НКЦК

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

CYBER DIGEST

Огляд ключових подій у світі
кібербезпеки за листопад 2022 року

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

Зміни воєнно-політичної ситуації внаслідок російсько-української війни все активніше змушують країни та міжнародні організації змінювати та переосмислювати свою кіберполітику. ЄС вперше розробив власну політику кіберзахисту (як частину ширшої політики безпеки і оборони ЄС). Міністр внутрішніх справ Німеччини закликав до зміни архітектури системи безпеки держави для більш ефективної відповіді на нові загрози. А країни-члени НАТО створюють нові підрозділи швидкого реагування на інциденти у кіберпросторі. Ці кроки є лише першими наслідками російського вторгнення в Україну та активізації російських хакерських угрупувань на міжнародній арені (що містить в собі атаки проти сайту Європарламенту чи урядових сайтів східноєвропейських країн).

Набувають поширення наступальні операції у кіберпросторі. Так, Австралія у відповідь на хакерські атаки на її банківську систему, запровадила оперативну групу для боротьби з хакерами. Її завданням є пошук хакерів та їх нейтралізація ще до моменту здійснення ними атак. Про проведення таких операцій в кіберпросторі заявив і Директор ФБР Крістофер Рей, який наголосив, що стримування державних акторів у кіберпросторі є складнішим, ніж просто зрив їх операцій. Очікується, що Президент Байден не зменшить доволі широкі повноваження у цій царині, надані Міністерству оборони США адміністрацією Трампа.

Віруси-вимагачі продовжують становити головний виклик для органів державної влади центрального та регіонального рівня, а також для бізнесу. Значну увагу цьому питанню приділяє уряд Великої Британії. Уряд острова Вануату зазнав нищівної атаки, яка вивела з ладу його цифрову інфраструктуру на 11 днів. Повідомляють і про збільшення ransomware-атак на Україну з боку угрупування Sandworm, пов'язаного з ГРУ. На міжнародному рівні відбувся саміт з питань протидії ransomware. Казначейство США повідомило, що у 2021 році фінансові установи зазнали збитків від програм-вимагачів на 1,2 мільярда доларів. Це призводить і до посилення двосторонньої співпраці з цих питань (наприклад – нова угода про співробітництво між американськими та іспанськими безпековими органами з цього питання).

Координація міжнародних зусиль у реагуванні на масштабні кіберінциденти залишається важливим елементом міжнародної співпраці. За останній місяць відбулись кібернавчання CYBER FLAG23 (США), а за підтримки ENISA пройшли навчання Blue OLEx. Про важливість таких навчань свідчить той факт, що Японія повноцінно приєдналась до Центру передового досвіду кіберзахисту НАТО (CCDCOE) в т.ч. через бажання активніше долучатись до міжнародних навчань Locked Shields, які організовує зазначена установа.

Критична інфраструктура залишається у фокусі уваги злочинців. Хоча найпомітнішим інцидентом звітного періоду стала атака проти данської залізниці, яка частково призупинила її функціонування, однак справжніми довгостроковими загрозами залишаються віруси-вимагачі та атаки через ланцюжки постачання (при тому, що європейські постачальники основних послуг цього року знизили видатки на власну кібербезпеку). Найбільше занепокоєння викликає той факт, що все частіше атаки вимагачів спрямовані на операційно-технологічні складові об'єктів критичної інфраструктури, а однією з найбільш привабливих цілей є термінали інженерів підприємств. Все це змушує безпекові органи активніше шукати шляхи запобігання таким загрозам. Сюди відноситься посилення вимог щодо використання MFA, нові інструкції щодо більшої безпеки ланцюжків постачання (і навіть додатковий акцент на ролі споживачів в цьому питанні), оновлення стандартів кібербезпеки для критичних секторів, а також вжиття заходів щодо поліпшення інформування уповноважених органів про такі інциденти.

Міжнародна спільнота та безпекові агенції продовжують робити висновки з російсько-української кібервійни та оптимізувати свою політику захисту. Хоча українські безпекові структури вказують на те, що російські кібератаки переважно опортуністичні та неефективні (через нездатність координувати свої дії), російські хакерські групи активізують свою діяльність за кордоном (зокрема проти OKI у країнах НАТО). Техніки цих атак переважно традиційні – DDoS та ransomware (наприклад, операція Prestige). Однак проти України застосовуються і нові тактики – змінюються вектори атак з основних систем на периферійні брандмауери, маршрутизатори та сервери електронної пошти.

Кібервійна прискорює і впровадження нових практик кібербезпеки. Разом з оприлюдненням нової політики кіберзахисту ЄС, Пентагон проголосив про перехід до повного впровадження політики «нульової довіри» до 2027 року. Також США проводить переоцінку навіть звичних для всіх підходів до загроз цифровій інфраструктурі. Так, поряд з суто кіберзагрозами, все актуальнішими стають оцінки ризиків фізичного знищення цифрової інфраструктури. Ця інформація вже зараз надає країнам-партнерам можливості напрацювання механізмів кіберзахисту в умовах повномасштабної війни. Так само проходить переоцінка важливості глибшої горизонтальної співпраці між кіберфахівцями – не просто обмін досвідом під час разових акцій, але й залучення їх до спільних операцій чи завдань.

На тлі розвитку технологій та посилення конкуренції в технологічній сфері, Європейський Союз розбудовує свої цифрові спроможності. ЄС намагається з одного боку, убезпечити себе від загроз ланцюжкам постачання (European Chips Act), а з іншого – набути ваги у сфері технологій на противагу конкурентам із США та Китаю. Федеральні агенції США запроваджують директиви з метою пом'якшити ризики від запровадження технологій, які ще знаходяться у стадії розвитку, включаючи інтернет речей та квантові обчислення.

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

АВСТРАЛІЯ СТВОРИЛА ОПЕРАТИВНУ ГРУПУ ДЛЯ ПРОАКТИВНОЇ БОРОТЬБИ З ХАКЕРАМИ

12 листопада Міністерка внутрішніх справ Австралії Клер О'Ніл у відповідь на кібератаки на банківську систему (включаючи Medibank and Optus) оголосила про формування постійної оперативної групи, «яка буде щоденно полювати на покидьків, відповідальних за ці злісні злочини проти невинних людей».
Групу буде створено Федеральною поліцією Австралії у співпраці з Австралійським управлінням радіоелектронної розвідки (Australian Signals Directorate). Вона буде складатись зі 100 осіб і «буде не просто реагувати на злочини проти австралійців, переслідуватиме ці банди по всьому світу та перешкоджатиме діяльності цих людей».
Протягом наступних десяти років Уряд Австралії планує виділити на розвиток цього напрямку 6,3 млрд доларів США.
Австралійська влада вважає, що за атакою на Medibank стоїть добре організоване угруповання з росії. Неофіційні джерела в поліції повідомляють про синдикат, відомий як «REvil», який отримав свою назву від «ransomware evil».

БАЙДЕН МАЄ НАМІР ЗАТВЕРДИТИ ШИРОКІ ПОВНОВАЖЕННЯ ПЕНТАГОНУ ДЛЯ ПРОВЕДЕННЯ КІБЕРОПЕРАЦІЙ

17 листопада видання CyberScoop повідомило про те, що Міністерство оборони США здебільшого перемогло в тривалій бюрократичній боротьбі з Державним департаментом щодо збереження широких повноважень у галузі наступальних кібероперацій. Хоча точні відомості стосовно того, які саме повноваження Пентагон збереже, засекречені, обізнані джерела повідомили, що йому вдалося відстояти ключові частини широких повноважень, наданих Міністерству оборони адміністрацією Трампа у 2018 році.
Державному департаменту вдалось отримати деякі поступки. Остаточна версія меморандуму про політику включатиме положення, згідно з якими Білий дім має отримувати деталі планів кібероперацій від Міністерства оборони задовго до їх початку. Нова політика також дозволить агентствам позначати операції за допомогою «задокументованого процесу вирішення суперечок».
Тепер Президент Байден розгляне ці повноваження в рамках нещодавно переглянутої версії Меморандуму про політику національної безпеки-13 (National Security Policy Memorandum-13). Очікується, що Байден підпише документ.

ЄС РОЗРОБИВ ПОЛІТИКУ КІБЕРЗАХИСТУ

10 листопада ЄС презентував свою політику кіберзахисту як відповідь на зростаючі геополітичні виклики породжені російсько-українською війною. Політика буде зосереджена на декількох базових напрямках:

- розвиток спроможностей (включаючи збільшення інвестицій та нарощування підготовки фахівців з потрібними навичками);
- співпраця (між військовими, приватними структурами, кіберком'юніті та з міжнародними партнерами);
- готовність до відповіді (розвиток мережі SOC як «Кіберщита» ЄС);
- технології подвійного призначення (поліпшення ефективності використання тих IT-рішень, які можуть бути використані за принципом технологій подвійного призначення);
- міжнародна співпраця (розвиток точкового партнерства з країнами-однодумцями, а також проведення спільних навчань з НАТО).

ПАМ'ЯТКА ОФІСУ МЕНЕДЖМЕНТУ ТА БЮДЖЕТУ США ЩОДО ПЕРЕХОДУ НА ПОСТКВАНТОВЕ ШИФРУВАННЯ

18 листопада ЗМІ повідомили, що цивільні федеральні урядові установи США мають до травня 2023 року надати Агентству з кібербезпеки та безпеки інфраструктури (CISA) та Офісу національного кібердиректора список своїх систем, уразливих до криптографічно-відповідних квантових обчислень. Згідно з пам'яткою Офісу менеджменту та бюджету США, агентства повинні подати інформацію до 4 травня 2023 року та оновлювати список щорічно до 2035 року. Експерти говорять, що квантові обчислення ще далекі від здатності зламати поточні шифри, але збільшення розміру ключа в наявних шифрах може допомогти виграти додатковий час. Такі перехідні ініціативи доцільно розпочинати якомога раніше, задовго до виникнення реальної загрози.

ФЕДЕРАЛЬНІ АГЕНТСТВА США МАЮТЬ ВПРОВАДИТИ ІНСТРУКЦІЇ З КІБЕРБЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ (IOT)

До початку грудня, федеральні агентства США будуть зобов'язані запровадити інструкції з кібербезпеки Інтернету речей (IoT), розроблені Національним інститутом стандартів і технологій (NIST). Закон про кібербезпеку Інтернету речей від 2020 року (The IoT Cybersecurity Improvement Act of 2020) зобов'язав NIST розробити низку документів для задоволення потреб федеральних агентств, які прагнуть застосовувати пристрої IoT у своїх системах. Відповідні інструкції знаходяться на сайті Інституту у розділі SP 800-213 Series.

ОФІС ІНФОРМАЦІЙНОГО КОМІСАРА ВЕЛИКОБРИТАНІЇ ОПРИЛЮДНИВ РЕКОМЕНДАЦІЇ ЩОДО ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА ПЕРСОНАЛЬНИХ ДАНИХ

18 листопада Офіс інформаційного комісара (ICO) Великобританії оприлюднив рекомендації для регуляторів в різних сферах Як використовувати ШІ та персональні дані належним чином і законно. Мета документа – допомогти іншим регуляторам в ситуаціях, коли їм потрібно оцінити використання ШІ в секторах, які вони регулюють. Документ також допоможе регуляторним органам, які використовують ШІ для виконання своїх повноважень, робити це належним чином і законно.

БІЛЬШІСТЬ ЗАСІДАНЬ БРИТАНСЬКОГО УРЯДУ ЩОДО ВРЕГУЛЮВАННЯ КРИЗ ПРИСВЯЧЕНО ІНЦИДЕНТАМ З ПРОГРАМАМИ-ВИМАГАЧАМИ

18 листопада видання The Record повідомило, що на сьогодні інциденти, пов'язані з програмами-вимагачами (ransomware) мають настільки значні наслідки, що переважна більшість криз, на які змушений реагувати британський уряд, пов'язані саме з ними. Відповідно до щорічного огляду NCSC, Сполучене Королівство постраждало від 18 настільки серйозних інцидентів з ransomware цього року, що вони «вимагали узгодженої відповіді на національному рівні». Серед них атаки на компанію водопостачання Південного Стаффордшира та постачальника програмного забезпечення для Національної служби охорони здоров'я Advanced. Разом з тим, видання критикує увагу уряду та його дії щодо боротьби з програмами-вимагачами як неадекватні викликам.

БРИТАНСЬКИЙ УРЯД ЗАБОРОНЯЄ ВИКОРИСТОВУВАТИ КИТАЙСЬКІ КАМЕРИ СПОСТЕРЕЖЕННЯ В МІСЦЯХ З ОБМЕЖЕНИМ ДОСТУПОМ

25 листопада ЗМІ повідомили, що Британський уряд заборонив міністерствам встановлювати камери спостереження, виготовлені китайськими компаніями, у місцях з обмеженим доступом через можливі проблеми з інформаційною безпекою. Такі камери також не рекомендують під'єднувати до основних комп'ютерних систем. Уряд також отримує звернення із закликами повністю заборонити використання китайських камер спостереження в державному секторі. Основна причина – на більшість таких компаній поширюється дія Закону про національну розвідку Китайської Народної Республіки. Через це дані, що отримуються через ці камери, можуть потрапити до спеціальних служб КНР.

