунтів стерлінгів (20 мільйонів доларів США).

Нові вимоги будуть запроваджені через оновлення Регламенту мережевих та інформаційних систем (NIS). Також будуть оновлені чинні вимоги до звітності. Їхня ефективність була піддана критиці після того, як з'ясувалося, що попри численні порушення безпеки, які впливають як на енергетичний, так і на транспортний сектори, жоден інцидент не сягнув фактичного порогу, після якого необхідно було проінформувати уряд.

Про це урядовці заявили паралельно з публікацією 30 листопада відповіді уряду на заклик подати пропозиції щодо покращення кіберстійкості Великобританії. Вони також повідомили, що реакція представників індустрій була переважно позитивною.

ПРЕЗИДЕНТ БАЙДЕН СХВАЛИВ ФІНАНСУВАННЯ НА ЗБІЛЬШЕНІ ПОВНОВАЖЕННЯ ТА ЗОБОВ'ЯЗАННЯ КІБЕРКОМАНДУВАННЯ США

23 грудня президент Джо Байден підписав Закон про оборонну політику, який виділяє 858 мільярдів доларів на цілі оборони, а також надає більше повноважень і зобов'язань Кіберкомандуванню США.

Законом було виділено додаткові 44 мільйони доларів на «попереджувальне полювання (hunt forward)», яке проводить Кіберкомандування США. В рамках таких операцій представники США допомагають іншим країнам у протистоянні кіберзагрозам.

У законі також йдеться, що якщо президент визначить наявність «активної, системної та триваючої кампанії атак у кіберпросторі з боку іноземної держави» проти уряду США або критичної інфраструктури країни, CYBERCOM може проводити наступальні операції у відповідь зі схвалення президента.

Закон також зобов'язує міністра оборони щорічно інформувати законодавців Конгресу про відносини між CYBERCOM та Агентством національної безпеки, подавати кожні два роки відкритий звіт протягом виборчого циклу 2032 року про зусилля командування щодо безпеки виборів.

Підтриманий обома партіями закон створює посаду помічника міністра з питань кіберполітики в Пентагоні, а також врегульовує діяльність нового бюро кібербезпеки Державного департаменту, яке очолює перший кіберпосол Натаніель Фік.

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

НАТО ВІДСЛІДКОВУЄ «ПЕРЕТІК» РОСІЙСЬКИХ КІБЕРАТАК

За словами заступника генерального секретаря НАТО з питань розвідки та безпеки Девіда Кеттлера, НАТО спостерігає постійні та тривалі спроби зруйнувати українські урядові військові системи, а також певний процес «перетоку» такої активності, що зачіпає деякі сусідні країни. Кеттлер відмовився назвати країни, де НАТО спостерігає такі атаки.

Разом з тим, він зазначив, що Альянс працює над зміцненням кібербезпеки з чотирма державами-членами НАТО, які межують з Україною, а саме Польщею, Угорщиною, Словаччиною та Румунією. Також НАТО спостерігає збільшення кількості спроб здійснити кібератаки на власні критично важливі мережі з боку «зловмисників». Про це Кеттлер повідомив під час віртуального брифінгу.

ANSSI ТА BSI ПОГЛИБЛЮЮТЬ СПІВРОБІТНИЦТВО

У грудні 2022 року ANSSI та BSI (Bundesamt für Sicherheit in der Informationstechnik) підписали угоду про взаємне визнання сертифікатів безпеки для схем CSPN (Premier Security Certification. Level) та BSZ (Beschleunigte Sicherheitszertifizierung). Це вже п'ята спільна публікація ANSSI та BSI з 2018 року.

КИТАЙ ТА САУДІВСЬКА АРАВІЯ УКРІПЛЮЮТЬ СПІВРОБІТНИЦТВО

Серед угод, підписаних Президентом Китаю Сі Цзіньпіном і королем Саудівської Аравії Салман бін Абдель Азіз Аль Саудом під час їх зустрічі в Ер-Ріяді 8 грудня, є і Меморандум про порозуміння, що дозволить китайському технологічному гіганту Huawei надавати послуги у сфері хмарних обчислень та інші IT послуги уряду Саудівської Аравії. Домовленостей було досягнуто в той час, коли обидві країни переживають напругу у відносинах зі США. Як вважає оглядач Defense One Патрік Такер, ця домовленість ілюструє, як автократичні уряди шукають співпраці у протидії тиску з боку США у питаннях прав людини та громадянських свобод.

CCDCOE NATO ПРОВОДИТЬ 11 ЩОРІЧНІ КІБЕРНАВЧАННЯ CROSSED SWORDS

У грудні 2022 року у Таллінні розпочались 11-і навчання Crossed Swords, які об'єднують близько 120 учасників з 24 країн, як з країн-членів НАТО, так і з країн, що не входять до НАТО. Навчання проводяться в навчально-тренувальному центрі CR14. Цьогорічний сценарій зосереджений на співпраці та синхронізації зусиль в умовах ескалації конфлікту. Мета навчань – відпрацювати не лише захисні стратегії, але і наступальні операції у кіберпросторі на сучасному полі бою.

НАТО ПРОВЕЛО В ЕСТОНІЇ НАВЧАННЯ З КІБЕРБЕЗПЕКИ ЗА УЧАСТІ 26 КРАЇН

У Таллінні з 28 листопада до 2 грудня проходили навчання з кіберзахисту Cyber Coalition 22. Учасники навчалися протидіяти кібератакам на електромережі, програми та активи НАТО та членів Альянсу під час операцій. В заході взяли участь понад 1000 кіберспеціалістів із 26 країн-членів НАТО та з Фінляндії, Швеції, а також Грузії, Ірландії, Японії, Швейцарії, Європейського Союзу, та учасники з приватного сектору та наукових кіл.

Під час навчань тестувались можливості використання штучного інтелекту для протидії кіберзагрозам, стандартизації кіберповідомлень для кращого обміну інформацією та використання розвідки кіберзагроз для інформування про ситуацію в кіберпросторі.

ENISA ПІДВЕЛА ПІДСУМКИ НАВЧАНЬ CYBER EUROPE 2022

13 грудня ENISA оприлюднила фінальний звіт щодо результатів проведення кібернавчань Cyber Europe 2022 (відбулись у червні 2022 року). Основний сценарій навчань – кампанія дезінформації про підроблені лабораторні результати та кібератаку, спрямовану на мережі європейських лікарень.

В навчаннях взяли участь майже 1000 учасників. Основний висновок навчань – кібербезпека у сфері охорони здоров'я критично залежна від виділеного бюджету та забезпеченості кібербезпекових команд необхідними ресурсами. Також рекомендовано проводити регулярне тренування на місцевому рівні.

ПІДРОЗДІЛ КІБЕРОБОРОНИ ЦАХАЛ ПРОВІВ СПІЛЬНІ НАВЧАННЯ З КІБЕРКОМАНДУВАННЯМ США

Вже сьомі спільні навчання бригади кібероборони Армії оборони Ізраїлю та Кіберкомандування США відбулися протягом першого тижня грудня в кіберцентрі в штаті Джорджія. Вони включали відпрацювання «декількох реальних сценаріїв... з акцентом на Близькому Сході», повідомили в Армії оборони Ізраїлю.

США та Ізраїль стикаються з кіберзагрозами з боку Ірану, тому продовжують працювати разом, щоб протистояти їм. Ізраїль загалом дотримується політики неоднозначності (ambiguity) щодо своїх операцій проти Ірану та не розкриває своєї відповідальності за них.

ЗАСІДАННЯ РАДИ США ТА ЄС З ПИТАНЬ ТОРГІВЛІ ТА ТЕХНОЛОГІЙ

5 грудня в США відбулось третє засідання Ради США та ЄС з питань торгівлі та технологій (TTC). Цей механізм, започаткований наприкінці вересня 2021 року, слугує майданчиком для узгодження підходів у питаннях торгівлі, технологій та інновацій між США та ЄС.

Хоча засідання відбулось на тлі суперечки між США та ЄС щодо положення Закону США про скорочення інфляції («Купуй американське»), його практичним результатом стали два спільних проєкти в Африці в галузі безпечного зв'язку, які складуть конкуренцію експансії Китаю на Африканському континенті.

Також було ухвалено Спільну дорожню карту щодо гідного довіри ШІ та управління ризиками, яка допоможе створити спільний репозитарій показників для вимірювання надійності ШІ та методів управління ризиками. Потенційно дорожня карта також сприятиме обміну інформацією та просуванню спільних підходів у міжнародних органах зі стандартизації, пов'язаних з ШІ. З іншими ініціативами та напрацюваннями в рамках десяти робочих груп TTC можна ознайомитися за посиланням.

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

ХАКЕРИ ЗЛИЛИ ДАНІ, ВИКРАДЕНІ У АВСТРАЛІЙСЬКОЇ СТРАХОВОЇ КОМПАНІЇ MEDIBANK

Першого грудня австралійська компанія Medibank, що надає послуги медичного страхування, визнала, що дані, які було злито в Darknet, дійсно були викрадені у неї. Злив відбувся у відповідь на відмову компанії заплатити викуп після атаки ransomware.

Разом з тим, компанія стверджує, що оприлюднені дані не є достатніми для фінансових махінації та крадіжки особи їх клієнтів. Офіс Уповноваженого з питань інформації Австралії (OAIC) у той же день розпочав розслідування практики обробки особистої інформації компанією Medibank у зв'язку з витоком даних. 10-11 грудня Medibank відключила свої IT-системи від мережі, закрила свої філії та залучила групу реагування Microsoft, для допомоги у покращенні своєї кібербезпеки.

RACKSPACE ПОВІДОМИЛА, ЩО ЗБІЙ В РОБОТІ MICROSOFT СПРИЧИНИЛА АТАКА RANSOMWARE

Гігант хмарних обчислень Rackspace 6 грудня підтвердив, що з 2 грудня намагається виправити збій, який призвів до припинення роботи Microsoft Outlook Web App для тисяч клієнтів і спричинив інші проблеми, що випливають з цього.

Компанія надає послуги у розміщенні інфраструктури Microsoft Exchange, яка пропонує клієнтам програмне забезпечення електронної пошти, календаря та контактів Microsoft. Компанія заявила, що атака ransomware вплинула на її середовище Hosted Exchange, що є основною причиною збою в роботі сервісу.

КІЛЬКА ДЕРЖАВНИХ ОРГАНІВ У НОВІЙ ЗЕЛАНДІЇ ПОСТРАЖДАЛИ ЧЕРЕЗ АТАКУ RANSOMWARE НА IT-ПРОВАЙДЕРА

Вранці 6 грудня Уповноважений із питань конфіденційності Нової Зеландії підтвердив, що «кіберінцидент, пов'язаний з атакою ransomware», створив перешкоди для роботи сотень організацій в країні, включаючи низку державних органів. Мішенню атаки була компанія Mercury IT, яка «надає широкий спектр IT-послуг клієнтам по всій Новій Зеландії».

Серед державних органів, які оголосили, що постраждали від кібератаки, були Міністерство юстиції та Міністерство охорони здоров'я. Обидва міністерства повідомили, що відчувають складнощі з доступом до певних даних, але запевнили, що продовжують працювати, і що поки що немає підстав думати, що дані було викрадено. Дослідження масштабу інциденту триває.

LOCKBIT ПОГРОЖУЄ ОПРИЛЮДНИТИ 76 ГБ ВИКРАДЕНОЇ ІНФОРМАЦІЇ ДЕПАРТАМЕНТУ ФІНАНСІВ КАЛІФОРНІЇ

13 грудня влада Каліфорнії підтвердила, що група, яка стоїть за ransomware LockBit, вимагає викуп за неоприлюднення 76 Гб викраденої у Міністерства фінансів Каліфорнії інформації, яка за словами зловмисників включає «бази даних, конфіденційні дані, фінансові документи, сертифікати, судові та сексуальні провадження в суді, IT-документи тощо». Хакери вже опублікували кілька скріншотів, які демонструють фінансову інформацію, структуру каталогу, контракти та інші документи, щоб підтвердити свої претензії. Влада впевнена, що жодні державні дані не були скомпрометовані.

