НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

УКРАЇНСЬКА ФУНДАЦІЯ БЕЗПЕКОВИХ СТУДІЙ

CYBER DIGEST

Огляд подій в сфері кібербезпеки,
Травень 2024

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

ЗМІСТ

ОСНОВНІ ТЕНДЕНЦІЇ

На початку травня Державний департамент США оприлюднив Стратегію міжнародного кіберпростору та цифрової політики. Запроваджуючи цей документ, США прагне стримати цифровий вплив росії та Китаю в країнах, що розвиваються, і зробити ймовірні спроби цих країн втручатися у вибори менш ефективними. Стратегія прагне залучити більше країн, що розвиваються, до «позитивного бачення» кіберпростору, яке відкидає цифрові репресії. В її рамках США продовжать багаторічне лобіювання серед союзників і партнерів, щоб вони не використовували ключові комунікаційні технології та ПЗ, створене в автократичних країнах, таких як росія та Китай. Загалом, її можна схарактеризувати як намагання США створити коаліцію проти Китаю. Китай, своєю чергою, видав звіт «Загрози з боку США та саботаж безпеки та розвитку глобального кіберпростору», який викриває «гегемонію та агресивну поведінку Сполучених Штатів у кіберпросторі.»

Україна цього місяця концентрувалася на різних аспектах міжнародної співпраці. В рамках Першої науково-практичної міжнародної конференції з питань кібердипломатії, Міністр Закордонних Справ Дмитро Кулеба наголосив, що Україна з її досвідом протидії рф та репутацією новатора, є невід'ємною частиною європейської та євроатлантичної систем безпеки, а заступник Секретаря РНБО Сергій Демедюк закликав разом будувати стратегії для прогнозованого та постійного посилення колективної кіберстійкості. Представники України взяли участь у декількох важливих міжнародних подіях, серед яких Asian Leadership Conference та RSA 2024. В межах IT-коаліції Естонія передасть засоби для підсилення кіберспроможностей України. Також розпочато співпрацю з Польщею у сфері цифрових технологій та інновацій, розвитку IT-індустрії, штучного інтелекту, захисту критичної інформації та державних реєстрів.

США входить в період проведення оцінок ефективності виконання стратегічних доручень Президента США у сфері кібербезпеки. Так, Управління звітності уряду Сполучених Штатів оприлюднило результати оцінки урядовими структурами Указу Президента США 14028 «Покращення кібербезпеки країни» – 49 з 55 задач (90%) були виконані. Крім того, було ухвалено оновлений План реалізації Національної стратегії кібербезпеки – до плану було додано 31 нову задачу. Одночасно з цим Офіс національного кібердиректора (ONCD) провів оцінку ефективності виконання першого Плану імплементації – було реалізовано близько 90% задач (33 з 36 запланованих ініціатив). Слід відмітити, що уряд США помітно посилив контроль за процесами виконання ухвалених ним стратегічних рішень, зробивши процедури оцінки більш регулярними та публічними.

Людський фактор залишається одним з ключових джерел кіберзагроз для організацій та їх інформаційних систем. Про це свідчать останні дослідження Verizon та Proofpoint. Респонденти опитування Verizon вказали на те, що 68% порушень безпеки ставались через не зловмисний людський фактор – тобто інциденти пов'язані з інсайдерськими помилками або людьми, які потрапили на схеми соціальної інженерії. Схожа статистика у компанії Proofpoint – її дослідження охопило 1600 CISO компаній, 74% з яких вказали на те, що людські помилки є найбільшою кібервразливістю для їх організацій. Проблема має більш масштабний характер ніж виключно навчання персоналу організацій і пов'язана з загальним рівнем кіберобізнаності. Тому CISA у травні 2024 року запустила вже другу загальнонаціональну програму з кіберобізнаності, яка має охопити різні цільові аудиторії, а інформація кампанії буде поширюватись на всіх основних платформах та майданчиках: телебачення, радіо, цифрова реклама, торгові центри, соціальні мережі, зовнішня реклама.