ФЕДЕРАЛЬНА КОМІСІЯ ЗВ'ЯЗКУ США ЗАБОРОНИЛА ПРОДАЖ ОБЛАДНАННЯ HUAWEI ТА ZTE У США З МІРКУВАНЬ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

25 листопада Федеральна комісія зі зв'язку США оголосила про прийняття нових правил, що забороняють продаж і імпорт у США нових телекомунікаційних пристроїв Huawei та ZTE з міркувань національної безпеки. Інші компанії, які потрапили під заборону, включають Hytera Communications, Hangzhou Hikvision Digital Technology і Dahua Technology. Рішення було прийнято одноголосно.
FCC повинна була прийняти відповідне рішення протягом року після прийняття Закону про безпечне обладнання, який президент Байден підписав 11 листопада 2021 року. Цей закон вимагав від FCC заборонити продаж обладнання, виробленого компаніями, які становлять «неприйнятний ризик для національної безпеки» США.

FTC ПОСИЛЮЄ ВИМОГИ ДЛЯ ПРИВАТНОГО СЕКТОРУ ЩОДО ВИКОРИСТАННЯ СТІЙКОГО ДО ФІШИНГУ MFA

Федеральна торгова комісія (FTC) США активно виступає за запровадженням учасникам ринку більш жорстких вимог безпеки для стійкого до фішингу MFA. Це стало результатом декількох масштабних витоків персональних даних користувачів з американських цифрових платформ. FTC орієнтується на рекомендації CISA щодо надійних методів MFA і вимагає їх впровадження для співробітників компаній.

ДО 2027 РОКУ ПЕНТАГОН ПЛАНУЄ ВПРОВАДИТИ ПОЛІТИКУ НУЛЬОВОЇ ДОВІРИ

22 листопада Пентагон оприлюднив Стратегію впровадження політики нульової довіри і відповідну Дорожню карту. У документах детально описано понад 100 заходів, необхідних для досягнення нульової довіри як нової парадигми кібербезпеки. Ці заходи поділені на сім ключових сфер: користувачі, девайси, застосунки, дані, мережі, автоматизація та оркестрація, а також аналітика. Це рішення є одним з наслідків вивчення уроків російсько-української війни.

МІНІСТР ВНУТРІШНІХ СПРАВ НІМЕЧЧИНИ ВИСТУПАЄ ЗА ПЕРЕГЛЯД АРХІТЕКТУРИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ФОНІ ЕСКАЛАЦІЇ МІЖНАРОДНОЇ СИТУАЦІЇ

Міністр внутрішніх справ Німеччини Ненсі Фезер заявила, що Німеччині необхідно переглянути не лише стратегію територіальної оборони, але й архітектуру національної безпеки: «Ми занадто довго почувалися в безпеці. Ось чому зараз ми повинні зробити все, що в наших силах, щоб компенсувати великі невдачі останніх років і десятиліть», – відмітила Н. Фезер. Це стосується більшої уваги до питань кібербезпеки, протидії дезінформації та захисту критичної інфраструктури. Вона також пропонує розширити повноваження та статус BSI – ключового федерального відомства у питаннях інформаційної та кібербезпеки.

CISA, NSA ТА ODNI ОПРИЛЮДНИЛИ ІНСТРУКЦІЇ ЩОДО БЕЗПЕКИ ЛАНЦЮЖКІВ ПОСТАЧАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

17 листопада CISA, Агентство національної безпеки (NSA) і Офіс директора національної розвідки (ODNI) опублікували третю частину рекомендацій щодо безпеки ланцюжків постачання програмного забезпечення, адресовану користувачам – Securing Software Supply Chain - Recommended Practices Guide for Customers. Ця публікація є останньою у серії після випуску інструкцій для розробників у серпні 2022 року та випуску інструкцій для постачальників у жовтні 2022 року.
Серія Securing Software Supply Chain є результатом Enduring Security Framework (ESF), державно-приватної міжгалузевої робочої групи під керівництвом NSA та CISA.

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

САМІТ З ПИТАНЬ ПРОГРАМ-ВИМАГАЧІВ

31 жовтня та першого листопада Білий дім зібрав представників 36 країн та Європейського Союзу на саміт з питань ransomware. Представники Counter Ransomware Initiative (міжурядове партнерство, створене Білим домом у жовтні минулого року) співпрацювали протягом останнього року у питаннях арештів учасників рансомвер атак, покращення захисту потенційних жертв, відстежування цифрових валют, які сприяють вимагачам, і тиску на держави, які не займаються питанням діяльності програм-вимагачів на своїй території. Мета саміту – обговорити результати та поділитися досвідом. На саміт також було запрошено представників 13 приватних компаній. росія, яка надає прихисток вимагачам, запрошення знову не отримала.
Наприкінці саміту учасники прийняли спільну заяву та factsheet. В рамках ініціативи буде створено добровільну міжнародну робочу групу з боротьби з програмами-вимагачами під керівництвом уряду Австралії. Її мета – сприяти обміну інформацією про загрози та відстеження фінансів угруповань програм-вимагачів. Члени ініціативи також кожні два роки проводитимуть навчання для посилення стійкості та стримування зловмисників. А також видаватимуть спільні рекомендації, які детально описують тактику, методи та процедури, які використовують кіберзлочинці. І створять «набір інструментів слідчого, який міститиме «засвоєні уроки та стратегії реагування на значні інциденти за участю програм-вимагачів».

НОВИЙ ГОЛОВА ВІДДІЛУ СТАНДАРТІВ МІЖНАРОДНОГО СОЮЗУ ТЕЛЕКОМУНІКАЦІЙ ПРО СВОЇ ПРІОРИТЕТИ

Наприкінці вересня колишній очільник японської NTT Docomo Сізо Оное був обраний головою відділу стандартів Міжнародного союзу телекомунікацій (ITU). Він розпочне виконувати обов'язки у наступному році.
Щодо геополітичної конкуренції між заходом та РФ з Китаєм, Сізо Оное вважає, що ITU повинен говорити з суто технічної точки зору. «Я заохочуватиму відкритість і інклюзивність», – сказав він. На його думку, прийняття рішень консенсусом не дозволяє ITU бути достатньо гнучким, тому важливою є співпраця з іншими організаціями, які працюють швидше та розробляють складніші стандарти завдяки ухваленню рішень більшістю голосів. Мета такої співпраці – прийняття розроблених ними стандартів на рівні ITU через систему голосування кожною країною в індивідуальному порядку. Такий підхід надаватиме перевагу західному погляду на рівень свободи інтернету від державного втручання.

США РОЗВИВАЄ СПІВПРАЦЮ З ІСПАНІЄЮ ЩОДО ПРОТИДІЇ RANSOMWARE

10 листопада CISA за підтримки Держдепартаменту США анонсувало спільний проєкт з Міністерством внутрішніх справ Іспанії щодо розвитку інструменту державно-приватного партнерства для протидії ransomware (програми-вимагачі). Цей проєкт є результатом Другого саміту міжнародної ініціативи щодо протидії ransomware започаткованої в Вашингтоні. Інструмент передбачає опис низки типових прикладів державно-приватного партнерства, які можуть бути поширені в інших країнах для протидії програмам-вимагачам.

КРАЇНИ-ЧЛЕНИ НАТО ЗОБОВ'ЯЗАЛИСЯ СТВОРИТИ ДОБРОВІЛЬНУ ГРУПУ ШВИДКОГО РЕАГУВАННЯ У КІБЕРПРОСТОРІ

9-10 листопада 2022 року в Римі відбулась конференція НАТО щодо кіберзахисту 2022. Конференція була присвячена темам стійкості, готовності та реагуванні на кіберзагрози критичній інфраструктурі. Вона проходила у закритому форматі, в YouTube транслювали лише звернення представників Італії, США та НАТО, які виступили її співорганізаторами. За результатами конференції Країни НАТО зобов'язалися створити добровільну групу швидкого реагування на «значну зловмисну кіберактивність».

250 КІБЕРСПЕЦІАЛІСТІВ ІЗ ВОСЬМИ КРАЇН ВЗЯЛИ УЧАСТЬ У CYBER FLAG 23 – CYBERCOM

4 листопада CYBERCOM США підбили підсумки тактичних кібернавчань CYBER FLAG 23, які проходили 17-28 жовтня у штаті Вірджинія. CYBER FLAG – це щорічні оборонні кібернавчання CYBERCOM, які забезпечують реалістичні навчання проти дій умовних зловмисників у віртуальному навчальному середовищі. Для цього використовується Національний кіберполігон NCR TRMC Центру управління тестовими ресурсами. Тема CF23-1 – події на Азійсько-тихоокеанському театрі дій.

ЄВРОПЕЙСЬКИЙ СОЮЗ ТРЕНУЄТЬСЯ РЕАГУВАТИ НА КІБЕРІНЦИДЕНТИ ЗАГАЛЬНОЄВРОПЕЙСЬКОГО МАСШТАБУ

7 листопада відбулись четверті навчання Blue OLEx, організовані Міністерством оборони Литви (MoND) разом з Агентством Європейського Союзу з кібербезпеки (ENISA). У навчаннях взяли участь представники 25 країн-членів, а також представники Єврокомісії. Темою цьогорічних навчань стала перевірка стандартних операційних процедур Європейської мережі організацій контактних офісів зв'язку з кіберкриз (EU Cyber Crisis Liaison Organisation Network Executives (CyCLONe).
EU CyCLONe був запущений у 2021 році для підтримки скоординованого управління великомасштабними інцидентами та кризами кібербезпеки на оперативному рівні та для забезпечення регулярного обміну інформацією між державами-членами та інститутами, органами та агентствами Європейського Союзу.

КРАЇНИ-ЧЛЕНИ НАТО МАЮТЬ ВКЛАДАТИ БІЛЬШЕ КОШТІВ У КІБЕРЗАХИСТ – ГЕНЕРАЛЬНИЙ СЕКРЕТАР НАТО ЙЕНС СТОЛТЕНБЕРГ

10 листопада 2022 року на конференції НАТО щодо кіберзахисту 2022 у Римі Генеральний секретар НАТО Йенс Столтенберг підкреслив, що для НАТО кіберзагрози (особливо на тлі триваючої російсько-української війни) продовжують залишатись важливим безпековим викликом. Він вважає, що хоч і після Варшавського саміту 2016 року країни-члени збільшили свої інвестиції у кіберзахист, але цього все ще не достатньо: «Я закликаю союзників знову взяти на себе зобов'язання щодо кіберзахисту. Більше грошей, більше досвіду та розширення співпраці. Це життєво важлива частина нашої колективної оборони», – зазначив він.

ЯПОНІЯ ОФІЦІЙНО ПРИЄДНАЛАСЯ ДО ЦЕНТРУ ПЕРЕДОВОГО ДОСВІДУ КІБЕРЗАХИСТУ НАТО

7 листопада стало відомо, що Міністерство оборони Японії (JMOD) оголосило про офіційне приєднання до Центру передового досвіду кіберзахисту НАТО (CCDCOE). Рішення про таке приєднання було оголошено ще у 2018 році. Основна мета – повноцінна участь у навчаннях Locked Shields (у 2021 та 2022 році представники Японії вже долучались до цих заходів).

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

ЗАСТОСУНКИ ДЛЯ ANDROID, ЯКІ МІЛЬЙОН РАЗІВ ВСТАНОВЛЕНІ З PLAY STORE, ПЕРЕНАПРАВЛЯЮТЬ КОРИСТУВАЧІВ НА ШКІДЛИВІ САЙТИ

За даними Malwarebytes, оприлюдненими 2 листопада, сімейство шкідливих програм від розробника Mobile apps Group, заражене Android/Trojan.HiddenAds.BTGTHB було розміщено в Google Play. Загалом воно складається з чотирьох застосунків, і разом вони зібрали щонайменше мільйон завантажень.
Ці застосунки направляють жертв на зловмисні вебсайти створені для отримання прибутку від реклами з оплатою за клік, які також спонукають їх встановлювати на свої телефони програми для очищування пам'яті з метою встановлення додаткових зловмисних програм. Ці шкідливі програми винайшли новий спосіб обійти захист Google Play Store. Одна з найпопулярніших тактик полягає в запровадженні затримок, які приховують зловмисну поведінку. Так ці додатки знаходилися в режимі очікування приблизно чотири дні, перш ніж відкрити перший фішинговий сайт у браузері Chrome.

КІБЕРАТАКА НА ОБСЕРВАТОРІЮ В ЧИЛІ ВИКЛИКАЛА ЗАНЕПОКОЄННЯ ЩОДО БЕЗПЕКИ КОСМІЧНИХ ТЕХНОЛОГІЙ

На початку листопада одна з найбільших у світі астрономічних обсерваторій Atacama Large Millimeter Array заявила, що у жовтні зазнала кібератаки і була змушена призупинити роботу. Кібератака вплинула на комп'ютерні системи обсерваторії та пошкодила публічну частину її вебсайту. Антени та наукові дані ALMA не були скомпрометовані, але вона припинила спостереження за космосом і обмежила використання електронної пошти.
І хоча зловмисники не завдали значної шкоди, сам факт атаки на космічні технології є серйозним інцидентом. Адже такі атаки завдають більш значної шкоди, а відновлення після них є значно складнішим та дорожчим. Дослідники очікують, що в майбутньому подібних атак буде ставати більше. Особливо, коли країни запускатимуть на орбіту підключені до мережі об'єкти, які зберігають конфіденційні дані або навіть ключову розвідувальну інформацію.