THE GUARDIAN БУЛО АТАКОВАНО RANSOMWARE

21 грудня The Guardian оголосила, що атака ransomware спричинила перебої в роботі окремих служб видання. Онлайн-видання продовжило свою роботу без змін, але відбувся збій у деяких внутрішніх системах, що вплинуло на вихід друкованої версії.

КИТАЙСЬКІ КІБЕРШПИГУНИ АКТИВІЗУВАЛИСЬ ПЕРЕД ВИБОРАМИ У ЯПОНІЇ – ESET

15 грудня компанія ESET повідомила, що виявила спрямовану активність китайської хакерської групи MirrorFace, яка розгортає власну шкідливу програму LodeInfo виключно проти японських організацій. LodeInfo — це бекдор, який підтримує захоплення скриншотів і натискань клавіш, а також завершення процесу, викрадення файлів, виконання файлів і команд і шифрування файлів.

Для доставлення зловмисного програмного забезпечення LodeInfo використовувалися приватні електронні листи. Операція (компанія ESET назвала її LiberalFace) почалася 29 червня з розсилки електронної пошти з інструкціями поширювати вкладені відео в профілях соціальних мереж.

ХАКЕР ЗАЯВИВ ПРО ТЕ, ЩО ЗМІГ ОТРИМАТИ ДОСТУП ДО ДАНИХ КОРИСТУВАЧІВ ПОРТАЛУ INFRAGARD

15 грудня з'явилось повідомлення, що хакер USDoD зміг отримати доступ до бази користувачів (близько 80 тисяч записів) порталу InfraGard. InfraGard – започатковане у 1996 році ФБР державно-приватне партнерство, учасниками якого є фахівці з кібербезпеки з усіх секторів, включно зі сферою національної безпеки та критичної інфраструктури. Хакер попередив потенційних покупців бази, що вона не містить номерів соціального страхування чи дат народження.

Хакер начебто отримав доступ до онлайн-порталу InfraGard, видаючи себе за генерального директора фінансової установи. Членство в спільності схвалюється ФБР після перевірки. Поки невідомо, як саме хакер зміг її пройти.

ВІРУС-ШИФРУВАЛЬНИК CRYPTONITE НЕ МОЖЕ РОЗШИФРУВАТИ ЗАШИФРОВАНІ НИМ ДАНІ – ВИПЛАТА ВИКУПУ НЕМАЄ СЕНСУ

6 грудня дослідники з Fortinet оприлюднили результати дослідження ransomware Cryptonite. Вони виявили, що ransomware має лише спроможність шифрування файлів і взагалі не пропонує засобів розшифровки, навіть якщо сплачено викуп. Наразі точно не відомо чи саме це було вихідною метою вірусу чи це проблема того, що поширювачі погано його зібрали (дослідники схильні до другої версії). Цей випадок також нагадує про те, що сплата викупу ніколи не є гарантією отримання ключа розшифровки або що він працюватиме належним чином.

КРИПТОБІРЖА BINANCE ЗАМОРОЗИЛА КРИПТОВАЛЮТУ ВАРТІСТЮ 3 МІЛЬЙОНИ ДОЛАРІВ, ВИКРАДЕНУ ПІД ЧАС ЗЛОМУ ANKR

Після зламу провайдера інфраструктури Web3 Ankr, Binance став одним з останніх криптогігантів, що заморозив криптовалюту на суму близько 3 мільйонів доларів 2 грудня. Компанія Ankr заявила, що з платформи було вкрадено валюти Binance на 5 мільйонів доларів і що вона планує покрити всі збитки, понесені її користувачами.

Інша платформа, Helio, підтвердила, що вона також зазнала атаки, але не розкрила інформацію щодо втраченої суми. Ankr є оператором розподіленого вузла для мереж із підтвердженням частки, що дозволяє користувачам легко підтвердити свої токени без купівлі необхідного обладнання.

ХАКЕРИ, ПОВ'ЯЗАНІ З КИТАЙСЬКИМ УРЯДОМ, ВКРАЛИ МІЛЬЙОНИ COVIDНИХ ГРОШЕЙ

5 грудня NBC повідомила, що за даними американських спецслужб, хакери, пов'язані з китайським урядом, викрали щонайменше 20 мільйонів доларів США, призначених на соціальні виплати в зв'язку з епідемією COVID, включаючи гроші на позики від Адміністрації малого бізнесу та страхові виплати через безробіття у більш ніж десяти штатах.

Крадіжка грошей китайською хакерською групою APT41, що базується в китайському місті Ченду, «є першим випадком пов'язаного з пандемією шахрайства, вчиненого іноземними, спонсорованими державою кіберзлочинцями, який уряд США визнав публічно», – зазначає NBC News.

Зараз незрозуміло чи китайський уряд прямо стояв за крадіжкою коштів чи просто вирішив не зупиняти такі дії. Однак дії APT41 вказують, що настала нова ера в кібербезпеці, за якої навіть федеральні грошові кошти не знаходяться у безпеці, коментують журналісти NBC.

ДОСЛІДНИКИ ОПИСАЛИ НОВИЙ МЕТОД АТАКИ, ЩО ДОЗВОЛЯЄ ОБХОДИТИ ПОПУЛЯРНІ БРАНДМАУЕРИ ВЕБЗАСТОСУНКІВ

Новий метод кібератаки може бути використаний для обходу брандмауерів різних вебзастосунків (WAF) для проникнення в системи, що може дозволити зловмисникам отримати доступ до конфіденційної інформації про бізнес і клієнтів.

МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я США ПОПЕРЕДЖАЄ ПРО ЗБІЛЬШЕННЯ КІЛЬКОСТІ АТАК НА ЛІКАРНІ З БОКУ RANSOMWARE ROYAL

Як зазначає Міністерство охорони здоров'я США у попередженні від 7 грудня, кількість атак ransomware під разовою Royal збільшуються. Воно є відносно новим угрупованням, адже вперше його було помічено у вересні цього року. Група використовує класичну схему, погрожуючи оприлюднити чутливі дані, отримані з комп'ютера жертви, у разі відмови сплатити викуп. Угрупування вимагало викупи розміром до мільйона доларів. З огляду на інтерес операторів ransomware до медичної сфери, Міністерство вважає його загрозою.

СИНДИКАТ КІБЕРЗЛОЧИНЦІВ FIN7 СТАЄ ГОЛОВНИМ ГРАВЦЕМ У СФЕРІ ПРОГРАМ-ВИМАГАЧІВ

Аналіз угрупування FIN7, опублікований компанією Profdat 22 грудня, розкрив організаційну ієрархію синдикату кіберзлочинців, а також розкрив його роль як учасника зростаючої кількості атак програм-вимагачів. Він також виявив глибші зв'язки між FIN7 та більш масштабною екосистемою загроз, що містить в собі вже неіснуючі сімейства програм-вимагачів, такі як DarkSide, REvil і LockBit.

Ця дуже активна група загроз, також відома як Carbanak, славиться тим, що використовує великий арсенал інструментів і тактик для розширення своїх «горизонтів кіберзлочинності», включаючи додавання програм-вимагачів до ігор і створення фальшивих компаній безпеки, щоб спонукати дослідників до проведення атак програм-вимагачів під виглядом тестування на проникнення.

Методи вторгнення FIN7 протягом багатьох років вийшли за межі традиційної соціальної інженерії, включивши заражені USB-накопичувачі, компрометацію ланцюжка постачання програмного забезпечення та використання викрадених облікових даних, придбаних на підпільних ринках.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

NSA ПОСИЛЮЄ УВАГУ ДО ПИТАНЬ ЗАХИСТ МІКРОЕЛЕКТРОНІКИ МІНІСТЕРСТВА ОБОРОНИ ВІД ЗЛОВМИСНИКІВ

8 грудня NSA оприлюднило чотири технічні звіти (рекомендації) для Міністерства оборони США. Вони мають допомогти Міністерству оборони захистити свої системи, які використовують програмовані мікроелектронні компоненти (FPGA) від зловмисного впливу. Звіти охоплюють чотири етапи потенційного впливу: виробництво, придбання, програмування та перше підключення пристроїв.

NIST ГОТУЄ НОВУ ВЕРСІЮ РЕКОМЕНДАЦІЙ ЩОДО ЦИФРОВОЇ ІДЕНТИФІКАЦІЇ У ФЕДЕРАЛЬНИХ СИСТЕМАХ

16 грудня NIST опублікував для обговорення оновлену версію Digital Identity Guidelines (NIST Special Publication 800-63). Документ має допомогти федеральним установам краще протидіяти злочинності в Інтернеті, зберігати конфіденційність та сприяти зручності використання. «Перевірка особи – це вхідні двері до федеральних послуг і пільг, і вона має забезпечувати безпеку, водночас забезпечуючи доступ для потенційних бенефіціарів», – сказав Джейсон Міллер, заступник директора з департаменту Управління та бюджету NIST.

Проєкт документа спрямований на те, щоб допомогти організаціям управляти ризиками пов'язаними з цифровими взаємодіями, однак при цьому і полегшуючи людям успішне використання цифрових даних, зокрема під час звернення за державними послугами.

КОМПАНІЯ TREND MICRO ОПРИЛЮДНИЛА ПРОГНОЗИ БЕЗПЕКИ НА 2023 РІК

13 грудня кібербезпекова компанія Trend Micro оприлюднила власне бачення основних загроз кібербезпеці, з якими можуть стикнутися компанії у 2023 році. До них відносяться:

- більша увага кіберзлочинців до помилок користувачів хмарних технологій;
- більше загроз для промислового Інтернету речей (IIoT);
- ще більше зусиль злочинців до використання соціальної інженерії;
- посилення уваги кіберзлочинців не так до отримання викупу за шифрування інформації, скільки за її нерозповсюдження.

СІМ ТЕНДЕНЦІЙ КІБЕРБЕЗПЕКИ НА 2023 РІК, НА ЯКІ ВАРТО ЗВЕРНУТИ УВАГУ

Попри те, що ситуація у світовій економіці змушує технологічні компанії зменшувати активність, станом на кінець 2022 року кібербезпека залишається пріоритетом, який не втрачає ваги, пише видання Dice.

Разом з тим, наступного року варто звернути увагу на такі тенденції:

1. Економічна невизначеність збільшить безпекові ризики. Переважна більшість економістів передбачають рецесію у 2023 році. Зважаючи на те, що вже зараз компаніям важко знаходити оптимальні варіанти інвестицій у кібербезпеку, економічна невизначеність може ускладнити ситуацію.
2. Шахрайство з криптовалютою зростає. Особливо вразливими до нього будуть люди похилого віку, та люди, які, перебуваючи у стані фінансової скрути, будуть шукати швидкого збагачення.
3. Застосування «нульової довіри» продовжуватиме поширюватися. Дослідники фірми Gartner вважають, що у 2023 році охоплення цією політикою безпеки становитиме 31%.
4. Слідкуйте за квантовими обчисленнями. Хоча експерти говорять, що до появи квантового комп'ютера ще далеко, технологія розвивається, і квантові обчислення стануть реальністю. Тому спеціалістам з кібербезпеки варто слідкувати за прогресом у цій сфері.
5. Поширення багатофакторної автентифікації.
6. Покращується якість діпфейків. Їх стає набагато складніше розпізнати без технології аналізу вихідних даних.
7. Зростуть кіберзагрози для малого бізнесу, але разом з тим, кібербезпекові компанії пропонуватимуть більш економічно ефективні рішення.