Підхід Secure by Design набуває все більшої ваги в державній політиці провідних держав. CISA активно просуває свою платформу Secure by Design pledge – добровільне об'єднання компаній, що беруть зобов'язання щодо дотримання правил Secure by Design – у травні таких компаній вже 68. Великобританія також готується до впровадження цього підходу для учасників ринку – на думку технічного директора британського NCSC Оллі Вайтхауса, нинішній підхід «тисячі пластирів» щодо кібербезпеки (коли розробники ПЗ чи технологій точково вирішують конкретні проблеми кібербезпеки у своїх продуктах) має повністю змінитись. Фактично мова йде і про більшу соціальну відповідальність компаній-розробників перед своїми клієнтами, особливо – з-поміж структур з традиційно обмеженими бюджетами на кібербезпеку: НУО, школи тощо. Державні структури, зі свого боку, також залучаються до посилення кібербезпеки таких соціально важливих організацій – CISA, DHS, ФБР спільно з міжнародними партнерами опублікували посібник для організацій з високим рівнем ризику.

Розвиток ШІ та його вплив на сферу кібербезпеки все частіше у фокусі уваги кібербезпекових організацій та дослідників. Поки Китай та США шукають можливості більше інвестувати в дослідження ШІ, а також розпочинають діалог на вищому рівні з цього питання, фахівці з кібербезпеки стикаються з викликами вже зараз. Наприклад, кібербезпековим фахівцям з Unit42 вдалось навчити ШІ створювати дієве зловмисне ПЗ користуючись релевантною базою вихідних даних – створене ШІ ПЗ не лише виявилось ефективним, але ШІ може оперативно модифікувати його, створювати численні варіації ядра шкідливого ПЗ та адаптувати його для різних платформ. Фахівці з Horizon3.ai вже пропонують нові сервіси з підтримкою ШІ для пришвидшення визначення пріоритетів кіберзахисту і виправлення вразливостей в кібербезпеці організацій. ШІ все частіше стає і предметом кібершпигунства – у травні невизначена APT група атакувала американських дослідників ШІ намагаючись отримати доступ до їх даних.

У США тривають дебати щодо UnitedHealth та руйнівної атаки ransomware проти IT систем її компанії Change Healthcare. За результатами низки розслідувань та слухань у Сенаті стало відомо, що компанія пішла на виплату 22 млн доларів викупу. Одночасно з тим були виявлені численні недоліки у політиці кібербезпеки організації, слабкий захист персональних даних клієнтів, а також невідповідної кадрової політики організації щодо кібербезпекового топменеджменту (CISO організації була людина без досвіду роботи на посадах, пов'язаних з кібербезпекою). Загальні втрати організації внаслідок цього інциденту вже склали понад 800 млн доларів і за попередніми оцінками сягнуть одного мільярда. Швидше за все кейс UnitedHealth призведе до посилення кібербезпекових вимог по всій медичній галузі в США. Схожою може бути ситуація для сектору водопостачання – через низку результативних кібератак за останні пів року Агентство з охорони навколишнього середовища США (EPA) провело низку перевірок, які виявили, що понад 70% систем водопостачання не повністю відповідають Закону про безпечну питну воду та мають критичні кібервразливості.

Правоохоронні органи змогли нанести ще один відчутний удар по інфраструктурі злочинних організацій – у травні правоохоронні органи 13 країн провели спецоперацію Endgame, яка дозволила знищити кримінальну інфраструктуру цілої низки зловмисних груп: IcedID, SystemBC, Pikabot, Smokeloader, Bumblebee і Trickbot. Українські правоохоронці активно долучились до цієї операції, провівши більшість арештів та обшуків. Також у травні британські, американські та австралійські правоохоронці розкрили особу лідера кіберзлочинної групи LockBit – ним виявився росіянин Дмитро Хорошев. Держдепартамент США вже встановив винагороду у 10 млн доларів за інформацію, яка дозволить його спіймати.