ROMCOM ВИКОРИСТОВУЄ ЗЛАМАНІ ВЕРСІЇ KEEPASS І SOLARWINDS ДЛЯ АТАК НА УКРАЇНУ ТА, МОЖЛИВО, СПОЛУЧЕНЕ КОРОЛІВСТВО

2 листопада група BlackBerry Threat Research and Intelligence Team оприлюднила звіт, у якому стверджує, що зловмисник, відомий як RomCom, проводить серію нових атак. Команда BlackBerry виявила, що RomCom імітує такі продукти як SolarWinds Network Performance Monitor, KeePass Open-Source Password Manager і PDF Reader Pro, щоб встановити RomComRAT. Він дозволяє забезпечити віддалений контроль над комп'ютером жертви. Оскільки основною мішенню зловмисників є Україна, та, можливо, Великобританія, враховуючи геополітичну ситуацію, дослідники вважають, що зловмисник керується не злочинними, а політичними мотивами.
Детальний опис атак можна знайти у звіті компанії.

КІБЕРЗЛОЧИННИЙ КАРТЕЛЬ FIN7 ПОВ'ЯЗАЛИ З ВИМАГАЧАМИ BLACK BASTA

4 листопада дослідники фірми SentinelOne заявили, що вони пов'язали давно відомий кіберзлочинний картель FIN7 з програмою-вимагачем Black Basta, яка стоїть за багатьма резонансними атаками, здійсненими між квітнем та вереснем цього року, включаючи атаки на Американську стоматологічну асоціацію та німецького оператора вітрових електростанцій Deutsche Windtechnik. Дослідники виявили, що у кількох випадках за участі Black Basta зловмисники використовували інструмент зламу кіберзахисту, розроблений FIN7.

РОСІЙСЬКЕ УГРУПОВАННЯ KILLNET СПРОБУВАЛО ЗДІЙСНИТИ DDOS АТАКУ НА МІНІСТЕРСТВО ФІНАНСІВ США

На початку листопада агентство Reuters повідомило, що у вересні угрупування KillNet спробувало здійснити DDoS атаку на Міністерство фінансів США. Спроба була невдалою. МінФін описав атаку як «DDoS активність на досить низькому рівні, спрямовану проти вузлів критичної інфраструктури Казначейства».

МЕРЕЖА KILLNET АТАКУВАЛА УРЯДОВІ САЙТИ СХІДНОЄВРОПЕЙСЬКИХ КРАЇН, АЛЕ НЕ ЗМОГЛА УТРИМАТИ ЇХ ОФФЛАЙН

Протягом вихідних 5-6 листопада російська мережа Killnet здійснила DDoS атаки на вебсайти, що належать кільком спецслужбам країн колишнього Східного блоку, а саме Естонії, Польщі, Румунії, Болгарії та Молдови. Про це мережа повідомила у своєму Телеграм-каналі. Разом з тим, станом на понеділок, 7 листопада, після недовгого відключення, атаковані сайти функціонували у нормальному режимі.
Експерти з кібербезпеки продовжують наголошувати, що ЗМІ приділяють атакам Killnet надто багато уваги, адже вони не завдають якої небудь помітної шкоди своїм жертвам.

УРЯД ТИХООКЕАНСЬКОГО ОСТРОВА ВАНУАТУ ЗАЗНАВ НИЩІВНОЇ КІБЕРАТАКИ

Уряд Вануату протягом понад 11 днів був відключений від інтернету після ймовірної кібератаки на сервери країни. Атака, швидше за все, розпочалась 4 листопада та призвела до відключення від мережі вебсайтів парламенту, поліції та офісу прем'єр-міністра країни. Також постраждала система електронної пошти, інтернет і онлайн-бази даних шкіл, лікарень та інших екстрених служб, а також усіх державних служб і відомств. Уряд країни заледве міг виконувати навіть базові функції.
Поки що невідомо, хто стоїть за атакою, але ЗМІ повідомляють, що вона фінансово вмотивована. Австралійська The Sydney Morning Herald повідомила, що нападники вимагали викуп, який уряд Вануату відмовився заплатити.

УРЯДОВЦІ МОЛДОВИ ЗАЗНАЛИ КІБЕРАТАКИ

16 листопада у мережу потрапили приватні розмови міністра юстиції Молдови, радника президента з питань оборони та нацбезпеки та колишнього міністра внутрішніх справ. Деякі з розмов містять натяки, що певні молдовські посадовці нечесно здобули перемогу на виборах або неналежним чином отримали посади. Злиття розмов видається спрямованим і на дискредитацію антикорупційних чиновників. У Мін'юсті підтвердили факт витоку, але додали, що деякі повідомлення були сильно змінені або вирвані з контексту.
Проросійська політична опозиція Молдови швидко розповсюдила звинувачення та закликала до усунення вищезгаданих чиновників з посад. Представники уряду звинуватили росію в організації провокації.

IBM: RANSOMEXX СТАЛА ЩЕ ОДНІЄЮ ГРУПОЮ ПРОГРАМ-ВИМАГАЧІВ, ЯКА СТВОРИЛА ВАРІАНТ МОВОЮ RUST

Дослідники IBM Security X-Force 23 листопада повідомили, що оператори програми-вимагача RansomExx розробили новий варіант програми, повністю написаний мовою програмування Rust. Вони наслідували приклад інших виробників зловмисного програмного забезпечення, таких як BlackCat, Hive і Luna. Остання версія, названа RansomExx2, в основному призначена для використання в операційній системі Linux, хоча очікується, що буде випущено і версію для Windows. Експертка IBM Security X-Force Шарлотта Хаммонд, розповіла The Record, що це важливий тренд, оскільки показники виявлення антивірусними програмами, як правило, нижчі для зловмисного програмного забезпечення мовою Rust, що допомагає йому обходити захист.

PALO ALTO NETWORKS ВІДСЛІДКОВУЄ ФІШИНГОВУ КАМПАНІЮ ІЗ ЗАСТОСУВАННЯМИ ТЕЛЕФОННОГО ЗВ'ЯЗКУ LUNA MOTH

21 листопада Unit 42 компанії Palo Alto Networks повідомив, що відстежує кампанію з вимагання, яка здійснюється без шифрування та за допомогою телефонного зв'язку – Callback Phishing Attack. Такі атаки вимагають більших витрат ресурсів, але часто є успішнішими. Їх побудовано таким чином, що мішень атаки має вступити в прямий контакт зі зловмисниками. Компанія наголошує, що в процесі атаки зловмисники використовують законні інструменти, які вони підлаштовують під свої потреби.
Типова схема виглядає таким чином, що мішень атаки отримує фішинговий імейл, який містить повідомлення про необхідність сплатити певну суму за якісь послуги. Повідомлення також містить номер телефону, за яким мішень має зв'язатися з оператором. У процесі розмови оператор під виглядом допомоги у відмові від небажаних послуг, проводить жертву кроками, які призводять до встановлення у неї на комп'ютері зловмисного ПЗ, що дозволяє оператору мати віддалений доступ до комп'ютера жертви. Після цього зловмисник шукає цінну інформацію, дістає її з комп'ютера жертви, а потім направляє листа з вимаганням грошей та погрозами оприлюднити інформацію. Таким чином, як правило, здійснюють атаки проти організацій через їх співробітників.

РЕЙТЕРС ВИКРИЛА РОСІЙСЬКЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ЗАМАСКОВАНЕ ПІД АМЕРИКАНСЬКЕ

14 листопада інформаційна агенція Рейтерс опублікувала дослідження, в якому йдеться про те, що велика кількість застосунків в онлайн магазинах Apple (AAPL.O) та Google's (GOOGL.O) містять код, розроблений компанією Pushwoosh, яка називає себе американською, але насправді є російською. США підтвердили інформацію розслідувачів – ним скористалось щонайменше 1000 військовослужбовців (переважно з-поміж тих, хто проходив службу у Національному тренінговому центрі у Форті Ірвін).
Дізнавшись про російське коріння компанії Pushwoosh, Центр з контролю та профілактики захворювань США (CDC) видалив її програмне забезпечення із семи загальнодоступних застосунків, посилаючись на проблеми безпеки. Армія США заявила, що видалила застосунок, який містив код Pushwoosh, у березні через ті ж проблеми. Цим застосунком користувалися солдати на одній із головних баз бойової підготовки країни. Програмне забезпечення з кодом від Pushwoosh також використовували багато міжнародних організацій.
Компанія Pushwoosh надає підтримку в обробці коду та даних розробникам програмного забезпечення, дозволяючи їм відстежувати та класифікувати онлайн-активність користувачів мобільних застосунків і надсилати їм індивідуальні push-повідомлення з серверів Pushwoosh. Таким чином, вона збирає великі масиви даних, включаючи точну геолокацію. І хоча компанія заявляє про те, що вона не ділиться інформацією з росією, але законодавча база рф з цього питання змушує фахівців ставити ці заяви під сумнів.

БОТНЕТ EMOTET ЗНОВУ АКТИВІЗУВАВ СВОЮ ДІЯЛЬНІСТЬ – CISCO TALOS, PROOFPOINT
ДЖЕРЕЛО 2

8 листопада команда Cisco Talos повідомила, що ботнет Emotet (діяльність якого була сильно ускладнена після масованої кампанії 2021 року) знову відновлюється. Дослідники вказують на збільшення спаму, що розповсюджує новий тип загрози (з використання макросів Auto_Open у документах XLS). Як і раніше, вірус намагається використати інструменти соціальної інженерії аби обійти вимкнення макросів Microsoft які необхідні для його активації.
16 листопада Proofpoint повідомила низку додаткових деталей щодо повернення цієї ботмережі до діяльності. Вони визначили як керівника ботнету MUMMY SPIDER (TA542), який за деякими даними пов'язаний з російськими кримінальними організаціями. Кількість спаму, що продукується Emotet для свого поширення, становить сотні тисяч щодня. Основні цілі: США, Велика Британія, Японія, Німеччина, Італія, Франція, Іспанія, Мексика, Бразилія.
Видання Hacker News зібрало інформацію про цей ботнет у статті «Все, що вам необхідно знати про Emotet у 2022 році».

ІРАНСЬКЕ APT УГРУПУВАННЯ ВДАЛО АТАКУВАЛО ФЕДЕРАЛЬНЕ ВІДОМСТВО

17 листопада CISA та FBI у спільному прес-релізі повідомили про вдалу атаку іранського APT угрупування на мережу федерального відомства. Зловмисники використали відому вразливість Log4Shell у не оновленому сервері VMware Horizon. Наслідки атаки не повідомлялись.

APT EARTH PRETA ПРОВОДИТЬ ШИРОКОМАСШТАБНУ КАМПАНІЮ КІБЕРШПИГУНСТВА – АНАЛІТИКИ TREND MICRO

18 листопада фахівці безпекової компанії Trend Micro виклали розгорнутий розбір нової кампанії кібершпигунства (орієнтовний початок – березень 2022 року), яка проводиться APT Earth Preta (вона ж Mustang Panda, китайське хакерське угрупування) проти М'янми, Австралії, Філіппін, Японії та Тайваню. Мета кампанії поки не до кінця зрозуміла, але традиційно група проникає в цільові системи жертви, викрадає конфіденційні документи які можуть бути використані для проникнення під час наступних хвиль.

ПРОГРАМА-ВИМАГАЧ HIVE ОТРИМАЛА ПОНАД 100 МІЛЬЙОНІВ ДОЛАРІВ ВІД ПОНАД 1300 ЖЕРТВ

Згідно з новим спільним звітом кількох агенцій США, з червня 2021 року по листопад 2022 року група програм-вимагачів Hive, яку класифікують програмою-вимагачем як послугою (RaaS), отримала понад 100 мільйонів доларів, атакувавши понад 1300 компаній у всьому світі. Як правило, учасники Hive отримують початковий доступ до комп'ютера жертв через фішингові електронні листи зі шкідливими вкладеннями. Група використовувала різноманітні тактики під час своїх атак і продемонструвала здатність обходити багатофакторну автентифікацію.
Детальний опис можна знайти у звіті на сайті CISA.

4. ПРОГНОЗИ ТА ВИКЛИКИ

NIST ОПУБЛІКУВАВ ПРОЄКТ ДОКУМЕНТУ ЩОДО БЕЗПЕКИ СИСТЕМ ВОДОПОСТАЧАННЯ ТА ВОДОВІДВЕДЕННЯ «КІБЕРБЕЗПЕКА ДЛЯ СЕКТОРУ ВОДОПОСТАЧАННЯ ТА ВОДОВІДВЕДЕННЯ»

2 листопада Національний центр передового досвіду з кібербезпеки NIST оприлюднив для публічного обговорення проєкт документа щодо безпеки систем водопостачання та водовідведення «Кібербезпека для сектору водопостачання та водовідведення». Він зосереджений на виявлені кіберзагроз цій критичній інфраструктурі в чотирьох основних напрямках: управління активами, цілісність даних, віддалений доступ та мережева сегментація. Також документ пропонує низку рекомендацій (спираючись на NIST CSF) щодо мінімізації загроз у цих складових.