У 2023 РОЦІ ПОСИЛИТЬСЯ ДІЯЛЬНІСТЬ ХАКТИВІСТІВ ТА ГЕОПОЛІТИЧНО ОБУМОВЛЕНИХ КІБЕРАТАК – TRELLIX

7 грудня компанія Trellix оприлюднила свої прогнози щодо ключових трендів кібербезпеки у 2023 році. Ключові з них – посилення ваги геополітичних чинників для кампаній з дезінформації та кібератак, присвячених до кінетичної військової активності, а також зростання ролі хактивізму.

Одночасно з цим буде підсилюватись активність підлітків-кіберзлочинців, ускладнення атрибуції кібератак через все більшу кількість аутсорсингових злочинних угрупувань, які втягнуті в кожну кібератаку. Також акцентовано на:

- зростанні загроз критичній інфраструктурі в умовах триваючої кібервійни;
- більша увага з боку хакерів до корпоративних пристроїв IoT задля майнінгу криптовалют;
- спроби компрометації космічних супутників;
- більше кібератак на Microsoft Windows з метою повного захоплення мережі.

У DARK WEB АКТИВНО РОЗВИВАЮТЬСЯ ПОСЛУГИ RECONNAISSANCE-AS-A-SERVICE – ACCENTURE

6 грудня спеціалісти кібербезпекової компанії Accenture опублікували матеріал, що описує ринок Reconnaissance-as-a-Service, яким активно користуються зловмисники, що спеціалізуються на ransomware. Вказується, що цей ринок постійно розвивається. Якщо раніше основна аутсорсингова послуга була пов'язана із наданням розвідувальної інформації злочинцям про те, як проникнути в мережу, то тепер до неї додалась нова – якісна оцінка отриманої зловмисниками інформації та визначення на цій основі суми викупу.

БІЗНЕС-МОДЕЛІ RANSOMWARE: МАЙБУТНІ НАПРЯМКИ ТА ТЕНДЕНЦІЇ – ЗВІТ TREND MICRO

15 грудня фахівці Trend Micro оприлюднили дослідження щодо очікуваних змін у бізнес-моделі ransomware. Компанія звертає увагу на декілька ключових тригерів, які змушують зловмисників модернізувати свою діяльність: запровадження урядами нормативні документи щодо статусу криптовалют та процесів їх функціонування, а також зміни в ландшафті IT-безпеки та перехід до хмарних сервісів.

На думку дослідників це призведе до зміни цільових кінцевих точок – передусім збільшиться увага до Інтернету речей (IoT) на Linux. А також групи RaaS або підвищуватимуть свій професіоналізм та автоматизацію процесів, або будуть швидко знайдені правоохоронними органами.

OPENAI'S CHATGPT ТА ЙОГО СУСПІЛЬНІ НАСЛІДКИ

Поява OpenAI's ChatGPT – моделі генеративного ШІ, який компанія випустила в останній день листопада, матиме непередбачувані суспільні наслідки. Серед них – наслідки для шкільної та університетської освіти, адже учні та студенти доволі швидко зрозуміють, що чатбот може писати твори, які учням та студентам задають додому. Така модель здатна вчитися у процесі виконання завдань, і, швидше за все, буде неможливо відрізнити згенерований текст від написаного людиною.

СТАН ШІ У 2022 РОЦІ ТА ОГЛЯД ЗА ОСТАННІХ 5 РОКІВ

У порівнянні з 2017 роком, коли компанія McKinsey вперше провела таке дослідження, кількість бізнесів, що використовують ШІ, збільшилася більш ніж вдвічі з 20 до 50%. Подвоїлась також і середня кількість засобів ШІ, які використовують компанії, і зараз складає 3,6.

Збільшується й розрив між тими лідерами на ринку, що інвестують у технології ШІ та іншими. Ті, хто інвестував у нього, отримують більші надходження від інвестицій, швидше розвиваються та масштабуються, і інвестують й надалі, в тому числі й у відповідних фахівців. Компаніям протягом останнього року було складно знаходити фахівців у сфері ШІ.

СУПУТНИКИ МОЖУТЬ СТАТИ НАСТУПНОЮ ЦІЛЛЮ КІБЕРЗЛОЧИНЦІВ – ZDNET

Оглядач ZDnet Денні Палмер у статті від 7 грудня досліджує проблему потенційних кібератак на супутники та можливий вплив цих заходів на кібербезпеку загалом. Акцентовано на тому, що вже запущені супутники часто мають застарілі та вразливі IT компоненти, які неможливо оновити без фізичного доступу до них.

Між тим злам супутникових систем може дозволити порушити їх основні функції, змістити їх з орбіти чи пошкодити їх іншим шляхом. Крім того, у статті звертається увага на те, що не виключеними є спроби виведення на орбіту IT-обладнання злочинців, якщо вони будуть розуміти як завдяки цьому збільшити можливості проведення атак.

5. КРИТИЧНА ІНФРАСТРУКТУРА

УПРАВЛІННЯ БЕЗПЕКИ НА ТРАНСПОРТІ США ПЛАНУЄ ЗАПРОВАДИТИ РЕГУЛЮВАННЯ ТРУБОПРОВОДІВ ТА ЗАЛІЗНИЦЬ

Управління безпеки на транспорті США планує розширити використання сторонніх органів сертифікації для регулювання питання кібербезпеки найважливіших операторів трубопроводів і залізниць.

З цією метою Управління видало Попереднє повідомлення про запропоноване нормотворення, а якому йдеться про те, що «Управління транспортної безпеки (TSA) просить надати інформацію щодо шляхів посилення кібербезпеки та стійкості в трубопровідному та залізничному (включаючи вантажні, пасажирські та транзитні) секторах. Це попереднє повідомлення про запропоновану нормотворчість (ANPRM) запрошує зацікавлених осіб та організації, зокрема власників/операторів трубопровідних і залізничних компаній із підвищеним ризиком, допомогти TSA розробити комплексний і перспективний підхід до вимог кібербезпеки».

Охочі мають 45 днів з моменту публікації документа, щоб надати власні пропозиції.

GAO: ДЛЯ КРАЩОГО ЗАХИСТУ ПРИСТРОЇВ, ПІДКЛЮЧЕНИХ ДО ІНТЕРНЕТУ НЕОБХІДНІ ДІЇ

У новому звіті, опублікованому 1 грудня, Управління підзвітності уряду (GAO) США закликає федеральні агентства краще захищати сектори критичної інфраструктури шляхом проведення оцінки ризиків Інтернету речей (IoT) і операційних технологій (OT), а також розробки кращих показників для оцінки вже наявних заходів захисту IoT та OT. Аналіз GAO стосувався таких секторів, як енергетика, охорона здоров'я та громадське здоров'я, а також транспортні системи.

ЗВІТ SANS: СТАН КІБЕРБЕЗПЕКИ ICS/OT В 2022 РОЦІ І НАДАЛІ

Опубліковано звіт компанії SANS щодо безпеки промислових систем управління (ICS)/ операційних технологій (OT). Три основних рекомендації:

1. Більший контроль над активами. Ефективне управління активами все ще залишається ключовим завданням на шляху протидії кібератакам. Чітке уявлення оператора про мережі організації, наявність інформації про активи (в т.ч. країна походження, мікропрограмне забезпечення, марка та модель тощо) – все це один з основних елементів пом'якшення ризиків вторгнення.
2. Більше контролю за тимчасовими активами/носіями. Саме такі активи несуть значний ризик для систем, особливо для тих галузей, які потребують фізичного розділення мереж. Впровадження рішень, які сканують тимчасові активи та знімні носії до того, як вони отримають можливість зв'язатися з мережею вашої компанії, має важливе значення для забезпечення безпеки об'єктів, співробітників і клієнтів.
3. Проактивний підхід. Наявність чіткої проактивної стратегії уникнення вторгнень через усі ключові вектори загроз є важливим елементом, який дозволить істотно зменшити ризики для ICS/OT.

НІМЕЦЬКИЙ ГІГАНТ ПРОМИСЛОВОГО МАШИНОБУДУВАННЯ ТА ВИРОБНИЦТВА СТАЛІ THYSSENKRUPP СТАВ МІШЕННЮ ДЛЯ КІБЕРЗЛОЧИНЦІВ

21 грудня стало відомо, що частина IT-систем Thyssenkrupp постраждала від атаки кіберзловмисників (тип атаки не повідомляється). Зокрема, було уражено частину відділу матеріальних послуг і корпоративного сегмента Thyssenkrupp. Команда IT-безпеки компанії виявила інцидент на ранній стадії, і зловмисники не встигли завдати суттєвої шкоди. Крім того, немає доказів того, що дані були викрадені або змінені.

ЗЛОВМИСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ RASPBERRY ROBIN НАЦІЛЕНО НА СЕКТОР ТЕЛЕКОМУНІКАЦІЙ ТА УРЯДОВІ УСТАНОВИ – TREND MICRO

20 грудня компанія Trend Micro оприлюднила свій аналіз зловмисного програмного забезпечення Raspberry Robin. Більшість жертв групи, яка поширює це ПЗ, – державні установи або телекомунікаційні організації з Латинської Америки, Океанії (Австралія) та Європи. Дослідники поки не можуть визначити мотиви угрупування – чи є вони виключно фінансові, чи злочинці можуть переслідувати цілі кібершпигунства.

СІМЕЙСТВО RANSOMWARE AGENDA НАЦІЛИЛОСЬ НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТУРКТУРИ – ЗВІТ TREND MICRO

16 грудня Trend Micro оприлюднило своє дослідження сімейства ransomware Agenda. Наразі суб'єкти загрози, схоже, переносять свій код ransomware на Rust – кроссплатформену мову, яка полегшує адаптацію шкідливих програм до різних операційних систем, як-от Windows і Linux. Вже відмічається збільшення випадків атаки такими вірусами секторів охорони здоров'я та освіти.

6. АНАЛІТИЧНІ ОЦІНКИ

КОМПАНІЯ CISCO TALOS ОПРИЛЮНИЛА СВІЙ РІЧНИЙ ЗВІТ ЗА 2022 З ОКРЕМИМ БЛОКОМ ПРО УКРАЇНУ

14 грудня безпека компанія Cisco Talos оприлюднила звіт про основні загрози кібербезпеки у 2022 році. Окремий блок цього звіту присвячено кібербезпековій ситуації в Україні. Фахівці компанії підсумували основні джерела загроз, найбільш помітні кібератаки, в також дають огляд основних патернів поведінки зловмисних акторів, які виступають проти України та її союзників в кіберпросторі. «Наша телеметрія, результати роботи оперативного підрозділу та полювання на загрози свідчать про те, що рівень загрози проти українських організацій не зменшується», – вказують автори звіту.

ДОСЛІДНИКИ КІБЕРБЕЗПЕКИ ВКАЗУЮТЬ НА ЗРОСТАННЯ ЗАГРОЗ ВІД XLL – CISCO TALOS

20 грудня аналітики компанії Cisco Talos оприлюднили звіт про поширення популярності у зловмисних груп вразливості в XLL – файлах Microsoft Excel. Починаючи з 2021 року вразливості в цьому типі файлів набуває все більшої популярності у зловмисних груп, в т.ч. тих, що зорієнтовані на шпигунські дії: APT10 (КНР), TA410 (КНР), Fin7 (росія) та інші. Cisco Talos вважає, що підприємствам слід очікувати більше атак зловмисних програм на основі XLL.

ЗА RANSOMWARE ROYAL СТОЇТЬ CONTI TEAM ONE - TREND MICRO

21 грудня аналітики Trend Micro представили свій аналіз функціонування ransomware Royal. Вони роблять висновок, що за його розробкою та функціонуванням стоїть група Conti Team One. Аналіз охоплює період з вересня по грудень цього року – за цей період атаки Royal були спрямовані передусім на США та Бразилію.