У площині протидії кіберзагрозам, Служба безпеки України та ФБР спільно з правоохоронними органами Великої Британії та ЄС провели спецоперацію у 8 країнах Європи, викривши понад 30 учасників транснаціональних хакерських угруповань. Фахівці команди CERT-UA у другій половини 2023 року зафіксували підвищений інтерес ворожих хакерів до українського телекомунікаційного сектору. Атаки на військових з метою доступу, контролю та зняття розвідувальної інформації зі спеціалізованих систем ситуаційної обізнаності залишаються стратегічною військовою ціллю противника. CERT-UA також попередила про діяльність кіберзловмисників, які використовують легітимну програму для віддаленого управління комп'ютерами SuperOps RMM з метою отримання несанкціонованого доступу до інформаційних систем українських організацій.

У травні відбулось декілька дзеркальних кібератак проросійських та проукраїнських груп. 9 травня українським хакерам вдалось на деяких російських телеканалах замінити сигнал з параду на 9 травня на кадри з війни в Україні. Дзеркально російські хакери зламали супутниковий сигнал телеканалу Інтер і транслювали українським глядачам російський парад. російські хакери все активніше діють проти інформаційних ресурсів міжнародних партнерів України. APT28 націлилась на польські інституції, невстановлені російські хакери зламали сайт Польського агентства преси (PAP) і розмістили там фейкову статтю що була спрямована на погіршення україно-польських відносин, а ще одна вдала атака російських хакерів призвела до зламу сотні місцевих британських новинних сайтів.

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

CISA СТАЛА НАЦІОНАЛЬНИМ КООРДИНАТОРОМ З БЕЗПЕКИ ТА СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

30 квітня Президент США оприлюднив Меморандум національної безпеки NSM-22 – документ, що визначає цілі та завдання для більшості урядових структур в питаннях забезпечення більшої безпеки та стійкості критичної інфраструктури. Одним з важливих елементів Меморандуму є фіксація за CISA ролі Національного координатора з безпеки та стійкості критичної інфраструктури. У рамках цієї нової ролі CISA відповідатиме за оцінку прогресу в покращенні пріоритетів безпеки та стійкості шістнадцяти секторів критичної інфраструктури, а також за виявлення загроз і рекомендації щодо заходів для покращення кібербезпеки. Водночас експерти зазначають, що поряд з цим очікуваним посиленням ролі CISA не відбулось розширення списку критичних секторів – очікувалось, що до шістнадцяти наявних будуть додані ще два – космічний та біоекономіка.

МОРГАН АДАМСКІ ПРИЗНАЧЕНА НОВИМ ВИКОНАВЧИМ ДИРЕКТОРОМ USCYBERCOM

3 травня USCYBERCOM повідомило про призначення нового виконавчого директора відомства. Нею стане Морган Адамскі, яка має значний досвід роботи в АНБ та Міністерстві оборони США. В минулому вона займалась питанням налагодження відносин між держорганами та галузевими структурами, долучалась до створення Кіберстратегії Міноборони США 2018 року, а також працювала головним операційним директором наступальної кібермісії NSA.

CISA ЗАПУСТИЛА ДРУГУ ЗАГАЛЬНОНАЦІОНАЛЬНУ ПРОГРАМУ З КІБЕРОБІЗНАНОСТІ

8 травня CISA запустила вже другий проєкт для підвищення кіберобізнаності американців – We Can Secure Our World. У 2024 році матеріали цієї програми будуть широко рекламуватися на території США (на всіх основних платформах та майданчиках: телебачення, радіо, цифрова реклама, торгові центри, соціальні мережі, зовнішня реклама). Перший такий проєкт, запущений у вересні 2023 року, отримав майже 20 000 переглядів на YouTube, а навчальні матеріали були завантажені близько 50 000 разів. Відео CISA транслювалося на NFL Experience перед Super Bowl і зібрало понад 200 000 переглядів у соціальних мережах.

В США ВІДБУЛИСЬ ДЕВ'ЯТІ НАЦІОНАЛЬНІ КІБЕРНАВЧАННЯ CYBER STORM

У травні 2024 року в США відбулись дев'яті національні кібернавчання Cyber Storm. До заходу долучилось 2200 учасників із 300 організацій, включаючи 80 приватних компаній, 35 федеральних агентств, 11 штатів, а також дев'ять країн. Протягом трьох днів учасники відпрацьовували реагування на кібератаки, зосереджуючись на неправильних конфігураціях хмарних середовищ і їхньому впливі на дані. Атаки починалися в харчовому та сільськогосподарському секторах і поширювалися на інші.