NIST ОПРИЛЮДНИВ ПРОЄКТ REV 2 «КЕРІВНИЦТВО З ВИМІРЮВАННЯ ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ» (SP 800-55)

14 листопада NIST оприлюднив для надання коментарів другу версію стандарту «Керівництво з вимірювання ефективності інформаційної безпеки» (SP 800-55) (перша версія була оприлюднена у 2008 році). NIST просить спеціалістів з кібербезпеки надати пріоритетні рекомендації з трьох питань: 1) можливі метрики вимірювання ефективності діяльності CIOs/CISOs; 2) як найкраще комунікувати потреби вимірювання ефективності інформаційної безпеки в межах організації; 3) які приклади метрик може включати ця оновлена публікація, щоб бути найбільш корисна у вашій діяльності.

MITRE ОПРИЛЮДНИВ НАСТАНОВИ ДЛЯ МЕДИЧНИХ ЗАКЛАДІВ ЩОДО ПІДВИЩЕННЯ ЇХНЬОЇ КІБЕРБЕЗПЕКИ

14 листопада корпорація MITRE оприлюднила настанови (Playbook) для медичних установ щодо підвищення їх готовності до реагування на кіберінциденти. Це вже друга версія настанов – перша була підготовлена у 2018 році. Настанови базуються на NIST SP 800-61r2 «Computer Security Incident Handling Guide» та надають практичні рекомендації щодо всіх стадій реагування на кіберінциденти (включаючи порядок інформування про них інші організації, а також поради щодо проведення навчань для персоналу).

КОМПАНІЯ PROOFPOINT ОПРИЛЮДНИЛА СВОЇ ПРОГНОЗИ ЩОДО КІБЕРБЕЗПЕКИ НА 2023 РІК

2 листопада кібербезпекова компанія Proofpoint оприлюднила свої прогнозні оцінки щодо трендів кібербезпеки у 2023 році. Виокремлено сім основних трендів:

- глобальна економічна криза та фінансова турбулентність може призвести до нових ризиків кібербезпеці організацій;
- подальша комерціалізація хакерських інструментів у dark web веде до збільшення кіберзлочинців;
- схеми «подвійного вимагання» стануть не виключенням, а постійною практикою;
- зросте кількість атак, спрямованих на обхід MFA;
- атаки через ланцюжки постачання залишаться важливою загрозою;
- кіберзлочинці будуть активніше використовувати технології Deepfake у своїй соціальній інженерії;
- тиск на CISO організацій з боку керівництва буде лише зростати.

MIT TECHNOLOGY REVIEW: ЩО БУДЕ ДАЛІ В КІБЕРБЕЗПЕЦІ

Згідно з публікацією MIT Technology Review від 28 листопада, тенденції, які спостерігалися цього року, триватимуть наступного року та найближчим часом. Серед них:

- хакерські атаки РФ, спрямовані проти України;
- збільшення кількості атак програм-вимагачів проти лікарень і шкіл, а також проти цілих урядів;
- дуже велика кількість дорогих криптозломів;
- гучні зломи таких компаній, як Microsoft, Nvidia та виробника Grand Theft Auto Rockstar Games.

АРМІЇ СОЮЗНИКІВ США ЗІШТОВХНУЛИСЬ З ПРОБЛЕМОЮ УПРАВЛІННЯ ДАНИМИ ТА МЕРЕЖУВАННЯ НА ПОЛІ БОЮ

Армія США та союзники завершують щорічний експеримент Project Convergence, який має на меті продемонструвати спільне командування та контроль у всіх доменах. Таким чином Міністерство оборони США бачить мережеві сили, пов'язані із підтримкою даних. Навчання проходили в жовтні-листопаді на заході США та в Тихому океані.
В процесі союзники дізналися, що керувати даними та мережувати зброю та підрозділи на полі бою набагато складніше, ніж вони думали. Міністр армії Кристін Вормут заявила журналістам, що хоче, щоб Офіс міністра оборони надав вказівки щодо стандартизації форматів даних. Інші учасники заявили, що було досягнуто прогресу в обміні даними, але кількість інформації, наданої учасникам, була настільки великою, що від неї не було користі.

ГЕНЕРАТИВНИЙ ШТУЧНИЙ ІНТЕЛЕКТ ТА ПИТАННЯ АВТОРСЬКОГО ПРАВА

21 листопада видання Wired повідомило про позов, поданий до федерального суду Каліфорнії, який може вплинути на майбутнє генеративного штучного інтелекту.
Генеративний штучний інтелект (ШІ) здатний створювати зв'язний текст, зображення та функціональний комп'ютерний код, вироблений алгоритмами, які тренуються на роботах, створених людьми. Останнім часом він зазнає значного розвитку. Але той факт, що у своєму навчанні він використовує роботи, раніше створені людьми, не згадуючи первинних творців, викликає все більше нарікань.
Позов, про який йдеться, стосується GitHub Copilot – потужного інструменту, який автоматично пише робочий код, коли програміст починає вводити текст. Програміст, який подав позов, стверджує, що GitHub порушує авторські права, оскільки не надає посилання на джерело, коли Copilot відтворює код з відкритим вихідним кодом з ліцензією, яка цього вимагає.

ЧЕРВОНИЙ ХРЕСТ ШУКАЄ ЦИФРОВИЙ ЕКВІВАЛЕНТ СВОЇХ ЕМБЛЕМ

Міжнародний Комітет Червоного Хреста (МКЧХ) хоче розробити цифровий еквівалент своїх емблем (червоного хреста та червоного півмісяця), щоб позначити певні цифрові ресурси як «захищені» та такі, що не можуть бути цілями під час кібервійни. Зараз розглядається три основні варіанти реалізації цієї ідеї: заснована на DNS (через спеціальну мітку у назві домену, наприклад «www.hospital.emblem», заснована на IP – виділенні спеціального діапазону IP адрес для захищених об'єктів; та ADEM (Authenticated Digital Emblem) – використання спеціальних сертифікатів, що визначають захищених суб'єктів.

ОПРИЛЮДНЕНО ПЕРШІ РЕЗУЛЬТАТИ РОЗСЛІДУВАННЯ ЩОДО ШПИГУНСЬКОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ТЕЛЕФОНАХ ОПОЗИЦІОНЕРІВ І ЖУРНАЛІСТІВ

8 листопада доповідачка Комітету з розслідування випадків використання Pegasus та подібних шпигунських програм (Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA)) Софі Ін’т Велд, представила перший драфт звіту за результатами розслідування.
Члени Комітету, сформованого Європейським парламентом в березні 2022 року, проводять розслідування серії скандалів у європейських країнах, серед яких Іспанія, Греція, Угорщина та Польща. Воно стосується використання урядами шпигунського програмного забезпечення, яке було знайдено в телефонах опозиціонерів і журналістів. Результати розслідування «приголомшливі, і вони повинні насторожити кожного європейського громадянина», – йдеться у проєкті звіту, представленого Ін’т Велд.

5. КРИТИЧНА ІНФРАСТРУКТУРА

ДАНСЬКА ЗАЛІЗНИЦЯ ТИМЧАСОВО ЗУПИНИЛАСЬ ЧЕРЕЗ КІБЕРАТАКУ

3 листопада стало відомо, що зупинка данської залізниці у попередні вихідні стала наслідком хакерської атаки. Представник данського залізничного оператора DSB заявив, що атаку було здійснено на підрядника компанії (Supeo) з кримінальною метою. Це стало результатом ransomware-атаки проти іншої данської компанії – Supeo, яка надає низку послуг операторам залізничних перевезень. Однією з них є підтримка мобільного застосунку, який надає операторам потягів доступ до критичної операційної інформації, такої як межі швидкості. Внаслідок кібератаки Supeo вирішив відключити сервери, що призвело до зупинки роботи застосунку, а це своєю чергою – до зупинки поїздів.

ПРОТИДІЯ АТАКАМ ЧЕРЕЗ ЛАНЦЮЖКИ ПОСТАВОК ЦЕ ВІДПОВІДАЛЬНІСТЬ НЕ ЛИШЕ РОЗРОБНИКА ПЗ, АЛЕ І СПОЖИВАЧА – NSA

17 листопада NSA спільно з CISA та державно-приватною робочою групою оприлюднили рекомендації «Безпека ланцюжків постачання ПЗ для користувачів», у яких надано рекомендації споживачам ПЗ щодо долучення до забезпечення безпеки всього ланцюжка постачання ПЗ. NSA вказує, що хоча основна відповідальність за безпеку продуктів продовжує залишатись за їх розробниками, але складність загроз вимагає і від споживачів більшої уваги та відповідальності за користування ПЗ. Своєю чергою розробники мають надавати споживачам всю необхідну інформацію та допомогу щодо перевірки цілісності програмних продуктів.

ЄВРОПЕЙСЬКІ ОПЕРАТОРИ КРИТИЧНИХ ПОСЛУГ СТАЛИ МЕНШЕ ВКЛАДАТИ В КІБЕРБЕЗПЕКУ – ДОСЛІДЖЕННЯ ENISA

23 листопада ENISA оприлюднила результати свого дослідження 1000 операторів критичних послуг з 27 країн-членів ЄС. Мета дослідження – перевірити стан інвестицій в мережеву та інформаційну безпеку в ЄС, а також як на ці видатки вплинуло прийняття Директиви NIS. Акцент у досліджені було зроблено на сектори енергетики та охорони здоров'я. Основний результат – у 2022 році видатки на інформаційну безпеку зменшились з 7,7% до 6,7% у порівнянні з минулим роком.
Серед ключових показників:

- великі оператори в середньому інвестують 120 000 євро в систему розвідки кіберзагроз (CTI) у порівнянні з 5 500 євро малих і середніх підприємств;
- сектори охорони здоров'я та банківський сектор несуть найбільші витрати серед критичних секторів у разі серйозних інцидентів кібербезпеки. Середня пряма вартість інциденту в цих секторах становить 300 000 євро;
- 37% операторів основних послуг і постачальників цифрових послуг не використовують SOC;
- лише 5% МСП вдаються до кіберстрахування.

CISA ПУБЛІКУЄ РЕКОМЕНДАЦІЇ ДЛЯ МАЛИХ ОРГАНІЗАЦІЙ ЩОДО ЕФЕКТИВНОГО УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ

14 листопада виконавчий помічник директора з кібербезпеки CISA Ерік Голдштейн оприлюднив пропозиції CISA як краще побудувати відповідну екосистему у своїй організації для компаній, які не мають досвіду з управління вразливостями. Ці рекомендації стосуються впровадження трьох елементів:

- запровадження більшої автоматизації в управлінні вразливостями (зокрема шляхом розширення використання Common Security Advisory Framework, CSAF);
- широкому застосуванню Vulnerability Exploitability eXchange (VEX);
- ефективнішому визначенню пріоритетності ресурсів для керування вразливостями за допомогою Stakeholder Specific Vulnerability Categorization (SSVC), включаючи визначення пріоритетності вразливостей у каталозі CISA's Known Exploited Vulnerabilities (KEV).

NSA ВИПУСТИЛА РЕКОМЕНДАЦІЇ ДЛЯ РОЗРОБНИКІВ ЩОДО ЗАПОБІГАННЯ ПРОБЛЕМАМ З ВИКОРИСТАННЯ ПАМ'ЯТІ В ПЗ

10 листопада NSA оприлюднило набір рекомендацій для розробників ПЗ як уникнути найбільш типових помилок при програмуванні елементів, які стосуються доступу до пам'яті. Неправильне програмування цих блоків продовжує залишатись важливим джерелом загроз, яким користуються зловмисники. Це веде до технічних збоїв, а також порушень конфіденційності інформації. Рекомендації заохочують організації переходити від мов програмування, таких як C і C++, до безпечних для пам'яті альтернатив, а саме C#, Rust, Go, Java, Ruby або Swift.

ІНЖЕНЕРНІ РОБОЧІ СТАНЦІЇ Є БАЖАНОЮ МІШЕННЮ ДЛЯ ЗЛОВМИСНИКІВ, ЩО НАЦІЛЕНІ НА АТАКИ ПРОТИ ICS/OT – ДОСЛІДЖЕННЯ SANS

Інститут SANS на замовлення фірми з промислової кібербезпеки Nozomi Networks провів дослідження щодо кібербезпеки OT/ICS у 2022 році. Було опитано 332 особи з тих, що відповідають за проблеми кібербезпеки OT/ICS. Більша частина респондентів сказали, що вони впевнені, що зможуть виявити вторгнення протягом 24 годин. А понад дві третини вважають, що вони можуть перейти від виявлення до локалізації протягом 6-24 годин. 34,7% відзначили, що інженерні робочі станції є бажаною мішенню для зловмисників, що націлені на атаки проти ICS/OT. Найбільшою загрозою для ICS/OT продовжують залишатись програми-вимагачі.