RANSOMWARE CUBA ВИКОРИСТОВУЄ У СВОЇХ АТАКАХ ЗЛОВМИСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ПІДПИСАНЕ СЕРТИФІКАТОМ MICROSOFT – WIRED

13 грудня видання Wired повідомило, що безпекові компанії, які вивчають діяльність групи Cuba Ransomware помітили, що ransomware для закріплення в системі використовує підписані сертифікатом Microsoft драйвери (Microsoft Windows Hardware Developer Program). Корпорація Майкрософт заявила, що призупинила роботу облікових записів Центру партнерів, які зазнали зловживань, відкликала фальшиві сертифікати та випустила оновлення безпеки для Windows, пов'язані з цією ситуацією.

NASA МАЄ ПРОБЛЕМИ ІЗ ПОБУДОВОЮ КІБЕРБЕЗПЕКИ – УПРАВЛІННЯ ГЕНЕРАЛЬНОГО ІНСПЕКТОРА NASA (OIG)

21 грудня Управління генерального інспектора NASA (OIG) опублікувало свій щорічний аудит інформаційної безпеки аерокосмічного агентства. Результат оцінки «Не ефективний». Метою оцінки було визначення рівня кіберзрілості організації відповідно до вимог федерального Закону про модернізацію інформаційної безпеки від 2014 року. Він визначає 5 рівнів кіберзрілості – NASA не змогла досягти за жодною з 5 вимірюваних функцій вище 3-го рівня кіберзрілості. Агентства було надано список із 17 рекомендованих дій для поліпшення стану кіберзахисту. У 2019 році схожа оцінка продемонструвала ще нижчий рівень кіберзрілості організації.

NSA ОПРИЛЮДНИЛО СВІЙ ОГЛЯД КІБЕРБЕЗПЕКИ ЗА 2022 РІК

15 грудня NSA оприлюднило свій комплексний звіт про стан кібербезпеки у 2022 році. Звіт концентрується на основних здобутках NSA за рік та вказує на низку пріоритетних сфер інтересу NSA: кібербезпека критичної інфраструктури, просування політики zero trust на всіх рівнях, розвиток партнерських відносин з приватним сектором, посилення спроможностей американських військових на полі бою. Також звіт визначає три головні суб'єкти загроз, які найбільш активно загрожують безпеці США в кіберпросторі: Іран, росія (передусім через підтримку США України) та КНР.

ЄВРОПЕЙСЬКІ КРАЇНИ ПРОДОВЖУЮТЬ КОРИСТУВАТИСЬ КИТАЙСЬКИМ ОБЛАДНАННЯМ ДЛЯ 5G – ДОСЛІДЖЕННЯ STRAND CONSULT

Дослідження Strand Consult показує, що у численних європейських країнах (серед яких Німеччина, Румунія, Нідерланди, Австрія, Угорщина та інші) все ще більш ніж 50% обладнання 5G належить китайським виробникам. Найбільше проблем з заміною такого обладнання відчувають ті країни, які першими почали розбудовувати 5G мережі – це істотно звужує їх можливості із заміни постачальників.

ЕКСПЛУАТАЦІЯ ВІДОМИХ СТАРИХ ВРАЗЛИВОСТЕЙ, АТАКИ НА API ТА ІНШІ ЗАГРОЗИ – ПРОГНОЗИ TRUSTWAVE НА 2023 РІК

У грудні 2022 року спеціалісти компанії Trustwave оприлюднили декілька своїх прогнозів (перша та друга частини) щодо кіберзагроз у 2023 році. Серед цих прогнозів:

- зростання вірогідності експлуатація вже відомих вразливостей;
- нові атаки на API;
- розширення ринку RaaS, більший акцент на MDR замість «традиційних» SOC;
- збільшення ролі невеликого кола постачальників послуг кібербезпеки;
- поява нових технік атак на фоні триваючої російсько-української кібервійни;
- зростання атак на хмарні сервіси;
- більше загроз для SCADA/OT.

НОВИЙ ЗВІТ: У 2022 РОЦІ ШАХРАЙСТВО З ОСОБИСТИМИ ДАНИМИ ПОДВОЇЛОСЯ В КРИПТО- ТА БАНКІВСЬКІЙ СФЕРІ

Першого грудня Sumsub опублікувала другий щорічний звіт про шахрайство з ідентифікаційною інформацією, який описує тенденції та статистику на основі мільйонів перевірок ідентифікаційних даних у 21 галузі та більше ніж 500 000 випадків шахрайства між 2021-2022 роками.

Сім ключових висновків зі звіту Sumsub про шахрайство з особистими даними:
1. 55,8% усіх випадків шахрайства відбувається в 5 країнах, а саме у В'єтнамі, Бангладеш, Нігерії та Пакистані та США, де було зафіксовано 5,1% випадків.
2. У кіберспорті найбільше випадків шахрайства з особистими даними, їх частка складає 2,9% від загальної кількості випадків
3. У 2022 році як у криптовалюті, так і в банківській справі кількість шахрайства з особистими даними зросла майже вдвічі
4. Шахрайство з платежами зросло на 40% у 2022 році
5. ID-картки – найпоширеніший вид документів, який підробляли у 2022 році
6. У 2022 році в 79% усіх підроблених документів були видані на осіб чоловічої статі
7. Deepfakes стають все більш досконалими і їх популярність зростає

ДЕТАЛЬНИЙ АНАЛІЗ ТЕХНІК ЗЛОВМИСНОЇ ГРУПИ TA453 – ЗВІТ PROOFPOINT

14 грудня кібербезпекова компанія Proofpoint оприлюднила свій детальний аналіз діяльності зловмисної групи TA453, яку пов'язують із Корпусом стражів ісламської революції (Іран). Серед ключових висновків:
- угрупування активно змінює свої техніки та процедури з метою більшої ефективності кожної операції;
- коло атакованих об'єктів розширюється – від медичних дослідників до рієлторів і туристичних агентств;
- певні приклади кіберактивності TA453 демонструє можливий їх зв'язок з проведенням таємних і навіть кінетичних операцій Корпусу стражів ісламської революції.

ГЕОПОЛІТИКА ШІ ТА ЗАКРІПЛЕННЯ ІДЕЇ ЦИФРОВОГО СУВЕРЕНІТЕТУ

Дослідниця Brookings Бріанна Нікер (Brieanna Nicker) пише, що Раду США–ЄС з питань торгівлі та технологій (ТТС) можна розглядати як початкові кроки до формування альянсу навколо орієнтованого на права людини підходу до розвитку ШІ в демократичних країнах. Однак різниця підходів з авторитарними країнами може призвести до технологічного відокремлення, яке стане національним стратегічним відокремленням інших пов'язаних технологій.

Історично склалося так, що поява інтернету створила можливість для світу бути взаємопов'язаним в одну глобальну цифрову екосистему. Однак зростання недовіри між країнами спричинило зростання цифрового суверенітету, що означає здатність нації контролювати напрямок свого руху у цифровому просторі та може включати контроль над усім ланцюжком постачання ШІ – від даних до апаратного та програмного забезпечення.

Наслідком тенденції до більшого цифрового суверенітету, яка потім посилює цю тенденцію, є зростаючий страх бути відрізаними від критично важливих цифрових компонентів, таких як комп'ютерні чіпи, і відсутність контролю над міжнародним потоком даних громадян. Ці події загрожують наявним формам взаємозв'язку, спричиняючи фрагментацію ринків високих технологій і, різною мірою, повернення до національної держави.

ЯК ШПИГУНСЬКЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЗАГРОЖУЄ ДЕМОКРАТІЇ

У статті для Foreign Affairs Директор Citizen Lab Університету Торонто Рональд Дейберт попереджає про загрозу, яку «революція шпигунського програмного забезпечення» становить для демократії. Технології стеження стали легкодоступними і дозволяють державам і приватним особам стежити майже за ким завгодно в будь-якій точці світу за допомогою мобільних телефонів.

Автократичні режими все частіше використовують ці технології для стеження за громадянами, нейтралізації політичної опозиції та придушення інакомислення, але використовують їх не лише авторитарні уряди. Багато демократичних країн також почали використовувати передові технології шпигунського програмного забезпечення.

«Поширення цієї технології загрожує розмиванням багатьох інституцій, процесів і цінностей, від яких залежить ліберальний міжнародний порядок». Якщо еліти в будь-якій країні можуть використовувати шпигунські технології для консолідації влади, то майбутнє демократії «незабаром може бути не більш безпечним, ніж паролі на наших телефонах», – пише Дейберт.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

НКЦК ПРОВІВ КОМАНДНО-ШТАБНІ НАВЧАННЯ СТРАТЕГІЧНОГО РІВНЯ З ПИТАНЬ КІБЕРБЕЗПЕКИ

НКЦК за підтримки Проєкту USAID Cybersecurity Activity вдруге провів щорічні командно-штабні навчання (ТТХ) стратегічного рівня «Національна кіберготовність – 2022». У них взяли участь представники всіх членів НКЦК, суб'єктів кібербезпеки України, об'єктів критичної інфраструктури, НКЕК та ряду міністерств.

Під час навчань відпрацьовано алгоритм застосування Порядку взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки, затвердженого на засіданні НКЦК 22 вересня 2022 року, зокрема щодо реагування на загрози червоного та чорного рівнів небезпеки.

Командно-штабні навчання дозволили скоординувати дії всіх суб'єктів кібербезпеки й відпрацювати ефективний алгоритм взаємодії, щоб весь сектор безпеки і оборони був готовий злагоджено відреагувати у разі ескалації з боку країни-агресора.

ОГОВОРЕНО ПРОМІЖНІ ЗДОБУТКИ ТА НАСЛІДКИ ВІЙНИ У КІБЕРПРОСТОРІ НА XVI ЗАСІДАННІ НАЦІОНАЛЬНОГО КЛАСТЕРА КІБЕРБЕЗПЕКИ

8 грудня 2022 року відбулося XVI підсумкове засідання Національного кластера кібербезпеки на тему «Війна в кіберпросторі 2022: підсумки, здобутки та прогалини». Захід організовано НКЦК з Фондом цивільних досліджень та розвитку США за підтримки Державного департаменту США.

До обговорення підсумків 2022 року долучилися близько 200 представників державних органів, приватного сектору, об'єктів критичної інфраструктури, а також міжнародних організацій з США та країн-членів ЄС. З-поміж них – представники Міноборони, МЗС, СБУ, Держспецзв'язку, Кіберполіції, USAID, урядів США та Естонії, CDTO міністерств та представники приватного сектору.

Під час засідання були представленні результати двох незалежних досліджень стану кібербезпеки України. За результатами Щорічного дослідження щодо ефективності взаємодії та координації суб'єктів національної системи кібербезпеки індекс ефективності координації зростає третій рік поспіль, і в цьому році становить 6,5. Досягнення такого показника було заплановано на 2024 рік. Також порівняно з минулими роками вдвічі більше респондентів відзначили важливість координації на національному рівні, та сказали, що НКЦК потрібні додаткові повноваження в цій сфері.

НКЦК ПРАЦЮЄ НАД УДОСКОНАЛЕННЯМ ПРОЦЕДУРИ ВЗАЄМОДІЇ ТА ЗАБЕЗПЕЧЕННЯ СВОЄЧАСНОГО ІНФОРМУВАННЯ ПРО КІБЕРІНЦИДЕНТИ НА ЗАКОНОДАВЧОМУ РІВНІ

15 грудня 2022 року НКЦК за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури» провів засідання круглого столу на тему: «Національний план реагування на надзвичайні ситуації в кіберпросторі: законодавчі аспекти взаємодії, забезпечення надійного та своєчасного інформування про кіберінциденти».