ОПРИЛЮДНЕНО ОНОВЛЕНИЙ ПЛАН ІМПЛЕМЕНТАЦІЇ НАЦІОНАЛЬНОЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ США

7 травня Адміністрація Байдена-Гарріса опублікувала оновлений План реалізації Національної стратегії кібербезпеки. Він описує 100 федеральних ініціатив для покращення кібербезпеки США. Новий план доповнює попередній документ новими ініціативами, в тому числі посилення кібербезпеки в секторі охорони здоров'я. Загалом документ включає 31 нову ініціативу для посилення кібербезпеки федеральних відомств. Це оновлення стало реакцією на оприлюднення звіту про стан кібербезпеки США за 2024 рік, підготовленого Офісом національного кібердиректора (ONCD). За даними звіту, перший План впровадження NCS (NCSIP) було реалізовано на майже 90% (33 з 36 запланованих ініціатив).

ВЕЛИКОБРИТАНІЯ ГОТУЄТЬСЯ ДО МАСШТАБНОГО ВПРОВАДЖЕННЯ ПОЛІТИКИ SECURE BY DESIGN

15 травня під час свого виступу на конференції CYBERUK, технічний директор британського NCSC Оллі Вайтхаус підкреслив, що нинішній підхід «тисячі пластирів» щодо кібербезпеки (коли розробники ПЗ чи технологій точково вирішують конкретні проблеми кібербезпеки у своїх продуктах) має повністю змінитись. Він зазначає, що розробники знають як робити свої продукти безпечними та стійкими, але проблема в тому, що ринок не стимулює такої політики. Відтак має змінитись сам підхід до розробки, адже швидкий розвиток технологій робить неможливим аналогічні швидкі зміни в державній політиці.

ANSSI ПРОВОДИТЬ КОНСУЛЬТАЦІЇ ЗІ СТЕЙКХОЛДЕРАМИ ЩОДО ІМПЛЕМЕНТАЦІЇ NIS2

29 травня ANSSI повідомила, що продовжує серію консультацій з учасниками ринку та стейкхолдерами щодо особливостей імплементації NIS2 Директиви у Франції. Ці консультації охопили понад 70 організацій, що представляють приватні та державні компанії. Серед них професійні федерації, асоціації та спілки з усіх секторів, яких стосується директива. Мета консультацій – почути позицію учасників ринку, яких безпосередньо торкнуться зміни внаслідок імплементації NIS2 Директиви. Консультації тривають з квітня місяця і все ще продовжуються.

ЄВРОПЕЙСЬКА РАДА УХВАЛИЛА КЕРІВНІ НАСТАНОВИ ДЛЯ СТВОРЕННЯ ГІБРИДНИХ ГРУП ШВИДКОГО РЕАГУВАННЯ

21 травня Європейська Рада схвалила Керівні настанови, що сприятимуть створенню гібридних груп швидкого реагування. Такі групи (які розгортаються за запитом) потрібні для підготовки та протидії гібридним загрозам і кампаніям впливу у сьогоднішньому світі. Вони будуть орієнтовані на протидію дезінформації, кібератакам, атакам на критичну інфраструктуру тощо. Гібридні групи мають стати одним із ключових інструментів для підтримки держав-членів ЄС і країн-партнерів у протидії гібридним загрозам у рамках EU Hybrid Toolbox.

АВСТРАЛІЙСЬКИЙ УРЯД ВКЛАДЕ 620 МЛН ДОЛАРІВ У СТВОРЕННЯ КВАНТОВОГО КОМП'ЮТЕРА ДЛЯ ЗЛАМУ ШИФРІВ

На початку травня уряд Австралії оголосив про підписання контракту з приватною компанією PsiQuantum на створення першого у світі універсального, відмовостійкого квантового комп'ютера. Сума контракту – 620 млн доларів. Комп'ютер займатиме цілу будівлю, а його створення розпочнеться наступного року. Комп'ютер розпочне функціонувати у 2027 році.