МІНІСТЕРСТВО ВНУТРІШНЬОЇ БЕЗПЕКИ США ГОТУЄТЬСЯ ДО ЗМІНИ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ КРАЇНИ

Згідно з новим звітом, оприлюдненим 12 листопада, Міністерство внутрішньої безпеки США очікує серйозних змін складного, майже десятирічного підходу, який виконавча влада використовує для захисту критичної інфраструктури.
Звіт розкриває методологію віднесення до критичної інфраструктури, яка раніше не була публічною. Космос та біоекономіку додано до переліку секторів критичної інфраструктури. У звіті визначено, які федеральні органи матимуть наглядові повноваження над певними секторами. Також він містить рекомендацію розглянути можливі додаткові повноваження, добровільні регуляторні механізми та посилені стандарти, з метою зменшення ризиків.
Як повідомляє видання Politico, звіт уже отримав схвалення адміністрацією Байдена.
Тепер Білий дім повинен надати вказівки DHS, переписавши ще один ключовий документ виконавчої влади щодо захисту критичної інфраструктури, а саме Президентську директиву щодо політики 21 (Presidential Policy Directive 21).

РОСІЙСЬКІ ХАКЕРИ АТАКУВАЛИ ГОЛЛАНДСЬКИЙ ГАЗОВИЙ ТЕРМІНАЛ

25 листопада компанія з промислової кібербезпеки Dragos попередила, що угрупування Xenotime і Kamacite вірогідно займаються розвідкою терміналів зрідженого природного газу в Нідерландах. Ці два угруповання в минулому були пов'язані зі спробами ГРУ атакувати промислові об'єкти. Видання цитує слова Кейсі Брукса з Dragos: «Ми знаємо, що СПГ-термінали є мішенню. Питання лише в тому, коли і як». За словами Брукса, угрупування намагаються віднайти можливі вектори потенційної цифрової атаки. Дослідники помітили ознаки такої підготовки в системах СПГ-терміналу Gasunie в роттердамському порту Емсхафен.

ЕНЕРГЕТИЧНА ІНФРАСТРУКТУРА ЄВРОПИ СТАЛА МІШЕННЮ ДЛЯ РФ

25 листопада видання OilPrice.com повідомило, що фірма EclecticIQ, яка займається аналізом загроз і безпекою, помітила «підвищену активність» навколо критичної інфраструктури у Нідерландах та в Європі загалом. Джоеп Гоммерс з ELectricIQ сказав RTL, що російські хакерські атаки на голландські СПГ-термінали є логічними на сьогодні. «Це, безумовно, відповідає методам роботи та поточним цілям росії».

6. АНАЛІТИЧНІ ОЦІНКИ

ЩОРІЧНИЙ ЗВІТ НАЦІОНАЛЬНОГО ЦЕНТРУ КІБЕРБЕЗПЕКИ ВЕЛИКОБРИТАНІЇ ЗА 2022 РІК

1 листопада Британський Національний центр кібербезпеки оприлюднив шостий щорічний огляд своєї роботи за 2022 рік. В ньому йдеться про ключові події та основні моменти з 1 вересня 2021 року по 31 серпня 2022. Звіт розповідає про діяльність центру за чотирма напрямками, а саме загрози, ризики та вразливості; резилієнс; технології та екосистема. Звіт також містить прогнози британських фахівців щодо подальшого розвитку ситуації у цих сферах.
Серед низки питань вказується на проблему приховування жертвами ransomware фактів вдалих атак проти них. Серед причин – небажання повідомляти про недостатні практики кіберзахисту в організації, а також готовність заплатити викуп зловмисникам, що може бути не схвально сприйнято державними установами. Між тим за даними звіту лише за період з 1 вересня 2021 по 31 серпня 2022 року було зафіксовано 18 ransomware інцидентів, які потребували координації на національному рівні (зокрема, це атаки проти Національної служби здоров'я та компанії South Staffordshire Water).

THREAT LANDSCAPE 2022 ЗВІТ ВІД ENISA

3 листопада було опубліковано 10-е видання звіту Threat Landscape Агентства Європейського Союзу з кібербезпеки (ENISA) за рік – звітний період з липня 2021 року по липень 2022 року. Оскільки щомісяця викрадається понад 10 терабайтів даних, програми-вимагачі й надалі вважаються однією з головних загроз у звіті, а фішинг визначено як найпоширеніший початковий вектор таких атак. Іншими загрозами, які займають найвище місце серед програм-вимагачів, є атаки на доступність, які також називаються розподіленими атаками на відмову в обслуговуванні (DDoS).
Проте геополітична ситуація, зокрема російське вторгнення в Україну, за звітний період змінила правила глобальної кіберсфери. Хоча ми все ще спостерігаємо збільшення кількості загроз, ми також бачимо, що з'являється ширший спектр векторів, таких як експлойти нульового дня, дезінформація та глибокі фейки за допомогою ШІ. У результаті з'являються більш зловмисні та поширені атаки, які мають більш руйнівний вплив.

ДОСЛІДЖЕННЯ ДАНИХ XDR ВИЯВИЛО ТЕНДЕНЦІЇ У ПРОЯВАХ ЗАГРОЗ

2 листопада компанія Barracuda оприлюднила результати дослідження, щодо серйозності загроз у 2022 році, в якому йдеться про те, що більшість серйозних атак на організації відбуваються влітку, поки багато працівників знаходяться у відпустках. Було виявлено, що влітку почастішали зломи облікових записів Microsoft 365. 40% атак у період з червня по вересень 2022 року стосувалися входу в облікові записи Microsoft 365 із підозрілих країн. Barracuda класифікує ці атаки як атаки «з високим ризиком».

ЕКСПЕРТИ SANS ОПРИЛЮДНИЛИ П’ЯТЬ НАЙБНЕБЕЗПЕЧНІШИХ КІБЕРЗАГРОЗ

16 листопада SANS поділився основними тезами доповіді своїх співробітників на конференції RSA 2022. Цей виступ був присвячений найбільш небезпечним методам кібератак, з якими стикаються зараз користувачі всіх рівнів. Передусім це:

- хмарні середовища – зловмисники атакують такі сервіси аби отримати доступ до ресурсів користувачів;
- «обхід» MFA – зловмисники намагаються отримати доступ до неналежним чином деактивованих облікових записів аби за допомогою них обійти MFA;
- «Ghost Backup» (приховане резервне копіювання) – зловмисники впроваджують команди резервного копіювання на сторонні ресурси, які контролюються зловмисником);
- Stalkerware – використання зловмисниками різноманітного моніторингового ПЗ для отримання даних, які допоможуть атакувати інші ресурси жертви;
- кібервійна – розмивання межі між військовими та невійськовими інформаційними технологіями.

КІЛЬКІСТЬ КІБЕРЗЛОЧИНІВ У АВСТРАЛІЇ ЗРОСТАЄ. НАЙБІЛЬШУ ЗАГРОЗУ ВСЕ ЩЕ НЕСУТЬ АТАКИ RANSOMWARE – АВСТРАЛІЙСЬКИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

4 листопада Австралійський центр кібербезпеки оприлюднив щорічний звіт «Annual Cyber Threat Report 2021-2022». Відповідно до нього за звітний період кількість кіберзлочинів зросла на 13% (минулого року було зафіксовано 76 тисяч кіберзлочинів). Атаки через ransomware хоча і становлять порівняно незначну частку зафіксованих злочинів, але є найбільш руйнівними. Звіт також звертає увагу на проблему приховування таких атак з боку жертв (особливо якщо вони обрали рішення виплатити викуп).

НЕГАТИВНИЙ ВИПЛИВ ВІД RANSOMWARE СУТТЄВО ВИХОДИТЬ ЗА МЕЖІ ВИКЛЮЧНО ФІНАНСОВИХ ВТРАТ ОРГАНІЗАЦІЙ – RUSI

15 листопада було оприлюднено проміжні результати діяльності проєкту «Наслідки ransomware та досвід жертв», який організовано королівським об’єднаним інститутом послуг (Royal United Service Institute (RUSI). Його мета – дослідити ширший контекст впливу, який здійснюють ransomware атаки на їх жертв. Результати вказують, що жертви атак часто відчувають соціальний тиск (відповідальність) за продовження функціонування своїх систем для інших споживачів, що змушує їх виплачувати викуп. В деяких випадках наслідки ransomware атак виходять суттєво за межі навіть очікуваних кіберзлочинцями складнощів для їх жертв. Це вказує на необхідність приділяти більше уваги попередженню таких інцидентів.

ПЕРЕХІД ДО КРАЩОЇ КІБЕРБЕЗПЕКИ ДЛЯ СЕКТОРА ОХОРОНИ ЗДОРОВ’Я США ЗАЛИШАЄТЬСЯ ПОВІЛЬНИМ І НЕЗАДОВІЛЬНИМ – СЕНАТОР США МАРК ВОРНЕР

3 листопада сенатор США Марк Ворнер опублікував 35-сторінковий звіт «Кібербезпека для захисту пацієнтів», у якому дається негативна оцінка темпів впровадження практик кібербезпеки у секторі охорони здоров’я. У звіті зазначається, що сектор охорони здоров’я вразливий до кібератак через його залежність від застарілих технологій, що створює широку та різноманітну поверхню для кібератак. Ця загроза посилюється через постійне впровадження нових медичних пристроїв IoT.
У трьох розділах звіту йдеться про те, що федеральний уряд може зробити аби допомогти сектору охорони здоров’я поліпшити свою кібербезпеку: посилення ролі федерального уряду в цьому питанні, збільшення якості послуг кібербезпеки у сфері медичних послуг за допомогою системи стимулів і вимог, федеральна допомога у випадку надзвичайних ситуацій і відновлення після кібератак.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

MICROSOFT У 2023 РОЦІ НАДАСТЬ УКРАЇНІ ДОПОМОГУ НА 100 МЛН ДОЛАРІВ

3 листопада Бред Сміт, віце-голова та президент Microsoft, на спільній прес-конференції з віце-прем'єр-міністром України Михайлом Федоровим під час WebSummit (Лісабон, Португалія) оголосив, що Microsoft продовжить надавати Україні допомогу, зокрема державним установам, критичній інфраструктурі та іншим секторам в Україні які зможуть продовжувати використовувати цифрову інфраструктуру Microsoft та обслуговувати громадян через Microsoft Cloud. Сума цієї допомоги – 100 млн доларів.

190 ПРЕДСТАВНИКІВ ІЗ 50 КРАЇН СВІТУ АПЛОДУВАЛИ СТОЯЧИ НА ПІДТРИМКУ УКРАЇНИ ПІСЛЯ ВИСТУПУ СЕКРЕТАРЯ НКЦК НАТАЛІЇ ТКАЧУК НА МІЖНАРОДНІЙ КОНФЕРЕНЦІЇ

Керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО Україн, секретар Національного координаційного центру кібербезпеки Наталія Ткачук взяла участь у Міжнародній конференції із просування ролі жінок у протидії кіберзлочинності, що відбулася в м. Сан-Хосе (Коста-Рика) 10-11 листопада 2022 року.

Відкриваючи конференцію, керівник профільної служби наголосила, що нині триває перша у світі кібервійна, та поінформувала про кіберзлочини, які рф вчиняє проти України, зокрема, про численні кібератаки країни-агресора на критичну інфраструктуру та їх наслідки, які зараз відчуває кожен українець.

«Україна перемагає у цій кібервійні, зокрема, завдяки талановитим жінкам сектору безпеки та оборони, які щодня важко працюють для захисту кіберпростору. Багато дівчат в IT-армії, з-поміж кіберволонтерів тощо демонструють приголомшливі результати. В Україні десятки тисяч жінок виборюють перемогу пліч-о-пліч з чоловіками на передовій та у кіберпросторі. Наш приклад показує, що гендер не має значення, коли відбувається боротьба з країною-терористом за незалежність своєї держави», – сказала Наталія Ткачук.

НКЦК ТА CRDF GLOBAL ПРОВЕЛИ ОНЛАЙН-КОНФЕРЕНЦІЮ ЩОДО КІБЕРНЕТИЧНИХ ТА ФІЗИЧНИХ РИЗИКІВ БЕЗПЕКИ ДЛЯ СЕКТОРУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УКРАЇНІ

Національний координаційний центр кібербезпеки разом з CRDF Global 14 листопада 2022 року провели конференцію на тему: «Термінові дії: пом'якшення кіберзагроз і ризиків фізичної безпеки в секторі критичної інфраструктури». У ній взяли участь понад 170 представників профільних українських та міжнародних відомств, а також приватного сектору.
Основна мета заходу – привернути увагу донорів та міжнародної спільноти до питання важливості невідкладних дій щодо актуальних загроз кібер- та фізичній безпеці, які впливають на широку міжнародну систему.

ПРЕЗИДЕНТ УКРАЇНИ ВОЛОДИМИР ЗЕЛЕНСЬКИЙ ЗАЯВИВ, ЩО УКРАЇНА ГОТОВА ДОПОМОГТИ СВІТОВІ У ЗАБЕЗПЕЧЕННІ ЦИФРОВОЇ БЕЗПЕКИ

«Моя вам добра порада – візьміть український досвід захисту, щоб гарантувати безпеку вашим народам. Ми створили ІТ-армію, яка перемагає у кіберпросторі. Найкращі фахівці та компанії об'єдналися для захисту держави. Понад 1300 кібератак ми відбили за вісім місяців російської війни», – сказав Володимир Зеленський під час участі у панелі «Цифрова трансформація» у межах саміту G20.
Президент розповів, що у перший тиждень вторгнення росія знищила ключовий дата-центр нашої країни, і рішенням у відповідь були «хмари», до яких перенесли частину інформаційних систем. Це дозволило збудувати захист державних реєстрів та зберегти цифрову стійкість банків.
«Кіберзахист – це співпраця. Стійкість інституцій – це співпраця. Надійний зв'язок, зокрема супутниковий, – це також співпраця. Що нам усім треба – це відкинути суперечки й розвивати колективні зусилля заради глобального миру. Україна готова допомагати. Наш безпековий досвід – це ваш безпековий досвід», – наголосив Володимир Зеленський.