Мета заходу – формування спільного бачення критичної важливості своєчасного і вичерпного інформування про виявлені кібератаки як складової забезпечення стійкості та готовності до кіберінцидентів.Важливим аспектом обговорення також стало реагування на надзвичайні ситуації в кіберпросторі, зокрема на національному рівні, та розробка пропозицій для внесення змін до українського законодавства щодо забезпечення стійкості і готовності до кіберінцидентів, зокрема про інформування.

У заході взяли участь представники Апарату РНБО України, Верховної Ради України, об'єктів критичної інфраструктури, Кіберполіції, державного сектору, приватних компаній, експерти у сфері кібербезпеки. За результатами обговорення внесено пропозиції щодо наповнення та реалізації Плану з урахуванням досвіду реагування на кібератаки під час війни.

ДОСВІД УКРАЇНСЬКИХ ІТ-ФАХІВЦІВ ТА РОЗРОБНИКІВ МОЖЕ ВИКОРИСТОВУВАТИСЯ У МАЙБУТНІХ ВІЙСЬКОВИХ ОПЕРАЦІЯХ США

Про це на зустрічі із заступником Міністра оборони України з питань цифрового розвитку, цифрових трансформацій і цифровізації Олегом Гайдуком заявила заступниця Державного секретаря США з політичних питань Вікторія Нуланд, яка перебувала з візитом у Києві. Обговорено актуальні та перспективні питання співпраці в оборонній сфері.

Вікторія Нуланд високо оцінила можливості української військової системи ситуаційної обізнаності «Дельта», її гнучкість та сумісність з аналогічними платформами країн-членів НАТО. Заступниця Держсекретаря США підтримала ініціативи української сторони з розширення спроможностей ІТ-системи, яка допомагає отримувати повну оперативну картинку поля бою та сил ворога.

З ПОЧАТКУ РОКУ СБУ НЕЙТРАЛІЗУВАЛА ПОНАД 4,5 ТИС. КІБЕРАТАК НА УКРАЇНУ

«Ми підійшли до 2022-го року, маючи позаду 8-річний досвід гібридної війни. Адже війна у кіберпросторі тривала і раніше. На момент вторгнення ми вже були готові до найгірших сценаріїв. А масовані кібератаки, які ми відбили в січні та лютому, стали додатковими «тренуваннями» перед вторгненням», – зазначив начальник Департаменту кібербезпеки СБУ Ілля Вітюк.

Він підкреслив, що з початком повномасштабної агресії роботи стало набагато більше. Якщо у 2020 році було зафіксовано майже 800 кібератак, у 2021 – 1400, то вже цьогоріч – їхня кількість зросла у понад 3 рази. В зоні особливої уваги ворога є енергетика, логістика, військові об'єкти, а також – бази даних органів влади та інформресурси.

КІБЕРПОЛІЦІЯ ПРОВЕЛА ЗАГАЛЬНОНАЦІОНАЛЬНУ ОПЕРАЦІЮ З ПРИПИНЕННЯ ДІЯЛЬНОСТІ ВОРОЖИХ БОТОФЕРМ

Під час обшуків вилучено понад 100 тисяч SIM-карток, які використовувалися для реєстрації фейкових акаунтів. Загалом бот-мережі налічували понад півтора мільйона облікових записів у різних соцмережах, поштових сервісах та месенджерах. Ботів реєстрували для поширення фейків і пропаганди, проросійських наративів, виправдання дій окупантів, розповсюдження протиправного контенту.

За результатами операції Департаменту кіберполіції викрито протиправну діяльність 31 фігуранта з різних областей України. Крім цього, припинено діяльність ботоферми, яка функціонувала для розсилки неправдивих повідомлень про мінування об'єктів на території України.

Також під час операції кіберполіцейські виявили факт «зараження» мобільних пристроїв громадян шкідливим програмним забезпеченням. Принцип його дії полягав у прихованому віддаленому отриманні перевірочних SMS-повідомлень при реєстрації акаунтів на різних сервісах.

Загалом припинено діяльність 13 ботоферм, які налічували понад 1,5 мільйона фейкових акаунтів. Заблоковано роботу 28 вебресурсів на території України, які використовувались для реєстрації мобільних номерів і подальшого створення бот-мереж.

МІНЦИФРА СПІВПРАЦЮВАТИМЕ З НАЙБІЛЬШОЮ РОЗВІДУВАЛЬНОЮ КОМПАНІЄЮ У СВІТІ RECORDED FUTURE У СФЕРІ КІБЕРЗАХИСТУ – ПІДПИСАНО МЕМОРАНДУМ

Мінцифра розширює співпрацю з найбільшою розвідувально-аналітичною компанією у світі Recorded Future. Команда підписала Меморандум у сфері захисту критичної інфраструктури в Україні від військової та кіберагресії з боку росії. Також домовилися про спільну роботу над створенням нових продуктів і технологій для захисту критичної інфраструктури, які зможуть використовувати в усьому світі.

Підписаний меморандум дасть змогу підсилити партнерство та використовувати розвідувальні дані для захисту України у фізичному та кіберпросторі. У межах документа Recorded Future надасть свою розвідувальну платформу, спеціалізованих інженерів та аналітиків розвідки. Зі свого боку Мінцифра надасть власну експертизу та спеціалістів, які співпрацюватимуть з Recorded Future.

З початку повномасштабної війни Recorded Future надала розвідувальні дані для захисту критичної інфраструктури України, допомогла в розслідуванні воєнних злочинів росіян в Україні, відкрила доступ до програмної платформи Intelligence Cloud на понад $10 мільйонів. Окрім цього, розширила розвідку про загрози щодо російських кібератак.

СБУ ВИКРИЛА ПІД ЧАС ВІЙНИ БІЛЬШЕ ОДНІЄЇ ТИСЯЧІ ВОРОЖИХ ІНТЕРНЕТ-АГІТАТОРІВ, ЯКІ ПОШИРЮВАЛИ ФЕЙКИ ПРО ВІЙНУ В УКРАЇНІ

З початку повномасштабного вторгнення рф кіберфахівці СБУ викрили понад 1200 агітаторів, які поширювали в інтернеті фейки та російські наративи. Майже 600 із них – уже отримали повідомлення про підозру. Про це заявив начальник Департаменту кібербезпеки СБУ Ілля Вітюк.

«СБУ виявляє зрадників, ворожих агітаторів і колаборантів, що діють в інтернет-просторі. Сьогодні в нас майже 1200 кримінальних проваджень по них, 600 фігурантам повідомлено про підозри та майже 230 засуджено до різних термінів ув'язнення. Також цього року вже заблокували 45 масштабних ботоферм потужністю понад 2 млн фейкових акаунтів, майже 500 проросійських Youtube-каналів з аудиторією більше ніж 15 млн підписників і близько тисячі інформресурсів, які працювали проти України», – розповів він.

Водночас Вітюк зауважив, що потужний кіберспротив – це результат взаємодії багатьох людей і організацій, бо наші громадяни перетворилися на справжню кіберТрО.

ВІКТОР ЖОРА ЗАКЛИКАВ МІЖНАРОДНУ СПІЛЬНОТУ АКТИВНО ДОЛУЧИТИСЯ ДО ПОБУДОВИ ГЛОБАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ

Заступник голови Держспецзв'язку Віктор Жора став одним із ключових спікерів міжнародного Cybersecurity@CEPS Summit 2022, що проходив у Брюсселі. Ключовою темою конференції став пошук нових правил безпеки для мереж і продуктів, посилення координації зусиль на рівні ЄС для реагування на кіберкризи та нові виклики, зокрема – формування глобального управління кібербезпекою для нового світового порядку.

Під час онлайн-виступу на сесії-відкритті заступник голови ДССЗЗІ наголосив на необхідності концентрації уваги цивілізованого світу на захисті від кібертероризму та від цілеспрямованої кіберагресії.

«Після 24 лютого світовий порядок змінився. Як раніше вже не буде. Розв'язана росією повномасштабна війна проти України точиться, в тому числі і в кіберпросторі. Більш того, під прицілом російських хакерів не тільки Україна, а й її союзники – практично весь демократичний, цивілізований світ. Сьогодні ми стоїмо перед викликами, які ще декілька років тому могли здатися малоймовірними. Сьогодні наша солідарна робота задля захисту в кіберпросторі важлива як ніколи», – зазначив Віктор Жора.

ДЕРЖСПЕЦЗВ'ЯЗКУ ВІДВІДАЛА ЗАСТУПНИЦЯ ДЕРЖСЕКРЕТАРЯ США ВІКТОРІЯ НУЛАНД

Держспецзв'язку відвідала заступниця Державного секретаря США з політичних питань Вікторія Нуланд та зустрілася з керівництвом Служби. Під час візиту заступниця Державного секретаря США ознайомилася з роботою Урядової команди реагування на комп'ютерні надзвичайні події (CERT-UA), діяльністю Кіберцентру UA30, а також інноваційними розробками українських виробників, закупленими Держспецзв'язку для потреб українських захисників, які дозволяють українським військовим ефективніше протидіяти ворогу на полі бою.

НКЦК ЗА ПІДТРИМКИ CRDF GLOBAL В УКРАЇНІ ПРОВЕЛИ ТРЕНІНГ НА ТЕМУ «ЦИФРОВА КРИМІНАЛІСТИКА» ДЛЯ СПЕЦІАЛІСТІВ З КІБЕРБЕЗПЕКИ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ

Протягом п'яти днів понад 40 представників сектору безпеки та оборони навчались виявляти, фіксувати та вилучати цифрову інформацію, яка може стати доказом скоєних злочинів проти нашої держави та її громадян.

Саме завдяки збору якісної доказової бази про злочинні дії рф, яка буде визнана допустимою та належною як для національних, так і міжнародних судів, ми зможемо притягнути кожного винного до відповідальності.

КУРСАНТИ ІНСТИТУТУ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ ПРОЙШЛИ ПІДГОТОВКУ НА БАЗІ КІБЕРЦЕНТРУ UA30

Студенти четвертого курсу Інституту спеціального зв'язку та захисту інформації (ІСЗЗІ) Національного технічного університету України «КПІ імені Ігоря Сікорського» пройшли навчання на базі Тренінгового центру Кіберцентру UA30.

У межах практичного тренінгу «Промислові системи керування. Основи кібербезпеки» курсанти ІСЗЗІ ознайомилися з особливостями кібербезпеки в середовищах промислових систем керування (ПСК), розглянули стандарти та платформи для керування кібербезпекою, а також моделі застосування принципів кібербезпеки до промислових мереж.

КІБЕРПОЛІЦІЯ ВИКРИЛА ЗЛОВМИСНИКА У ПРИВЛАСНЕННІ МАЙЖЕ 2,4 МЛН ГРН НА ПРОДАЖІ НЕІСНУЮЧИХ ТОВАРІВ

Протиправну діяльність 61-річного чоловіка викрили співробітники управління протидії кіберзлочинам Києва спільно зі слідчими Дарницького управління поліції. Чоловік на інтернет-майданчиках розміщував фейкові оголошення щодо продажу товарів. Зокрема пропонував постачання гуртових партій медичних масок. Фігурант також утворював фіктивні підприємства для переконання клієнтів у безпечності купівлі. Однак, отримавши гроші покупців, зловмисник зникав.

Встановлено, що у такий спосіб він ошукав фізичних та юридичних осіб на майже 2,4 млн грн. Підозрюваному може загрожувати до дванадцяти років позбавлення волі з конфіскацією майна. Наразі тривають слідчі дії.