НІМЕЧЧИНА ГОТУЄТЬСЯ ЗАБОРОНИТИ ВИКОРИСТАННЯ КИТАЙСЬКОГО ТЕЛЕКОМ-ОБЛАДНАННЯ В МЕРЕЖАХ 5G

За даними Bloomberg, Міністерство закордонних справ Німеччини та Міністерство економіки підтримують пропозицію Міністерства внутрішніх справ вилучити техніку китайського виробництва з міркувань національної безпеки. Якщо таке рішення буде прийняте, німецькі телекомунікаційні компанії повинні будуть видалити компоненти, виготовлені Huawei та ZTE, з базових мереж до 1 січня 2026 року. Наразі не зрозуміло якими можуть бути видатки на масштабну заміну китайського обладнання – за деякими даними 60% мережевого обладнання 5G Німеччини походить від Huawei.

У ЗВІТІ GAO ЗАЗНАЧЕНО, ЩО NASA МАЄ ОНОВИТИ ПОЛІТИКУ ПРИДБАННЯ КОСМІЧНИХ АПАРАТІВ І СТАНДАРТИ КІБЕРБЕЗПЕКИ

Управління звітності уряду США (GAO) уважно вивчило практику NASA з кібербезпеки, виявивши потребу оновити політику придбання космічних апаратів. Хоча контракти NASA включають вимоги кібербезпеки, їм не вистачає послідовного впровадження. GAO рекомендувало розробити план із часовими рамками для інтеграції основних засобів контролю кіберзагроз, наголошуючи на важливості профілактичних заходів проти нових кіберзагроз. Крім того, GAO оцінило продукти CISA OT з кібербезпеки, зазначивши позитивний досвід, але підкресливши проблеми, з якими стикаються CISA та деякі не федеральні організації.

Крім того, президент Байден підписав Меморандум про національну безпеку для підвищення стійкості критичної інфраструктури, хоча космічний простір не був включений як сектор критичної інфраструктури. Це рішення викликало заклики до його розгляду через зростаючі загрози, при цьому експерти наголошували на необхідності надійних правил і основ для захисту космосу, враховуючи роль Космічних сил у захисті суспільства від потенційних ворогів.

СПОЛУЧЕНІ ШТАТИ ОПРИЛЮДНИЛИ СТРАТЕГІЮ ЩОДО МІЖНАРОДНОГО КІБЕРПРОСТОРУ ТА ЦИФРОВОЇ ПОЛІТИКИ

6 травня під час конференції в Сан-Франциско Державний департамент США оприлюднив Стратегію міжнародного кіберпростору та цифрової політики. Ця стратегія задає напрямки міжнародної технологічної дипломатії та посилює Стратегію національної безпеки та кібербезпеки США. Стратегія наголошує на «цифровій солідарності», виступаючи за спільні зусилля для створення безпечних і стійких цифрових екосистем, одночасно підтримуючи міжнародних партнерів. Стратегія базується на трьох принципах:

- безпечний та інклюзивний кіберпростір, заснований на міжнародному праві;
- інтеграція кібербезпеки зі сталим розвитком та інноваціями;
- комплексний політичний підхід із використанням дипломатії.

Чотири ключові дії включають сприяння стійкій цифровій екосистемі, узгодження цифрового управління з міжнародними партнерами, заохочення відповідальної поведінки держави в кіберпросторі та підвищення глобальної цифрової та кіберспроможності.