ДИРЕКТОР ОБ'ЄДНАНОГО ЦЕНТРУ ПЕРЕДОВИХ ТЕХНОЛОГІЙ З КІБЕРОБОРОНИ НАТО ВІДВІДАВ КИЇВ ЗАДЛЯ ОБГОВОРЕННЯ ПИТАНЬ ПОГЛИБЛЕННЯ ПРАКТИЧНОГО СПІВРОБІТНИЦТВА МІЖ УКРАЇНОЮ ТА ЦЕНТРОМ

21 листопада 2022 року директор Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE) Март Ноорма провів зустріч з керівництвом суб'єктів забезпечення кібербезпеки України у Кабінеті Міністрів України. У ній взяли участь представники НКЦК, МЗС, Мінцифри, Міноборони, Держспецзв'язку, СБУ та Апарату РНБО України. Під час зустрічі учасники обговорили обмін досвідом у сфері організації кіберзахисту та протистояння кібератакам. Така співпраця допоможе забезпечити спільний безпечний кіберпростір.
Під час візиту Марта Ноорми до Києва також відбулась низка двосторонніх зустрічей з представниками зазначених відомств.
Зокрема, 21 листопада 2022 року відбувся візит пана Ноорми до НКЦК в ході якого заступник Секретаря РНБО України Сергій Демедюк та керівник служби з питань інформаційної та кібербезпеки Апарату РНБО України – секретар НКЦК Наталія Ткачук обговорили з директором CCDCOE NATO шляхи поглиблення практичного співробітництва між Україною та Об'єднаним центром передових технологій з кібероборони Альянсу. Зокрема відбувся обмін думками щодо залучення українських фахівців до роботи CCDCOE, що базується у м. Таллінн.

«КОЛИ МИ ПРАЦЮЄМО СПІЛЬНО, НАШУ КРАЇНУ НЕ ЗМОЖЕ ПОДОЛАТИ ЖОДЕН ВОРОГ», – ОЛЕКСІЙ ДАНІЛОВ, ВІДКРИВАЮЧИ NATIONAL DEFENCE HACKHATON 2022

24 листопада 2022 року відбулось офіційне відкриття Національного оборонного хакатону 2022. Секретар РНБО України Олексій Данілов, звертаючись до учасників, зазначив, що переважна більшість з них «вже знаходиться на фронті 3192 дні» – з 27 лютого 2014 року, коли «російська ганчірка з'явилася на одному з офіційних приміщень України в Криму».
«Те, чим ви займаєтесь, є абсолютно неперевершеним, тому що вперше у світі триває відкрита кібервійна з дуже складним і сильним супротивником, який має на меті знищити нашу країну, нашу державність, наш народ. Але я більш ніж впевнений, що завдяки та вашій службі, вашій роботі, вашій спільноті перемога буде за нами», – зазначив Олексій Данілов.

У СТОЛИЦІ ЗАВЕРШИВСЯ НАЦІОНАЛЬНИЙ ОБОРОННИЙ ХАКАТОН

У Києві відбулося офіційне закриття наймасштабнішого за всю історію України National Defence Hackathon 2022 (Національного оборонного хакатону — 2022) та нагородження переможців. Протягом трьох днів провідні експерти у сфері IT приватного та державних секторів, фахівці з кібербезпеки, протидії дезінформації, інженери, конструктори та навіть юристи працювали над інноваційними рішеннями, які мають прискорити нашу перемогу над агресором.
Це був найбільший за кількістю учасників захід, який до цього проводився в Україні. Загалом у Національному оборонному хакатоні 2022 взяли участь майже 500 осіб. Безпосередньо змагалися майже 300 учасників — 41 команда. На виставці технічних рішень було проставлено 17 відібраних проєктів. Близько 200 фахівців взяли участь у панельних дискусіях, які проводилися у рамках хакатону.

У НАЦІОНАЛЬНОМУ ОБОРОННОМУ ХАКАТОНІ 2022 ПЕРЕМОГЛИ 5 КОМАНД ДЕРЖАВНОГО ТА 6 КОМАНД ПРИВАТНОГО СЕКТОРІВ

26 листопада 2022 року відбулись презентації проєктів та рішень учасників Хакатону, а також визначено та нагороджено переможців.
Змагання проходили за трьома напрямками: технічний, протидія дезінформації та юридичний. Серед завдань – розробка систем аналітики даних та відеопотоків, збору та аналізу великих обсягів даних, системи ідентифікації ворога тощо, а також засобів інформаційно-психологічної протидії.
Команди отримали цінні призи від організаторів, партнерів хакатону та NATO в Україні. Зокрема, сертифікати на навчання з кібербезпеки за стандартами НАТО на суму від 500 до 1000 євро, а також сучасні ноутбуки, смартфони та інші подарунки. Володарі першого місця державного сектору отримали право на участь у NATO TIDE Hackathon 2023, який відбудеться у лютому в Польщі.

ДЕРЖСПЕЦЗВ'ЯЗКУ ЗА ПІДТРИМКИ USAID ПРОВЕЛИ КРУГЛИЙ СТІЛ НА ТЕМУ: «ФОРМУВАННЯ НАЦІОНАЛЬНОЇ РАМКИ КВАЛІФІКАЦІЇ З КІБЕРБЕЗПЕКИ»

Представники Апарату РНБО України, Міністерства оборони України, Держспецзв'язку, Служби безпеки України та інших суб'єктів національної системи кібербезпеки України, міжнародні експерти обговорили перспективи реформ та подальші плани щодо підготовки фахівців під час Круглого столу «Формування національної рамки кваліфікації з кібербезпеки».
Заступник голови Держспецзв'язку Олександр Потій у межах заходу презентував Концепцію розбудови кадрового потенціалу України у сфері кібербезпеки та зазначив, що головна її мета – побудова та розвиток сталої екосистеми освіти, професійного навчання та трудового ресурсу.
«Успіхам нашої держави на кіберфронті ми завдячуємо саме висококваліфікованим фахівцям. Тому нині один з пріоритетів – збільшувати якісний кадровий потенціал держави у сфері кібербезпеки як у приватному, так і в державному секторі. Запровадження професійних стандартів сприятиме суттєвому підвищенню якості освіти», – сказав заступник Секретаря РНБО України.
Керівник служби з питань інформаційної та кібербезпеки Апарату РНБО України Н. Ткачук наголосила, що під час роботи над Стратегією кібербезпеки України закладалося бачення необхідності розвитку кадрового потенціалу національної системи кібербезпеки на стратегічному рівні як один з першочергових пріоритетів.

СБУ ЗАБЛОКУВАЛА МАСШТАБНЕ ОНЛАЙН-КАЗИНО, ЯКЕ «ПЕРЕРАХУВАЛО» В РФ МАЙЖЕ 3 МЛРД ГРН

Кіберфахівці СБУ провели безпрецедентну спецоперацію із документування і блокування організованого злочинного угруповання, створеного громадянами рф в Україні. В результаті вдалося ліквідувати їхнє незаконне онлайн-казино, через яке до рф через криптоперекази «пішло» близько 3 млрд у гривневому еквіваленті.
Як встановив Департамент кібербезпеки СБУ, до злочинної організації входили громадяни України та рф. Зловмисники мали ієрархічну управлінську вертикаль, на чолі якої стояли росіяни.
Українські громадяни в угрупованні відповідали за пошук офісів та обслуговуючого персоналу, а також за рекламну підтримку, облаштування комп'ютерної техніки і авторизацію клієнтів віртуального казино. Крім того, вони моніторили платежі та налагоджували інфраструктуру, необхідну для роботи азартних ігор в мережі «Інтернет».

СБУ ЛІКВІДУВАЛА ВОРОЖУ БОТОФЕРМУ, ЯКА ЩОДНЯ СТВОРЮВАЛА ПОНАД 500 АКАУНТІВ ДЛЯ ПОШИРЕННЯ КРЕМЛІВСЬКОЇ ПРОПАГАНДИ

Кіберфахівці Служби безпеки заблокували потужну ботоферму, яка працювала на користь спецслужб країни-агресора. В результаті слідчо-оперативних дій у Києві та Вінницькій області викрито п'ятьох її організаторів, які проводили інформаційні диверсії проти нашої держави.
Спеціалізоване обладнання ворожого «осередку» дозволяло щодня реєструвати понад 500 анонімних облікових записів у різних соцмережах, у тому числі заборонених в Україні. Саме ці фейкові акаунти використовували для поширення кремлівської пропаганди в інтернет-просторі.

РФ ЩОДНЯ ЗДІЙСНЮЄ ПОНАД 10 КІБЕРАТАК НА СТРАТЕГІЧНІ ОБ'ЄКТИ УКРАЇНИ, – КЕРІВНИК ДЕПАРТАМЕНТУ КІБЕРБЕЗПЕКИ СБУ

Росія супроводжує свої ракетні удари по енергетичних об'єктах України потужними кібератаками, щоб спричинити максимальний «блекаут». Проте такі сценарії є прогнозованими, а відтак – не досягають своєї мети. Про це в інтерв'ю виданню «Ліга.НЕТ» розповів начальник Департаменту кібербезпеки СБУ Ілля Вітюк.
«СБУ постійно блокує кібератаки на об'єкти енергетики. Саме ця галузь, разом з інфраструктурою і логістикою – це пріоритетні цілі для російських спецслужб. Останні обстріли ТЕЦ та ГЕС супроводжувалися і кібератаками. В СБУ очікували на такий сценарій, тому жодна з них не була ефективною», – підкреслює Ілля Вітюк.
За його словами, в середньому рф здійснює понад 10 кібератак на Україну за добу. Більшість із них залишаються непоміченими для суспільства, але не для фахівців, які їх відбивають і локалізують.

ВІДБУЛИСЯ СПЕЦІАЛЬНІ НАВЧАННЯ НА БАЗІ ТРЕНІНГОВОГО ЦЕНТРУ КІБЕРЦЕНТРУ UA30

На базі Тренінгового центру Кіберцентру UA30, що діє при Державному центрі кіберзахисту Держспецзв'язку, пройшла серія практичних кібертренінгів.
У межах навчань слухачі ознайомилися з особливостями кібербезпеки в середовищі промислових систем керування, стандартами та платформами для керування кібербезпекою, а також моделями застосування принципів кібербезпеки до промислових мереж. Крім того, слухачі ознайомилися з такою категорією кіберзахисту як Управління активами, що належать до класу заходів кіберзахисту – ідентифікація ризиків кібербезпеки. Здобуті знання закріплювали практичними навичками, адже особливу увагу в межах тренінгів було приділено практичній складовій – впровадженню заходів кіберзахисту в тестовому стенді з кібербезпеки промислових систем керування енергетичного сектору.

ПРЕЗИДЕНТ УКРАЇНИ ВОЛОДИМИР ЗЕЛЕНСЬКИЙ ПІДПИСАВ УХВАЛЕНИЙ ВЕРХОВНОЮ РАДОЮ ЗАКОН, ЗГІДНО ЯКОГО, ДЕРЖСПЕЦЗВ'ЯЗКУ ВИКОНУВАТИМЕ ФУНКЦІЇ УПОВНОВАЖЕНОГО ОРГАНУ З ПИТАНЬ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

«Вже триває робота над створенням переліку ОКІ. Також буде сформовано та наповнено реєстр об'єктів критичної інформаційної інфраструктури. Це дасть можливість проаналізувати рівень їхньої захищеності та посилити стійкість там, де необхідно, ефективніше виявляти загрози та запобігати їм, забезпечувати постійний і надійний захист таких об'єктів», – зазначає голова Держспецзв'язку Юрій Щиголь.
Відповідно до Закону, Держспецзв'язку здійснюватиме повноваження уповноваженого органу з питань захисту критичної інфраструктури України під час дії воєнного стану, а також протягом 12 місяців після його припинення чи скасування.

ЗАТВЕРДЖЕНО ПЕРШІ ШІСТЬ ПРОФЕСІЙНИХ СТАНДАРТІВ ДЛЯ ПРОФЕСІЙ У СФЕРІ КІБЕРБЕЗПЕКИ

Держспецзв'язку реформує професійну освіту України в галузі кібербезпеки.Реформа ґрунтується на запровадженні системи професійних стандартів і створенні в Україні мережі незалежних кваліфікаційних центрів, які поліпшуватимуть можливості професійного зростання та підтвердження кваліфікації наявних на ринку фахівців.
Торік Держспецзв'язку було зроблено перший крок: до державного класифікатора професій були додані 17 професій у галузі кіберзахисту та інформаційної безпеки.
Цього року за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України» були розроблені перші шість професійних стандартів для таких професій: розробник систем захисту інформації, адміністратор мереж і систем, фахівець сфери захисту інформації, аналітик з безпеки інформаційно-телекомунікаційних систем, фахівець з питань безпеки та інструктор-методист з інформаційної безпеки та кібербезпеки.
Наступного року Держспецзв'язку продовжуватиме роботу над розробленням професійних стандартів. Зокрема, на 2023 рік заплановано збільшити кількість професій у сфері кібербезпеки та захисту інформації до 20 для створення кваліфікаційної рамки, а також розробити стандарти до 14 професій.

АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ ОТРИМАЛА 50 ГЕНЕРАТОРІВ ВІД АМЕРИКАНСЬКИХ ПАРТНЕРІВ

USAID передав Адміністрації Держспецзв'язку 50 генераторів у межах постійної співпраці. Вони допоможуть забезпечити безперебійну роботу Адміністрації Держспецзв'язку, що позитивно відобразиться на діяльності підпорядкованих установ, а також операторів критичної інфраструктури України в умовах постійних ракетних ударів росіян по українській цивільній інфраструктурі України.
Співпраця USAID та Держспецзв'язку сприятиме підвищенню стійкості національної телекомунікаційної мережі України, публічних інформаційних ресурсів і комунікаційних послуг. Генераторні установки були придбані у межах реалізації Проєкту USAID «Кібербезпека для критично важливої інфраструктури в Україні».

МИ ТУТ, ЩОБ ДОПОМАГАТИ В КІБЕРЗАХИСТІ – ЗАСТУПНИК ГОЛОВИ ДЕРЖСПЕЦЗВ'ЯЗКУ ЗАКЛИКАВ БІЗНЕС ПОСИЛИТИ СПІВПРАЦЮ ЗАДЛЯ КІБЕРСТІЙКОСТІ

Заступник голови Держспецзв'язку Віктор Жора взяв участь в українській технологічній конференції Forbes Tech, де став гостем дискусії «HardTalk – Кіберзагрози: масштаб виклику». Ключовими темами розмови стала співпраця держави і бізнесу в посиленні кіберстійкості України та міжнародна робота у розбудові єдиного захищеного кіберпростору цивілізованого світу.
Під час виступу заступник голови Держспецзв'язку наголосив на тому, що після повномасштабного воєнного вторгнення росії в Україну російські хакери значно збільшили кількість атак на інформаційну інфраструктуру не лише України, але й інших країн – наших партнерів. Саме тому побудова єдиної солідарної системи кібербезпеки демократичного світу має бути одним із пріоритетів міжнародної політики.
В цьому напрямку Україна проактивно працює на міжнародному рівні: з урядами інших країн, глобальним бізнесом, міждержавними об'єднаннями й інституціями.

ПІДТРИМКА УКРАЇНИ ТА БЕЗПЕКОВА СИТУАЦІЯ У СВІТІ – ГОЛОВНІ ТЕМИ МІЖНАРОДНОГО ГАЛІФАКСЬКОГО ФОРУМУ

У канадському Галіфаксі проходить Міжнародний безпековий форум – щорічна світова конференція з питань безпеки, у якій беруть участь урядовці, представники парламентів демократичних країн світу, фахівці, експерти з міжнародних відносин, безпеки та оборони. У центрі уваги цьогорічного заходу – ситуація в Україні, протистояння російському воєнному вторгненню, яке спричинило наслідки, відчутні не тільки для українців, а і для всього світу. Перший заступник голови Держспецзв'язку Дмитро Маковський розповів про руйнування окупантами телеком-інфраструктури та потреби України під час її відновлення на деокупованих територіях, а також про становище у кіберпросторі та протистояння атакам російських хакерів. Зокрема нагадав, що кіберпростір не має кордонів, і для посилення кіберзахисту потрібні спільні зусилля. Він також наголосив на важливості підтримки України щодо посилення фізичного захисту критичної інфраструктури, особливо – енергетичної, яка зараз є основною ціллю країни-терориста.

НАЦІОНАЛЬНИЙ БАНК ПРЕДСТАВИВ УЧАСНИКАМ ПЛАТІЖНОГО РИНКУ ТА РИНКУ ВІРТУАЛЬНИХ АКТИВІВ ПРОЄКТ КОНЦЕПЦІЇ Е-ГРИВНІ

Національний банк презентував представникам банків, небанківських фінансових установ та ринку віртуальних активів для обговорення та отримання зворотного зв'язку проєкт концепції е-гривні – цифрових грошей Національного банку України.
Під час обговорення з учасниками ринків НБУ презентував також можливий дизайн е-гривні, її архітектуру, характеристики та переваги для надавачів платіжних послуг. Зокрема використання технологічної платформи для миттєвих розрахунків е-гривнею, програмування послуг та аналізу потоків даних створить широкі можливості для виникнення нових бізнес-кейсів, цифровізації послуг, залучення нових клієнтів, оптимізації витрат тощо.

КІБЕРПОЛІЦІЯ ВИКРИЛА ЗЛОВМИСНИКІВ У НЕСАНКЦІОНОВАНОМУ ВТРУЧАННІ В ЕЛЕКТРОННІ СИСТЕМИ ДЕРЖАВНОЇ УСТАНОВИ З ВИГОТОВЛЕННЯ УКРАЇНСЬКИХ ДОКУМЕНТІВ

Протиправну схему фігуранти налагодили з метою заробітку. Вони створювали штучне навантаження на електронні системи, відтак унеможливлювали реєстрацію користувачів в електронній черзі для отримання документів за кордоном. Щонайменше 150 громадян України вимушено скористалися платними послугами фігурантів для отримання талонів у черзі. Фігуранти за допомогою великої кількості зовнішніх запитів створювали навантаження на системи ДП «Документ» у Польщі. У такий спосіб вони перешкоджали іншим користувачам отримати електронні талони у черзі для оформлення документів. Паралельно зловмисники розміщували рекламу у соцмережах та месенджерах щодо «місця у черзі». Коштувала така послуга 800-1500 гривень.

У ДНІПРІ КІБЕРПОЛІЦІЯ ВИКРИЛА ЗЛОВМИСНИКІВ У ШАХРАЙСТВІ З ВИКОРИСТАННЯМ ФІШИНГУ НА ПЛАТФОРМІ ОГОЛОШЕНЬ

Використовуючи фішингові посилання, зловмисники привласнили понад 400 тисяч гривень. За скоєне їм може загрожувати до восьми років позбавлення волі.
Фігуранти знаходили оголошення щодо продажу товарів на тематичних платформах та для обговорення деталей писали продавцям у сторонні месенджери. Туди зловмисники надсилали фішингові посилання нібито про інтернет-оплату. Коли продавці переходили за посиланням та вводили дані банківської карти, ці відомості одразу ставали відомі шахраям. Отримавши доступ до банківських рахунків, зловмисники переводили гроші потерпілих на підконтрольні картки, оформлені на третіх осіб. Встановлено, що у такий спосіб вони привласнили понад 400 тисяч гривень.

КІБЕРПОЛІЦІЯ ЗАБЛОКУВАЛА РЕСУРС, ЯКИЙ ВИКОРИСТОВУВАЛИ ІНОЗЕМЦІ ДЛЯ ТЕЛЕФОННОГО ШАХРАЙСТВА

Ресурс, що розміщувався на українському домені, пропонував платні послуги з підміни мобільних номерів. Використовуючи технологію спуфінгу, шахраї вдавали, нібито громадянам телефонують з банку і надалі отримували доступ до їхніх карток.
Організував схему громадянин Великої Британії, який наразі вже перебуває під вартою. Чоловік створив власний сайт, де пропонувався «пакет послуг» для вчинення шахрайства із використанням соціальної інженерії.
Зокрема пропонувалося здійснювати спуфінг – підміну номера телефону. У такий спосіб зловмисники могли імітувати дзвінки від банків. Роботизований голос, під різними приводами, повідомляв про необхідність надання банківських даних фейковому працівнику банку. Отримавши ці відомості, зловмисники привласнювали гроші з рахунків потерпілих. Також сервіси давали змогу перехоплювати одноразові паролі.
Встановлено, що від протиправної діяльності ресурсу постраждали тисячі осіб, збитки сягають понад 100 мільйонів фунтів стерлінгів.

8. ПЕРША СВІТОВА КІБЕРВІЙНА

ДОПОМОГА США ПЕРЕД ВТОРГНЕННЯМ: ПОПЕРЕДЖУВАЛЬНІ ОПЕРАЦІЇ В УКРАЇНІ

28 листопада кіберкомандування США розповсюдило повідомлення із загальною інформацією щодо допомоги Україні з боку уряду США у боротьбі з кіберзагрозами напередодні російського вторгнення.
The US Cyber National Mission Force (CNMF) у грудні минулого року розгорнула велику місію для проведедення упереджувальних операцій (hunt forward) у співпраці з кіберкомандуванням України. Її присутність тривала до березня 2022 року.
Попри агресивне звучання назви, операції «полювання», за словами Кіберкомандування США, мають оборонний характер. Полювання ведеться в мережах країни, що обороняється. «Операції полювання – це суто оборонна діяльність, і операції здійснюються за допомогою розвідки».
Попри те, що персонал Національної кібернетичної місії США більше не дислокується в Україні, безперервна підтримка кіберзахисту України продовжується.

ЗА ОЦІНКАМИ УКРАЇНСЬКОГО УРЯДУ РОСІЙСЬКІ КІБЕРАТАКИ Є ОПОРТУНІСТИЧНИМИ ТА НЕЕФЕКТИВНИМИ

Виступаючи на Blackberry Security Summit, заступник голови Держспецзв'язку Віктор Жора зазначив, що російські кібероперації не змогли пошкодити українську інфраструктуру, хоча і мали таку мету. На його думку, ця невдача частково пояснюється відсутністю інтеграції кібероперацій у стратегію росії. Через цю нездатність координувати дії, атаки були опортуністичними та неефективними. Напади тривають, але безрезультатно, зазначив Жора.

КІБЕРПРОСТІР ЛАТВІЇ СТИКАЄТЬСЯ З НОВИМИ ВИКЛИКАМИ НА ТЛІ ВІЙНИ В УКРАЇНІ

Заступник керівника команди готовності до комп'ютерних надзвичайних ситуацій Латвії (CERT) Варіс Тейванс розповів, що від початку російської агресії проти України, кількість кібератак проти Латвії зросла на 30%.
В основному країна стикнулась з інспірованим державою хактивізмом низького рівня складності (переважно KillNet, F*ckNet і XakNet). Їх атаки часто демонструють погану розвідувальну підготовку (наприклад, було атаковано вебсайт, пов'язаний із закритим аеропортом), і часто досягають лише «піар ефекту». Ще одним прикладом може слугувати публікація загальнодоступної інформації із заявою, що її було отримано шляхом злому. Власне державні організації, APT, якими безпосередньо керують російські спецслужби, викликають більше занепокоєння. І хоча їх мета та планування є кращими, виглядає так, що вони також, більше орієнтовані на DDoS атаки, які призводять лише до збоїв у наданні послуг.

ВЕЛИКА БРИТАНІЯ РОЗКРИЛА ДЕТАЛІ ПАКЕТА ДОПОМОГИ УКРАЇНІ В СФЕРІ КІБЕРЗАХИСТУ

Британські фахівці допомагали протистояти кібератакам з боку рф, які вона спрямувала проти України у кілька хвиль. Атаки стали інтенсивнішими у другій половині минулого року, коли Москва готувалася до вторгнення. Під час наступної хвилі росіяни прагнули зірвати роботу українських міністерств у січні та лютому, а потім перейшли до нової, більш опортуністичної фази протягом останнього часу.
Британські фахівці працювали з українськими протягом цього часу. Допомога зосереджувалася на співпраці з галузевими партнерами, наданні спеціалізованих криміналістичних інструментів для виявлення та розслідування атак, а також на наданні апаратного забезпечення та інших систем для посилення захисту. Вартість пакета допомоги склала 6 мільйонів фунтів.

РОСІЙСЬКІ ХАКЕРИ АКТИВІЗУЮТЬ АТАКИ НА ОКІ В УКРАЇНІ ТА КРАЇНАХ НАТО

Про це йдеться в аналітичному звіті компанії Microsoft Microsoft Digital Defense Report за 2022 рік, опублікованому 4 листопада 2022 року.
Кібератаки проти критичної інфраструктури становили 40% атак, виявлених компанією з липня 2021 року по червень цього року. Причиною цього Microsoft вважає спроби росії атакувати критичну інфраструктуру України та її союзників. Загалом 90% атак, пов'язаних з рф, були спрямовані проти країн НАТО. США були головною мішенню, але Microsoft також спостерігала «значний» акцент на Польщі.
Звіт також відзначає, що деякі державні актори все більше вдаються до складних операцій впливу на внутрішні та зовнішні аудиторії у кіберпросторі. Такі операції підривають довіру, посилюють поляризацію та становлять загрозу для демократичних процесів. Якщо раніше їх переважно застосовувала рф проти України, то сьогодні росія, Китай та Іран вдаються до цих методів з метою досягнення своїх геополітичних цілей.