ВІДБУВСЯ ТРЕТІЙ НАВЧАЛЬНИЙ МОДУЛЬ ПРОГРАМИ СТРАТЕГІЧНОГО ЛІДЕРСТВА ДЛЯ УПРАВЛІНЦІВ У СФЕРІ КІБЕРБЕЗПЕКИ «SJC-2022»

Головною метою програми є підвищення рівня професійної підготовленості керівників державного та приватного секторів, політиків, які залучені до створення спільних стратегічних рішень з питань кібербезпеки.

Третій модуль був присвячений неочевидним партнерствам, ролі стратега та принципам створення стратегії в надсистемах і екосистемах, а також виміру семантичного протистояння. Цього разу до викладачів долучились представники Cyber Defense Assistance Collaborative. Вони поділились успішними кейсами та прикладами стратегічних рішень у кіберпросторі національного рівня.

Програма стратегічного лідерства розроблена Global Cyber Cooperative Center спільно із кращими міжнародними експертами та за підтримки Національного координаційного центру кібербезпеки.

ДЕРЖСПЕЦЗВ'ЯЗКУ ПРОВЕЛА ОСВІТНІЙ КУРС ІЗ КІБЕРЗАХИСТУ ДЛЯ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВНОГО СЕКТОРУ

У грудні завершився курс для фахівців категорії «Б», які безпосередньо забезпечують захист. Курс складався із шести модулів: розуміння ландшафту загроз, державна інфраструктура для забезпечення кіберзахисту, законодавча база в галузі кібербезпеки та захисту інформації, особливості бюджетування в державному секторі, а також реформування системи підготовки кадрів у країні.

Метою курсу було допомогти державним органам підвищити власну кіберстійкість та налагодити плідну співпрацю між об'єктами кіберзахисту та структурними підрозділами Служби, які надають відповідні сервіси в галузі кіберзахисту та здійснюють формування державної політики.

ЗАДЛЯ ПОСИЛЕННЯ КІБЕРЗАХИСТУ МІНЦИФРА ПІДПИСАЛА МЕМОРАНДУМ З МІЖНАРОДНОЮ КОМПАНІЄЮ «ІНТЕРНЕТ 2.0»

Команда Мінцифри підписала меморандум про співпрацю з провідною організацією з кібербезпеки США та Австралії «Інтернет 2.0». Домовилися про співробітництво у сфері кіберзахисту та навчання українських ветеранів навичкам кібербезпеки.

«В Україні розпочав роботу провідний партнер міжнародної Ініціативи протидії кібервимагачам (Counter Ransomware Initiative, CRI) «Інтернет 2.0». Початок нашої співпраці – це позитивний сигнал для інших міжнародних компаній і брендів про те, що саме зараз Україна може і має стати потужним партнером у реалізації спільних проєктів», – зазначив заступник Міністра цифрової трансформації Георгій Дубинський.

Україна стала першим у світі партнером «Інтернет 2.0» за межами країн розвідувального альянсу ФВЕЙ (FVEY), до якого входять Австралія, Канада, Нова Зеландія, Велика Британія та США. Згідно з Меморандумом компанія забезпечить навчання українців з кібербезпеки та надаватиме аналітичну підтримку Україні у боротьбі з кібератаками.

У межах Меморандуму «Інтернет 2.0» надаватиме свої технології та поділиться передовим досвідом для потреб кіберзахисту України. Навчатиме українських ветеранів навичок кібербезпеки та цифрових технологій. Також компанія відкриє офіс в Україні.

КІБЕРПОЛІЦІЯ ВИКРИЛА ОДЕСЬКОГО ПРОВАЙДЕРА У НАДАННІ ДОСТУПУ АБОНЕНТАМ ДО РОСІЙСЬКОГО КОНТЕНТУ

Попри заборону, підприємство надавало безперешкодний доступ до трансляції пропагандистських телеканалів та інтернет-ресурсів рф і так званих «лднр». За такі дії фігурантам може загрожувати до 12 років позбавлення волі.

Попри заборону РНБОУ, компанія не здійснювала блокування контенту країни-агресора. Натомість співробітники підприємства налаштовували своє обладнання таким чином, щоб користувачі мали змогу безперешкодно отримувати доступ до телебачення, інтернет-ресурсів рф і тимчасово окупованих територій України. Послуга з підключення коштувала 3000 гривень і надалі користувачі сплачували 250 гривень щомісячної абонплати.

Відкрито кримінальне провадження відповідно до ст. 27, ч. 2 ст. 110 (Посягання на територіальну цілісність і недоторканність України) ч. 6 ст. 111-1 (Колабораційна діяльність) КК України. Слідчі дії тривають.

ДЕРЖСПЕЦЗВ'ЯЗКУ ЗМІЦНЮЄ СПІВПРАЦЮ З АВСТРАЛІЙСЬКИМ БІЗНЕСОМ ЗАДЛЯ ДОПОМОГИ ВІЙСЬКОВИМ ВЕТЕРАНАМ

Представники австралійської компанії Internet 2.0, яка спеціалізується на рішеннях у сфері кібербезпеки та кіберзахисту, завітали з візитом до Держспецзв'язку, відвідали Кіберцентр UA30 та ознайомилися з роботою Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

«Наша співпраця з Україною означає, що обидві сторони можуть вчитися одна в одної. Австралії може бути корисним досвід першої країни, яка витримала справжню кібервійну», – зазначив співголова компанії Роберт Поттер.

Під час зустрічі обговорили ініціативи, над якими працює Internet 2.0 в Україні.

З ПОЧАТКУ РОКУ КІБЕРПОЛІЦІЯ ВИКРИЛА ПОНАД 600 ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ ВІРТУАЛЬНИХ АКТИВІВ

Про це розповів начальник управління оперативно-аналітичного забезпечення та аналізу відкритих джерел Департаменту кіберполіції Євгеній Панченко. У складі делегації з України він взяв участь у міжнародному семінарі, присвяченому обговоренню механізмів арешту віртуальних активів, а також запровадження додаткових санкцій у цій сфері проти рф.

Представники кіберполіції поділилися досвідом розслідування злочинів, пов'язаних із використанням криптовалют. З початку 2022 року кіберполіцейські розслідували понад 600 таких кейсів. Здебільшого зловмисники використовують цифрові активи для приховування та «відмивання» доходів, отриманих злочинним шляхом, купівлі-продажу заборонених товарів у Darknet.

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПІД ЧАС НАДЗВИЧАЙНИХ СИТУАЦІЙ – У ЛЬВОВІ НАВЧАЛИСЯ ПРОТИДІЯТИ ЗАГРОЗАМ

У межах міжнародного проєкту EURO-MED-REACT у Львівському державному університеті безпеки життєдіяльності відбулися масштабні командно-штабні навчання із цивільного захисту. У заході взяли участь заступник голови Держспецзв'язку Олександр Потій та начальник Управління Держспецзв'язку у Львівській області Сергій Жук.

Під час навчань учасники відпрацьовували алгоритм реагування місцевих, національних та міжнародних сил цивільного захисту на змодельовану надзвичайну ситуацію, яка, за сценарієм, має загрозу для критичної інфраструктури та інфраструктури у прикордонних районах. А також вивчали процес активації Об'єднаного механізму цивільного захисту ЄС, співпрацю між країнами та надання міжнародної допомоги у критичних випадках.

AMAZON WEB SERVICES НАДАЄ УКРАЇНІ ПІДТРИМКИ НА 75 МЛН ДОЛАРІВ НА ХМАРНІ ТЕХНОЛОГІЇ, ЯКІ ДОПОМАГАЮТЬ СТАБІЛЬНО ПРАЦЮВАТИ ЦИФРОВІЙ ДЕРЖАВІ ТА ЕКОНОМІЦІ

Віцепрем'єр-міністр – Міністр цифрової трансформації України Михайло Федоров та Директор з питань державної трансформації Amazon Web Services Ліам Максвелл підписали Меморандум про співпрацю у галузях цифрової трансформації, державного управління, цифрової грамотності та інновацій.
Amazon Web Services надає підтримку Україні на 75 млн доларів. Ці кошти виділені на послуги з міграції державних реєстрів, інших необхідних для функціонування держави баз даних до хмарного середовища AWS. Завдяки цьому реєстри продовжують працювати навіть під час обстрілів та відключень електрики, а українці можуть безперебійно отримувати держпослуги. Також це забезпечує безпеку всіх даних, адже цифрову інфраструктуру неможливо знищити ракетами.
З перших днів повномасштабного вторгнення Amazon Web Services надала потужну підтримку Україні. Забезпечила хмарними технологіями, які дали змогу зберегти важливі українські державні, банківські та освітні дані. Завдяки міграції даних вдалося захистити критичну інфраструктуру, а держава продовжила функціонувати.

НАЦІОНАЛЬНЕ АГЕНТСТВО КВАЛІФІКАЦІЙ ВНЕСЛО ДО РЕЄСТРУ КВАЛІФІКАЦІЙ ВІДОМОСТІ ЩОДО НОВИХ ШЕСТИ ПРОФЕСІЙНИХ СТАНДАРТІВ У ГАЛУЗІ КІБЕРБЕЗПЕКИ

Національне агентство кваліфікацій поінформувало Адміністрацію Держспецзв'язку про внесення до Реєстру кваліфікацій відомостей щодо професійних стандартів «Розробник систем захисту інформації», «Адміністратор мереж і систем», «Фахівець сфери захисту інформації», «Аналітик з безпеки інформаційно-телекомунікаційних систем», «Фахівець з питань безпеки (інформаційно-комунікаційні технології)», «Інструктор-методист з інформаційної безпеки та кібербезпеки».
Внесення цих профстандартів до Реєстру кваліфікацій означає, що відтепер заклади вищої освіти можуть використовувати ці стандарти для вдосконалення освітніх програм та запровадження спеціалізації, а самі фахівці та роботодавці – для оцінки відповідності рівня знань, умінь та навичок актуальним потребам галузі.

GOOGLE АНОНСУВАВ НОВИЙ ПАКЕТ ПІДТРИМКИ ДЛЯ УКРАЇНИ

Першого грудня компанія Гугл анонсувала, що буде надавати більше підтримки українському уряду в питаннях технічної інфраструктури (безоплатний доступ до Google Workspace та модель нульової довіри у питаннях кібербезпеки), фінансувати програми набуття цифрових навичок і українські стартапи, а також надавати гуманітарну допомогу постраждалим у війні з росією.

ПІДВИЩУЄМО ОБІЗНАНІСТЬ ДІТЕЙ У СФЕРІ КІБЕРБЕЗПЕКИ ЗА ДОПОМОГОЮ КОМАНДНО-ШТАБНОЇ ГРИ «КІБЕРДЖУРА»

13 грудня 2022 року «Міжнародна академія геоінформатики» презентувала новий етап навчань — вдосконалену командно-штабну гру «Кіберджура-Форсайт», метою якої є ознайомлення дітей з основами організації простору за допомогою геоінформаційних систем (ГІС). Школярі зможуть моделювати історичні події, аналізувати причиново-наслідкові ланцюжки, досліджувати довкілля та проєктувати візію власного майбутнього в Україні.

«Кіберджура» – підхід національно-патріотичного виховання учнів та студентів через профорієнтацію. Він спрямований на впровадження сучасних інформаційних технологій в навчальному процесі в межах Всесвітнього проєкту модернізації освіти: створення шкільних інтегрованих уроків засобами ArcGIS від Esri (США).

8. ПЕРША СВІТОВА КІБЕРВІЙНА

АНАЛІЗ ЦИФРОВОГО ПОЛЯ БОЮ: ЯК ІНТЕРНЕТ ЗМІНИВ ВІЙНУ

Наразі внаслідок війни в Україні виникли три важливі цифрові тренди, пише Стівен Фельдштейн на ресурсі War on the Rocks. По-перше, технологічні інновації допомогли Україні компенсувати військову перевагу Росії, зокрема шляхом збільшення участі звичайних громадян.