ПЕНТАГОН РОЗРОБЛЯЄ ПРОГРАМУ СТВОРЕННЯ ХМАРИ ДЛЯ ОБОРОННИХ ВІДОМСТВ

На початку травня IT-агентство Пентагону запустило програму під назвою DOD Olympus, щоб спростити оборонним організаціям процес створення власних хмарних рішень. Ця програма має на меті надати готовий комплект, який включає підключення до корпоративної мережі, загальні служби та інтегровані заходи безпеки, що полегшує створення хмарних середовищ для організацій, особливо з невеликою кількістю IT-персоналу. Olympus, який є відгалуженням контракту Joint Warfighting Cloud Capability, розроблено таким чином, щоб не залежати від послуг, і пропонує такі інструменти, як Vulcan для інтеграції DevSecOps. Платформа наразі перебуває в бета-версії, і її розширення планується на основі попиту клієнтів. Вона спрямована на підтримку розгортання гібридної хмари шляхом підключення до центрів обробки даних DISA.

CISA, DHS ТА ФБР СПІЛЬНО З МІЖНАРОДНИМИ ПАРТНЕРАМИ ОПУБЛІКУВАЛИ ПОСІБНИК ДЛЯ ОРГАНІЗАЦІЙ З ВИСОКИМ РІВНЕМ РИЗИКУ

14 травня CISA, DHS, ФБР у співпраці з кіберпартнерами з Канади, Естонії, Японії та Великобританії опублікували посібник «Подолання кіберзагроз з обмеженими ресурсами: Посібник для громадянського суспільства». Цей короткий посібник (10 сторінок рекомендацій) надає громадським організаціям рекомендації та засоби для зменшення ризиків кібератак, включаючи ті, що спонсоруються державою. Рекомендації містять в собі:

- впровадження стійкої до фішингу багатофакторної автентифікації (MFA);
- обережність при обміні інформацією в соціальних мережах;
- вибір постачальників, які дотримуються принципів Secure by Design;
- підвищення обізнаності про тактики соціальної інженерії.

NIST ОНОВИВ СВОЇ РЕКОМЕНДАЦІЇ SP 800-171/ 171A ЩОДО ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

14 травня NIST оприлюднив фінальні редакції SP 800-171 «Захист контрольованої несекретної інформації в не федеральних системах і організаціях» та SP 800-171A «Оцінка вимог безпеки для контрольованої некласифікованої інформації». Дотримання вимог обох документів є обов'язковим для організацій, що працюють з федеральними установами та обробляють їх інформацію. Також NIST 171 та NIST 171A є частиною моделі кіберзрілості CMMC, яку використовує Міністерство оборони США для своїх підрядників.

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

АНБ, CISA ТА ФБР СПІЛЬНО З ПАРТНЕРАМИ ПОВІДОМЛЯЮТЬ ПРО ЗРОСТАННЯ ЗАГРОЗ ОТ СИСТЕМАМ З БОКУ РОСІЙСЬКИХ ХАКЕРІВ

1 травня АНБ, CISA та ФБР разом з партнерами підготували інформаційний бюлетень «Захист операцій з відкритого доступу проти триваючої проросійської хактивістської діяльності» щодо активності проросійських хакерів проти пристроїв операційних технологій (ОТ). Звіт вказує на особливості російської активності проти ОТ систем – хактивісти компрометують системи відкритого доступу в північноамериканських і європейських водних системах, дамбах, енергетичному та харчовому секторах.

ЄС І ЯПОНІЯ ПОГЛИБЛЮЮТЬ СПІВПРАЦЮ, ЩОБ ЗАБЕЗПЕЧИТИ МІЦНІШІ ТА НАДІЙНІШІ ЛАНЦЮЖКИ ПОСТАЧАННЯ

2 травня ЄС та Японія зробили спільну заяву щодо посилення співпраці для більшої безпеки ланцюжків постачання Ця заява стала результатом 5-го Економічного діалогу високого рівня (HLED) між ЄС та Японією. Сторони підкреслили, що безпека ланцюжків постачання має охопити не лише технологічні процеси, але і кібербезпекову складову.