УКРАЇНСЬКІ ХАКТИВІСТИ ЗАЯВЛЯЮТЬ, ЩО ЗЛИЛИ ДОКУМЕНТИ ЦЕНТРАЛЬНОГО БАНКУ РФ

7 листопада української IT-армія заявила у своєму телеграм-каналі, що її активісти зламали сайт Центрального банку рф та виклали у мережу 2.6 GB документів, які містять детальну інформацію про операції банку, його політику безпеки та персональні дані деяких його нинішніх і колишніх співробітників. Разом з тим, важко оцінити цінність викрадених документів, адже деякі з них є застарілими (10 років), деякі описують стратегію банку та не містять значних секретів.

MICROSOFT ЗВИНУВАЧУЄ РОСІЙСЬКИХ ХАКЕРІВ В АТАКАХ PRESTIGE RANSOMWARE НА УКРАЇНУ ТА ПОЛЬЩУ

11 листопада компанія Microsoft пов'язала низку нещодавніх інцидентів за участі програм-вимагачів, спрямованих на транспортні та логістичні сектори економіки України та Польщі, з кластером загроз, який збігається з російською державною групою Sandworm. Атаки здійснювалися за допомогою раніше не описаного шкідливого програмного забезпечення Prestige, і відбулися протягом години одна після одної. Microsoft Threat Intelligence Center (MSTIC) відстежує угрупування під назвою Iridium (або DEV-0960), яке є російським угрупованням, що публічно відстежується під назвою Sandworm (також Iron Viking, TeleBots і Voodoo Bear).

ОЦІНКА МІЖНАРОДНОЇ ПІДТРИМКИ КІБЕРЗАХИСТУ УКРАЇНИ

3 листопада Фонд Карнегі оприлюднив оцінку стану міжнародної допомоги, наданої Україні у сфері кіберзахисту. Така допомога принаймні частково пояснює, чому російська агресія проти України в кіберпросторі не виправдала очікувань.
Фонд Карнегі дослідив як допомогу з боку дружніх країн, так і допомогу від технологічних компаній, таких як Starlink, яка надала можливість користуватися супутниковим зв'язком. А також Microsoft, яка надала 400 мільйонів доларів, що дозволило Україні та надалі користуватися хмарними послугами Redmond.
Дослідження закінчується деякими уроками, які вже сьогодні можна винести з досвіду російської війни у кіберпросторі. Загалом ці уроки свідчать про ефективність колективного захисту.

ЗБРОЙНИЙ КОНФЛІКТ ДЕСТАБІЛІЗУЄ КІБЕРПРОСТІР ДЛЯ ВСІХ – CYBERPEACE INSTITUTE

11 листопада головний виконавчий директор Стефан Дюген (CyberPeace Institute) оприлюднив свої міркування щодо впливу кіберскладової російсько-української війни на міжнародну кібербезпеку. Він вказує, що хоча боротьба сторін у кіберпросторі цілком зрозуміла, але форми у яких вона ведеться, створюють загрози для інших суб'єктів.
Так, кібератака Росії на супутники KA-SAT мала на меті погіршити комунікації українських військових, але вплинула на вітрові турбіни у Німеччині. На думку Дюгена це знову ставить питання про необхідність запровадження правил «відповідальної поведінки» у кіберпросторі. Він пропонує введення шести норм – починаючи від недопустимості скеровування кібератаки проти критичної інфраструктури та закінчуючи документування впливу кібератак на звичайних людей аби спростити подальші розслідування.

ВЕБСАЙТ ЄВРОПАРЛАМЕНТУ БУЛО АТАКОВАНО ПІСЛЯ ПРОГОЛОШЕННЯ РОСІЇ ДЕРЖАВОЮ-ТЕРОРИСТОМ

23 листопада вебсайт Європарламенту було атаковано (DDoS) угрупуванням Killnet. Вебсайт парламенту припинив роботу невдовзі після того, як законодавці ЄС переважною більшістю голосів проголосували за визнання росії «державою спонсором тероризму» через її напади на Україну.

ХАКЕРИ ГРУ ЗМІНЮЮТЬ ТАКТИКУ В АТАЦІ УКРАЇНСЬКИХ ОБ'ЄКТІВ – ВИСНОВКИ MANDIANT

10 листопада під час конференції CyberwarCon в Арлінгтоні, штат Вірджинія фахівці компанії Mandiant оприлюднили результати свого дослідження щодо російської кіберактивності в Україні. Вони вказують на зміну тактики хакерів, що афільовані із російською військовою розвідкою: замість довготривалих спроб атакувати самі цілі вони почали концентруватись на периферійні цілі – брандмауери, маршрутизатори та сервери електронної пошти. Після їх зламу вони отримують доступ до систем в яких вони зацікавлені. Це дозволяє їм досягти значно швидших ефектів, ніж раніше. Нова тактика дозволяє їм не лише проводити операції швидше, але багаторазово атакувати одну і ту саму ціль – як з метою кібершпигунства, так і знищення даних.

ВІЙСЬКОВИЙ КОНФЛІКТ ЗМУШУЄ ІНАКШЕ ПОГЛЯНУТИ НА ЗАГРОЗИ ЦИФРОВІЙ ІНФРАСТРУКТУРІ – ПРЕДСТАВНИК ПЕНТАГОНУ

16 листопада Міейк Еойанг (Mieke Eoyang) заступник помічника Міністра оборони з питань кіберполітики під час Aspen Cyber Summit поділився окремими висновками, які для себе виніс Пентагон з російсько-української війни та, зокрема, кіберскладової. Ключовий висновок, що мислення про проблеми безпеки цифрової інфраструктури у мирний та воєнний час суттєво відрізняються: «Традиційний підхід до безпеки такої інфраструктури – це як часто вам треба зробити патчі вразливостей. Однак під час військового конфлікту вам треба думати про фізичну безпеку цих об'єктів. Чи дістануть їх ракети супротивника?».

ПОТРІБНІ ЛЮДИ У ПОТРІБНІЙ КІМНАТІ У ПОТРІБНИЙ ЧАС МОЖУТЬ БУТИ СТРАТЕГІЧНО ВАЖЛИВІ ДЛЯ КІБЕРБЕЗПЕКИ – ПОЛ НАКАСОНЕ

США продовжують вивчати уроки російсько-української війни та оцінювати ефективність різних практик у сфері кібербезпеки чи міжнародного співробітництва. Одним з таких висновків, за словами керівника NSA Пола Накасоне, є те, що фізична присутність фахівців з кібербезпеки у певних приміщеннях чи на певних об'єктах може бути критично важливою. Стаття «Попередня робота в Україні притупила кіберперевагу росії, кажуть США» оцінює діяльність з кіберпідтримки, яку США надавала низці країн, в тому числі Україні, перед вторгненням. Одним з елементів такої підтримки було направлення команди фахівців з кібербезпеки у грудні 2021 року.

РОСІЙСЬКА ПРОГРАМА-ВИМАГАЧ RANSOMBOGGS АТАКУВАЛА КІЛЬКА ОРГАНІЗАЦІЙ В УКРАЇНІ

Україна зазнала нових атак програм-вимагачів, які наслідують попередні, приписувані російському державному угрупованню Sandworm. Словацька компанія з кібербезпеки ESET, яка назвала новий штам програм-вимагачів RansomBoggs, заявила, що атаки на кілька українських організацій вперше були виявлені 21 листопада 2022 року. «Хоча зловмисне програмне забезпечення, написане в .NET, є новим, його розгортання схоже на попередні атаки, які приписують Sandworm», – заявила компанія у Твіттері. Аналіз нової програми-вимагача, проведений ESET, показує, що вона генерує випадковий ключ і шифрує файли за допомогою AES-256 у режимі CBC і додає розширення файлу «.chsch».

9. РІЗНЕ

КАЗНАЧЕЙСТВО США: У 2021 РОЦІ ФІНАНСОВІ УСТАНОВИ ПОВІДОМИЛИ ПРО ЗБИТКИ ВІД ПРОГРАМ-ВИМАГАЧІВ НА 1,2 МІЛЬЯРДА ДОЛАРІВ

Фінансові установи Сполучених Штатів повідомили про рекордний рік за кількістю атак програм-вимагачів і платежів у 2021 році. Причиною стали версії зловмисного програмного забезпечення, ймовірно, пов'язані з Росією. Загалом вартість інцидентів, зареєстрованих минулого року, підскочила з 416 мільйонів до 1,2 мільярда доларів США.
Було зареєстровано 1489 інцидентів порівняно з 487 у 2020 році, причому дослідники повідомили, що «програми-вимагачі продовжують становити значну загрозу для секторів критичної інфраструктури США, підприємств і громадськості». Дані були оприлюднені 1 листопада Мережею по боротьбі з фінансовими злочинами (FinCEN) Міністерства фінансів США.

ЯК ЄС НА ПРАКТИЦІ РЕАЛІЗУЄ ІДЕЮ ЦИФРОВОГО СУВЕРЕНІТЕТУ

2 листопада Європейська програма Atlantic Council оприлюднила дослідження політики ЄС, спрямованої на досягнення цифрового суверенітету та намагання вплинути на процес формування глобальної цифрової економіки.
Автори звіту стверджують, що хоча політика цифрового суверенітету ЄС не є чітко артикульованою, на практиці вона складається з трьох елементів:

- інтенсифікація підтримки розвитку технологій в ЄС;
- намагання розробити глобальні норми для управління даними та цифровим середовищем;
- збільшення обмежень для гравців, що не є членами ЄС, на ринку ЄС.

Така політика матиме значні наслідки для поточних та потенційних партнерів ЄС, адже ЄС намагається встановлювати «золотий стандарт» регулювання цифрової економіки у намаганні бути конкурентним на цифровому ринку.

США ПОСТУПАЮТЬСЯ КИТАЮ В КІЛЬКОСТІ ОПУБЛІКОВАНИХ НАУКОВИХ СТАТЕЙ НА ТЕМУ ЧІПІВ

США більше не можуть претендувати на перше місце за кількістю опублікованих і прийнятих дослідницьких робіт на тему дизайну мікросхем і передових технологій. Після останніх заявок на Міжнародну конференцію твердотільних схем (ISSCC 2023), одну з найвідоміших у світі подій з напівпровідникових схем, стало зрозуміло, що особлива нагорода тепер належить Китаю – попри тривалий клімат жорстких технологічних санкцій, які застосовуються проти країни. З 59 прийнятими документами з Китаю проти 42 з Північної Америки, США більше не можуть претендувати на першість у передових дослідженнях чіпів. Організатори конференції відзначають не лише збільшення кількості статей, а й покращення їх якості.

РОЛЬ ТЕХНОЛОГІЙ США В СИСТЕМІ ГРОМАДСЬКОЇ БЕЗПЕКИ КИТАЮ

1 листопада Insikt Group опублікувала звіт з результатами досліджень про те, як органи громадської безпеки Китаю отримують і використовують технології, що належать компаніям, розташованим у Сполучених Штатах.
Ці органи залучені до широкомасштабного насильства стосовно громадян Китаю з боку китайської держави, включаючи масове стеження, переслідування політичних і релігійних дисидентів та масове затримання етнічних меншин. Органи громадської безпеки в Китаї також займаються контррозвідкою та здійснюють розвідувальну діяльність у країні та за кордоном, спрямовану на запобігання політичних загроз Комуністичній партії Китаю (КПК). «Таким чином, передача технологій від американських компаній китайським органам громадської безпеки ризикує сприяти державному насильству, розвідці та контррозвідці в Китаї, незалежно від намірів компаній», – обґрунтовують автори звіту свій інтерес до досліджуваної ними теми.

ДИРЕКТОР ФБР КРІСТОФЕР РЕЙ ПОВІДОМИВ ЗАКОНОДАВЦЯМ, ЩО ФБР ПРОВОДИТЬ НАСТУПАЛЬНІ КІБЕРОПЕРАЦІЇ

Під час слухань у Комітеті з питань внутрішньої безпеки Сенату 17 листопада, Директор ФБР Крістофер Рей заявив, що його агентство проводить наступальні кібероперації проти державних і недержавних кіберакторів. Він підкреслив, що «стримування державних суб'єктів, що становлять загрозу, від продовження незаконної кіберактивності є набагато складнішим, ніж зрив їх операцій». Багато експертів вважають таку поведінку у кіберпросторі надто ризикованою та підкреслюють, що до таких дій варто вдаватися лише за крайніх умов та у випадку, якщо ти впевнений у своїй захищеності.

36% ФРАНЦУЗЬКИХ ВИПУСКНИКІВ ЗА КІБЕРБЕЗПЕКОВИМИ СПЕЦІАЛЬНОСТЯМИ НЕ ХОЧУТЬ ПРАЦЮВАТИ У КОМПАНІЯХ, ЯКІ СПЕЦІАЛІЗУЮТЬСЯ НА КІБЕРБЕЗПЕЦІ – ДОСЛІДЖЕННЯ РИНКУ ANSSI

У листопаді 2022 року французьке державне агентство кібербезпеки ANSSI оприлюднило результати дослідження майбутніх фахівців з кібербезпеки. Воно вказує на те, що у цій сфері все ще працюють переважно чоловіки (лише 11% жінок), а 36% студентів, які вивчають кібербезпеку, вважають, що краще працювати у відділі кібербезпеки компанії, для якої кібербезпека не є основною формою спеціалізації. 24% студентів вважають, що кібербезпека не цінується, однак при цьому 92% планують працювати за спеціальністю.