По-друге, оскільки ці громадяни стали винятково залученими до цифрової війни, межі між цивільними та військовими учасниками розмилися. Міжнародне гуманітарне право не встигає за цим, що викликає зростаюче занепокоєння щодо застосування правил війни в цифровому конфлікті.

По-третє, конфлікт породив величезну кількість даних, потенційно корисних для притягнення військових злочинців до відповідальності. Однак поширення розслідувань за відкритими джерелами також створює нові ризики аналітичної упередженості та процедурних неузгодженостей.

Фельдштейн не пропонує рішень, але закликає звернути увагу на ці проблеми.

НАЙАБСУРДНІША НОВИНА: ВБИВЦІ З ЧВК «ВАГНЕР» ПРОВОДЯТЬ ХАКАТОН

Незаконне збройне формування, відоме як ЧВК «Вагнер», оголосило про те, що збирається проводити хакатон, де шукатиме найкращих пілотів дрону. Це оголошення виклали на піддомені основного домену цієї групи.

Абсурдність цього оголошення вражає: група, яка на камеру страчує кувалдою своїх колишніх членів залучає до своїх лав зеків та масово вбиває мирне населення, намагається залучити до своєї діяльності програмістів та операторів дронів.

Група «Вагнер» відома багатьма воєнними злочинами, які її члени скоювали, зокрема і на українській території. Зараз вони оголосили хакатон, який триватиме з 20 по 23 грудня 2022, з призовим фондом у 1,5 млн рублів. Його учасники (якщо комусь прийде в голову на таке зголоситися) демонструватимуть свої навички роботи з дронами: шукатимуть інші дрони у зоні видимості, пілотуватимуть власні дрони, і таке інше.

Найкращих учасників покличуть працювати у ЧВК «Вагнер». Сайт цього «хакатону» (якщо перевіряти домен та пов'язані з ним IP) хоститься на AWS. Тож непоганою ідеєю було би оформити скаргу на нього на адресу Amazon.

ВАТИКАН, ВІРОГІДНО, ЗАЗНАВ КІБЕРАТАКИ ЧЕРЕЗ КІЛЬКА ДНІВ ПІСЛЯ ТОГО, ЯК ПАПА РИМСЬКИЙ РОЗКРИТИКУВАВ РОСІЮ

Першого грудня агенція Євроньюс повідомила, що Ватикан витримав значну DDoS атаку на свої сайти невдовзі після того, як Папа Римський Франциск зробив публічну заяву, інтерпретовану як критичну по відношенню до війни, яку веде рф. Ватикан заявив, що розслідування триває, і не атрибутував атаку. Посол України у Ватикані Андрій Юраш звинуватив рф.

ЗБРОЙНІ СИЛИ США ВИКОРИСТАЮТЬ ДОСВІД ОТРИМАНИЙ В РОСІЙСЬКО-УКРАЇНСЬКІЙ КІБЕРВІЙНІ У ДІЯЛЬНОСТІ СВОЄЇ СПЕЦІАЛЬНОЇ ГРУПИ, ЯКА СПЕЦІАЛІЗУЄТЬСЯ НА КНР

Першого грудня керівник Defense Intelligence Agency (DIA) генерал-лейтенант Скотт Бер'єр заявив, що вони врахують уроки, отримані під час російсько-української війни, зокрема, що стосується вказівок і попереджень, і застосують їх до сценаріїв, які можуть описати конфлікт навколо Тайваню. Цей досвід буде використано новоствореною New China Mission Group.

У травні Скотт Берріє визнав, що не врахував рішучості України до спротиву. Під час слухання у Сенаті він визнав, що не врахував низку факторів, які вплинули на український спротив: «я поставив під сумнів їх бажання боротися. Це була погана оцінка з мого боку, тому що вони воювали мужньо і чесно і чинять правильно» – сказав він.

РОСІЙСЬКІ ОРГАНІЗАЦІЇ АТАКУВАЛО НОВЕ ЗЛОВМИСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ CRYWIPER DATA WIPER, ЯКЕ ВИДАЄ СЕБЕ ЗА RANSOMWARE

Як повідомили 1 грудня дослідники компанії Kasperski, восени 2022 року було зафіксовано спроби раніше невідомого трояна, який вони назвали Crywiper, атакувати мережу організації в російській федерації. Дослідники компанії з'ясували, що цей троян, хоча і маскується під шифрувальника і вимагає від жертви грошей за «декодування» даних, насправді не шифрує, але цілеспрямовано руйнує дані в пошкодженій системі. До того ж, аналіз цієї програми показав, що це не помилка розробника, а його первісний задум. З деталями функціонування трояна можна ознайомитися у звіті компанії.

ПІДГОТОВКА ДО КІБЕРНАСТУПУ РОСІЇ ПРОТИ УКРАЇНИ ЦІЄЇ ЗИМИ

Після того як росія зазнала втрат на полі бою від України цієї осені, москва інтенсифікувала застосування багатовимірних гібридних технологічних підходів, щоб чинити тиск на внутрішні та зовнішні джерела військової та політичної підтримки Києва, пише у своєму звіті від 3 грудня компанія Microsoft.

Цей підхід включав руйнівні ракетні та кіберудари по цивільній інфраструктурі в Україні, кібератаки на українські, а тепер і закордонні ланцюги постачання, а також операції впливу з використанням кібернетичних засобів, спрямовані на підрив політичної підтримки України США, ЄС і НАТО, і похитнути впевненість і рішучість українських громадян. На думку компанії, цієї зими варто приготуватися до більш активного використання цих компонентів у війні рф проти України.

КІБЕРДИРЕКТОР NSA ПОПЕРЕДИВ ПРО РОСІЙСЬКІ АТАКИ НА СВІТОВИЙ ЕНЕРГЕТИЧНИЙ СЕКТОР

Кібердиректор Агентства національної безпеки (NSA) Роб Джойс заявив 15 грудня, що його продовжує турбувати можливість потужних кібератак з боку рф на глобальний енергетичний сектор, які можуть статися протягом наступних кількох місяців. Він закликав не втрачати пильність.

Попередження прозвучало в процесі представлення результатів щорічного кіберзвіту АНБ за 2022 рік, який зафіксував поширення російських загроз за межі України. Крім того, кібератаки на тлі триваючої російсько-української війни сприяли збільшенню обізнаності про кібербезпеку та інвестиціям. За словами Джойса, цього року кількість членів Центру кіберспівробітництва АНБ збільшилася майже втричі.

ЯК ЕСТОНІЯ ДОПОМАГАЄ УКРАЇНІ ПРОТИСТОЯТИ РОСІЙСЬКИМ КІБЕРЗАГРОЗАМ

Повідомлялося, що Естонія керує програмою Європейського Союзу вартістю майже 11 мільйонів євро для надання Україні послуг із захисту кібер- та цифрової конфіденційності.

Згідно з даними некомерційного Кільського інституту світової економіки, Естонія посідає друге місце в загальній фінансовій підтримці України за ВВП. Суму визначити складно, але це мільйони доларів.

Це партнерство ілюструє унікальний аспект сучасної кібервійни – деякі з найбільш постійних зусиль із захисту мереж надходять від менших або менш забезпечених ресурсами країн, які неодноразово ставали жертвами атак і на важкому шляху засвоїли необхідність інвестувати в кіберармії.

РОСІЯ СКОМПРОМЕТУВАЛА ВЕЛИКІ ОРГАНІЗАЦІЇ ВЕЛИКОБРИТАНІЇ ТА США ДЛЯ АТАК НА УКРАЇНУ

У звіті опублікованому компанією Lupovis 5 грудня, йдеться про те, що її дослідники використали платформу кіберобману, щоб дослідити поведінку російських хакерів. Тактика дослідження полягала у створенні приманок в Інтернеті, які використовувалися для заманювання російських зловмисників, щоб проаналізувати їх тактику, техніку та процедури (TTP).

Найбільше занепокоєння викликало те, що російські злочинці захопили мережі компаній Великобританії, США, Франції, Бразилії та Південної Африки, включно з компанією зі списку Fortune 500, і понад 15 медичних організацій, щоб здійснювати атаки на Україну.

РОСІЙСЬКИЙ ДЕРЖАВНИЙ БАНК ВТБ ПОСТРАЖДАВ ВІД НАЙБІЛЬШОЇ DDOS-АТАКИ В СВОЇЙ ІСТОРІЇ

Шостого грудня інформаційна агенція Рейтерс повідомила, що другий за розміром банк у рф зазнав DDoS-атаки з-за кордону. Працівники банку заявили, що атака є найбільшою в його історії, але запевнили своїх клієнтів, що їх дані не постраждали. Також вони підкреслили, що більша частина трафіку йшла з за меж росії.

У зв'язку з цим Microsoft попереджає європейські компанії про те, що росія може вдатись до контрзаходів в якості «помсти» за ці атаки, а такі країни як Польща, Німеччина, Великобританія та США знаходяться в зоні підвищеного ризику.

БІЙ З ТІННЮ ТА ГЕОПОЛІТИКА В ДАРКНЕТІ

У статті для американського видання Politico Мохар Чаттерджі (Mohar Chatterjee) описує, яким чином російсько-українська війна відобразилась на світі кіберзлочинних груп. На її думку, ці групи розділялися за геополітичними лініями і їх національні уподобання впливали на кіберзлочинну діяльність, яка до цього моменту була спрямована на отримання прибутку. Вона також описує, наскільки складно протистояти кіберзлочинності в ситуації геополітичного протистояння та розвитку технологій, які захищають анонімність користувачів.

У РОСІЙСЬКИХ МІСТАХ БУЛО ПОМІЧЕНО ЗБОЇ У РОБОТІ СИГНАЛУ GPS – WIRED

15 грудня видання Wired оприлюднило статтю про системні проблеми із функціонуванням GPS в російських містах (згадуються Саратов, Волгоград та Пенза). На думку опитаних журналістами експертів це, швидше за все, свідомі зусилля російської влади перешкодили можливим атакам дронів по важливим об'єктам військової інфраструктури. Водночас відмічається, що такі порушення сигналу GPS можуть створювати численні загрози цивільній інфраструктурі, а також руху водного та повітряного транспорту.

УКРАЇНСЬКА ЗАЛІЗНИЦЯ ТА ДЕРЖАВНІ ОРГАНИ ЙМОВІРНО УРАЖЕНІ ВІРУСОМ DOLPHINCAPE

Українські державні установи та Укрзалізниця стали жертвами нової хвилі фішингових атак, повідомила на початку грудня CERT-UA. Під час атаки хакери розсилали повідомлення нібито від імені Державної служби України з надзвичайних ситуацій із порадами щодо того, як ідентифікувати дрон-камікадзе, намагаючись скористатися страхом перед використанням росією дронів-камікадзе іранського виробництва Shahed-136 для завдавання ударів по критичній енергетичній інфраструктурі в Україні.

КІБЕРШПИГУНСЬКА ГРУПА CLOUD ATLAS АТАКУЄ РОСІЮ ТА ЇЇ ПРИХИЛЬНИКІВ

Згідно зі звітом компанії Check Point Research, оприлюдненим 9 грудня, з моменту виявлення у 2014 році, кібершпигунська група Cloud Atlas (або Inception) здійснювала численні атаки на критичну інфраструктуру в різних географічних зонах і політичних конфліктах. Тактика, техніка та процедури групи протягом багатьох років залишалися відносно незмінними.

Однак після стрімкої ескалації конфлікту між Росією та Україною у 2021 році та особливо після початку війни в лютому 2022 року масштаби діяльності групи значно звузилися, і її чітким фокусом стали росія, Білорусь та конфліктні регіони в Україні та Молдові. У звіті, опублікованому компанією, серед іншого, описано і новий інструмент, яким користується Cloud Atlas.