КРАЇНИ ЄС ТА АЛЬЯНС НАТО ОДНОСТАЙНО ЗАСУДИЛИ ЗЛОВМИСНУ КІБЕРАКТИВНІСТЬ РОСІЙСЬКОЇ APT28

3 травня уряд Німеччини публічно засудив APT28 кібератаку, яку угруповання здійснило проти політичної партії SPD. Під час атаки було використано вразливість Microsoft Outlook для витоку особистих даних. Того ж дня Міністерство закордонних справ (МЗС) Чехії так само публічно засудило дії російської групи APT28. Окремо НАТО також оприлюднив заяву про підтримку Німеччини, а також Європейський Союз та Велика Британія оприлюднили заяву, в якій засуджуються дії APT28. Ця скоординована відповідь НАТО відображає головне занепокоєння щодо кібершпигунської діяльності, яку проводить APT28. Ці занепокоєння зосереджені на втручанні у вибори та деструктивних атаках на сектори критичної інфраструктури.

ANNSI ТА BSI ПОНОВИЛИ СВОЮ УГОДУ ПРО ВЗАЄМНЕ ВИЗНАННЯ СЕРТИФІКАТІВ БЕЗПЕКИ CSPN-BSZ

15 травня керівники французької ANSSIA та німецької BSI оновили власну угоду від 2022 року, якою взаємно визнали сертифікати безпеки CSPN (Certification de Sécurité de Premier Niveau) та BSZ (Beschleunigte Sicherheitszertifizierung). Угода дозволяє взаємно визнавати сертифікати безпеки цього типу між Францією та Німеччиною, таким чином уникаючи дублювання оцінок. Ця угода також передбачає технічне співробітництво між двома агенціями з метою сприяння гармонізації практик та імплементації європейського законодавства щодо створення європейської схеми сертифікації.

СПІЛЬНА ОПЕРАЦІЯ ПРАВООХОРОННИХ ОРГАНІВ 13 КРАЇН ENDGAME ДОЗВОЛИЛА ЗНИЩИТИ КРИМІНАЛЬНУ ІНФРАСТРУКТУРУ ЦІЛОЇ НИЗКИ ЗЛОВМИСНИХ ГРУП

Між 27 та 29 травня спільна операція правоохоронних органів Франції, Німеччини, Нідерландів, Данії, Великобританії, Сполучених Штатів, України, Вірменії, Болгарії, Литви, Португалії, Румунії та Швейцарії (за підтримки майже 20 приватних компаній) дозволила ефективно атакувати інфраструктуру таких злочинних груп як IcedID, SystemBC, Pikabot, Smokeloader, Bumblebee і Trickbot. Це – найбільша в історії операція проти ботнетів, які відіграють важливу роль у розгортанні програм-вимагачів. За результатами операції: відбулось 4 арешти та 16 обшуків, виведено з ладу 100 серверів та взято під контроль 2000 доменів.

ПРЕДСТАВНИКИ КИТАЮ ТА США ПРОВЕЛИ ПЕРШИЙ ДІАЛОГ НА ВИЩОМУ РІВНІ ЩОДО ШТУЧНОГО ІНТЕЛЕКТУ

14 травня у Женеві відбулась перша зустріч з серії міжурядових діалогів щодо ШІ між президентом США Джо Байденом і президентом Китаю Сі Цзіньпіном. За словами речника Ради національної безпеки США, країни обговорили перспективи ШІ та наміри щодо дотримання правил безпеки ШІ. США висловили занепокоєння щодо зловживання технологією штучного інтелекту, тоді як Китай висловив занепокоєння з приводу суворої регулятивної та управлінської позиції США щодо ШІ.

ФРАНЦІЯ ЗАБОРОНИЛА TIKTOK НА ОСТРОВІ НОВА КАЛЕДОНІЯ

15 травня Уряд Франції оголосив про заборону TikTok на острові Нова Каледонія, щоб подолати масові заворушення на заморській території тихоокеанського острова. Прем'єр-міністр Франції Габріель Атталь заявив, що TikTok буде закрито в рамках надзвичайного стану, який включає розгортання армії та комендантську годину на острові, на якому мешкають приблизно 270 000 мешканців.