РОСІЙСЬКІ ХАКЕРИ АТАКУЮТЬ ШЛЯХИ НАДХОДЖЕННЯ ВІЙСЬКОВОЇ ДОПОМОГИ УКРАЇНІ

російські хакери намагаються завадити постачанню військової допомоги в Україну, а також здійснюють атаки на Польщу, куди часто надходить допомога від західних країн. Ці хакери є учасниками ширшої кампанії кібератак, пов'язаних з росією, що відбувається до та після вторгнення рф в Україну.

Вона містить у собі зусилля, спрямовані на руйнування енергетичної інфраструктури України в зимові місяці. «Безумовно, існує інтерес до постачання летальної зброї, які надходять до регіону від союзників України», — сказав журналістам Роб Джойс, директор відділу кібербезпеки АНБ.
«Ми бачимо розвідувальну діяльність у цьому напрямку, безумовно, зростання кількості нападів у Польщі, враховуючи характер постачання, які також надходять звідти».

Коментарі Джойса з'явилися після того, як у листопаді Microsoft заявила, що пов'язані з російським урядом хакери стоять за атаками програм-вимагачів на групи в Україні та Польщі, які займаються наданням військової та гуманітарної допомоги Україні.

НАФТОПЕРЕРОБНИЙ ЗАВОД КРАЇНИ-ЧЛЕНА НАТО СТАВ МІШЕННЮ РОСІЙСЬКОЇ APT В РАМКАХ КАМПАНІЇ ПРОТИ УКРАЇНИ

20 грудня Unit 42 фірми Palo Alto Networks повідомила, що було помічено нові тактики з боку APT групи Trident Ursa (також відомої як Gamaredon, Primitive Bear, Shuckworm і UAC-0010), за якою компанія спостерігає протягом останніх 10 місяців. Серед них фізичні погрози українському досліднику з кібербезпеки та невдала спроба проникнути на нафтопереробний завод у країні-члені НАТО в серпні цього року. Unit 42 також наголошує, що діяльність Trident Ursa відбувається в рамках підтримуваної російською державою кампанії проти України.

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ВІЙСЬКОВИХ ОПЕРАЦІЙ В УКРАЇНІ ЗАЗНАЛО АТАКИ РОСІЙСЬКИХ ХАКЕРІВ

18 грудня CERT-UA повідомила, що хакери атакували програмне забезпечення DELTA, критичне для українських військових операцій, за допомогою зловмисного програмного забезпечення для крадіжки інформації. Зловмисники в середині грудня скористалися зламаною електронною адресою співробітника Міноборони України для розсилки повідомлення користувачам програми, яке містило додаток зі зловмисними файлами.

РОСІЙСЬКІ ХАКЕРИ АТАКУЮТЬ АМЕРИКАНСЬКУ КОМПАНІЮ-ПОСТАЧАЛЬНИКА ЗБРОЇ ТА ОБЛАДНАННЯ

Дослідники пов'язали спонсоровану державою хакерську групу, що має відношення до росії, з інфраструктурою атаки, яка підробляє сторінку входу в Microsoft Global Ordnance законного військового постачальника зброї та обладнання, що базується в США. Recorded Future приписує нову інфраструктуру групі загроз, яку вона відстежує під назвою TAG-53 і широко відома кібербезпековій спільноті як Blue Callisto, Callisto, COLDRIVER, SEABORGIUM і TA446.

9. РІЗНЕ

КИТАЙСЬКА ІНДУСТРІЯ ЧІПІВ БОРЕТЬСЯ ЗА ТЕ, ЩОБ ВИЖИТИ НА ТЛІ ТЕХНОЛОГІЧНИХ ОБМЕЖЕНЬ США

Видання Nikkey Asia розповідає про те, як на тлі американських санкцій, спрямованих проти китайської техіндустрії, компанія Huawei лідирує в прихованому створенні внутрішнього ланцюга постачання напівпровідників.

ПРОВІДНА ТАЙВАНСЬКА ФІРМА З ВИРОБНИЦТВА ЧІПІВ БІЛЬШЕ НІЖ УТРИЧІ ЗБІЛЬШИТЬ ІНВЕСТИЦІЇ В США

Як 6 грудня повідомив виданню Nikkei офіційний представник Білого дому, Taiwan Semiconductor Manufacturing Company побудує перший завод у Сполучених Штатах з виробництва тринанометрових комп'ютерних мікросхем, які є найдосконалішими із доступних. Компанія планує потроїти інвестиції в чіпи, які будуть вироблятись на території США, до 40 мільярдів доларів для обслуговування Apple та інших компаній. Вона вже будує фабрику вартістю 12 мільярдів доларів у штаті Арізона.

ЯПОНІЯ ТА НІДЕРЛАНДИ ПОГОДИЛИСЯ НАСЛІДУВАТИ ПОЛІТИКУ США ЩОДО НАКЛАДЕННЯ ОБМЕЖЕНЬ НА КИТАЙ У ГАЛУЗІ НАПІВПРОВІДНИКІВ

13 грудня Japan Times повідомила, що Японія та Нідерланди погодилися запровадити обмеження на напівпровідники, які США раніше запровадили проти Пекіна. Це рішення стало перемогою для американських політиків, які прагнуть уповільнити впровадження Китаєм передових технологій. США звернулися до Токіо та Гааги, оскільки в цих країнах знаходяться Tokyo Electron та ASML, які є провідними компаніями, здатними виробляти обладнання для вироблення найсучасніших чіпів, що зараз є на ринку.

США ВНЕСЛИ 36 КОМПАНІЙ ДО ЧОРНОГО СПИСКУ

16 грудня Міністерство торгівлі США внесло 36 компаній до списку підсанкційних організацій за їх підтримку китайської армії та порушень прав людини в Китаї. Усі згадані компанії, крім однієї, мають штаб-квартири в Китаї. Тепер вони не матимуть доступу до американських технологій, і не зможуть продовжувати свою роботу, включаючи дослідження, розробку та виробництво чіпів штучного інтелекту.

Найбільш помітним доповненням до чорного списку є китайський виробник мікросхем Yangtze Memory Technologies, відомий як YMTC. Ця компанія, серед іншого, вже потрапляла в коло уваги високопоставлених американських законодавців за порушення експортного контролю через продажі на користь китайського телекомунікаційного гіганта Huawei та ймовірні зв'язки з китайською армією.

«YMTC становить безпосередню загрозу нашій національній безпеці, тому адміністрація Байдена мала діяти швидко, щоб не дати YMTC отримати хоча б на дюйм військової чи економічної переваги», – заявив лідер більшості в Сенаті Чак Шумер.

ТЕХНІЧНІ ЗАХОДИ БАЙДЕНА ПРОТИ КИТАЮ ЗАЛИШАЮТЬ СІ НЕБАГАТО СПОСОБІВ ВІДПОВІСТИ

У відповідь на обмеження, запроваджені адміністрацією Байдена, Китай звинуватив США в протекціонізмі, подав скаргу до Світової організації торгівлі та звернувся до виробника мікросхем Південної Кореї, ключового союзника США. Також повідомляється, що Пекін готує багатомільярдний пакет допомоги своїй напівпровідниковій промисловості.

Подібно до дій Пекіна під час торговельної війни з адміністрацією колишнього президента Трампа, коли Пекін не зміг виконати погрози додати американські компанії до так званого списку ненадійних організацій, будь-які дії щодо блокування американських інвестицій загрожують економіці, яка вже і так важко переживає наслідки політики президента Сі Цзіньпіна щодо нульової толерантності до COVID-19, яка лише щойно була скасована.

GOOGLE, ORACLE, AMAZON І MICROSOFT УКЛАЛИ УГОДУ З ПЕНТАГОНОМ ЩОДО ХМАРНИХ ПОСЛУГ НА СУМУ ДО 9 МІЛЬЯРДІВ ДОЛАРІВ

7 грудня CNBC повідомила, що Amazon, Google, Microsoft і Oracle спільно отримали від Пентагону контракт на хмарні обчислення на суму до 9 мільярдів доларів до 2028 року.

Контракт, який є результатом програми Joint Warfighting Cloud Capability, ілюструє намагання Міністерства оборони користуватися послугами декількох компаній, які надають послуги у галузі технологій дистанційної інфраструктури. Саме на такій стратегії наполягала адміністрація Трампа.

Така перемога є дивною для Oracle, яку аналітики не вважають найкращою компанією, що надає послуги хмарних обчислень. За останній квартал компанія отримала лише 900 мільйонів доларів доходу від хмарної інфраструктури в той час, як Amazon отримала 20,5 мільярдів доларів.

МІНІСТРИ ІННОВАЦІЙ КРАЇН ЄС УХВАЛИЛИ СТРАТЕГІЮ ЩОДО «ГЛИБОКИХ ТЕХНОЛОГІЙ»

Другого грудня міністри країн ЄС з питань інновацій схвалили порядок денний стратегії щодо «глибоких технологій», згідно з якою ЄС хоче уникнути відтворення часто ворожої динаміки, яка існує між ЄС та американськими технологічними гігантами, що виникли за нинішньої ери інновацій.

Термін deep tech (глибокі технології) – це позначення стартап-компаній, мета яких полягає в створенні технологічних рішень, базованих на серйозних наукових або інженерних розробках. Вони беруться дати відповідь на виклики, що вимагають тривалих досліджень і розробок, а також великих капіталовкладень до того, як їх буде успішно комерціалізовано.

СЕНАТ США УХВАЛИВ ЗАКОНОПРОЄКТ ПРО ЗАБОРОНУ TIKTOK НА ФЕДЕРАЛЬНИХ ПРИСТРОЯХ

Законопроєкт про заборону використання або завантаження TikTok на будь-якому федеральному пристрої був ухвалений Сенатом одноголосно 14 грудня. Зареєстрований у квітні 2021 року законопроєкт вимагає від уряду розробити стандарти та інструкції для державних органів щодо видалення програми з державних пристроїв. Виняток становлять правоохоронні органи, органи національної безпеки та дослідники. Але до кінця року він має пройти Палату представників, щоб потрапити на підпис до президента Байдена.

ЦЕНТРАЛЬНА ТА РЕГІОНАЛЬНА ВЛАДА США ЗАПРОВАДЖУЄ ЗАБОРОНУ ВИКОРИСТАННЯ TIKTOK НА УРЯДОВИХ ПРИСТРОЯХ

10 грудня штат Техас став п'ятим штатом США, який заборонив встановлювати додаток TikTok на державних пристроях через побоювання, що він збирає конфіденційні дані з пристроїв користувачів і, вірогідно, надає їх китайському уряду. Міністерство оборони США, Державний департамент та Міністерство внутрішньої безпеки США також заборонили використання TikTok на державних пристроях. На додачу до TikTok штат Меріленд також заборонив продукти Huawei Technologies, ZTE Corp., Tencent Holdings, включаючи WeChat, Alibaba та Kaspersky.

Керівництво TikTok запевняє, компанія не працює в Китаї, і додаток там недоступний. Хоча у TikTok дійсно є співробітники в Китаї, компанія суворо контролює, до яких даних ці співробітники мають доступ і де TikTok зберігає дані, запевнила операційна директорка TikTok Ванесса Паппас.

Раніше цього року компанія також оголосила, що запустила ініціативу під назвою «Проєкт Техас», покликану зміцнити довіру до гарантій, які компанія запровадила та запровадить для захисту даних користувачів США та інтересів національної безпеки. TikTok тепер зберігає 100% даних користувачів США в США в хмарному середовищі Oracle і працює з Oracle над впровадженням розширених засобів контролю безпеки даних, заявив генеральний директор TikTok Шоу Цзи Чу.