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

США ДЕМОНТУВАЛИ НАЙБІЛЬШИЙ У СВІТІ БОТНЕТ 911 S5, ЯКИЙ ВКЛЮЧАВ 19 МІЛЬЙОНІВ ЗАРАЖЕНИХ ПРИСТРОЇВ

30 травня Міністерство юстиції США заявило, що демонтувало «ймовірно, найбільший у світі ботнет», який складався з армії з 19 мільйонів заражених пристроїв, які були здані в оренду іншим суб'єктам загроз для вчинення широкого спектра злочинів. Ботнет, глобальний відбиток якого охоплює понад 190 країн, функціонував як домашній проксі-сервіс, відомий як 911 S5. 35-річний громадянин Китаю Юнь Хе Ван був заарештований у Сінгапурі 24 травня 2024 року за створення та роль головного адміністратора незаконної платформи з 2014 по липень 2022 року.

CISA НАДІСЛАЛА 2000 ПОВІДОМЛЕНЬ ПРИВАТНИМ КОМПАНІЯМ ЩОДО НАЯВНОСТІ ВРАЗЛИВОСТЕЙ В ЇХ СИСТЕМАХ

CISA активно просуває свою пілотну добровільну програму інформування організацій про наявність в їх мережах вразливостей – Cyber Hygiene. 9 травня стало відомо, що з моменту старту програми у січні 2024 року CISA понад 2000 разів надсилала повідомлення учасникам програми про наявність в їх системах відомих, але не виправлених вразливостей (CISA проводить сканування систем за допомогою програми Shodan, аналіз здійснюється на базі Known Exploited Vulnerabilities). В 49% випадків організації тим чи іншим чином відреагували на ці повідомлення та виправили вразливість. Наразі учасниками програми є понад 7000 організацій.

ПІВНІЧНОКОРЕЙСЬКІ ХАКЕРИ ВИКОРИСТОВУЮТЬ СЛАБКУ ПОЛІТИКУ БЕЗПЕКИ DMARC, ЩОБ ЗАМАСКУВАТИ ЗУСИЛЛЯ ЗІ СПАМ-ФІШИНГУ

2 травня АНБ, ФБР та Державний департамент США випустили Рекомендацію з кібербезпеки (CSA) «Північнокорейські актори використовують слабку політику безпеки DMARC, щоб замаскувати зусилля зі спам-фішингу». Метою документа є інформування стейкхолдерів про методи хакерів КНДР, які маскують електронні листи під легітимні повідомлення від журналістів, науковців чи експертів у справах Східної Азії. Звіт зазначає, що «фішинг є основою кіберпрограми КНДР». Звіт містить рекомендації щодо посилення політики DMARC, що може заблокувати зусилля хакерів КНДР.

РОСІЙСЬКІ ШПИГУНИ ТА КІБЕРЗЛОЧИНЦІ ПРОДОВЖУЮТЬ ВИКОРИСТОВУВАТИ БОТНЕТ, ЗЛАМАНИЙ ФБР

Ботнет, який використовувала пов'язана з російським гру APT28, складався не лише з роутерів Ubiquiti Edge OS, але також включав Raspberry Pi та інші пристрої Linux. В рамках операції з очищення після демонтажу ботнету з боку США в січні 2024 року, не вдалося повністю припинити доступ хакерів, оскільки на заражених пристроях залишалося додаткове невиявлене шкідливе ПЗ. Розслідування Trend Micro показало, що сотні маршрутизаторів Ubiquiti були перепрофільовані для різних зловмисних дій, таких як підбір SSH, спам і видобуток криптовалюти, причому деякі маршрутизатори, ймовірно, залишалися зараженими через юридичні обмеження. Крім того, оператори бот-мережі перемістили деяких ботів на нову інфраструктуру командування та контролю, включаючи понад 350 IP-адрес центрів обробки даних VPS. Крім APT28, інші учасники загрози, включно з угрупованням Canadian Pharmacy та зловмисниками, які використовують зловмисне ПЗ Ngioweb, також використовували заражені пристрої у незаконних цілях, підкреслюючи масштабний і багатогранний характер операцій ботнету.

НОВИЙ БОТНЕТ GOLDOON НАЦІЛЕНИЙ НА ПРИСТРОЇ D-LINK

1 травня компанія FortiGuard Labs повідомила, що у квітні помітила новий ботнет, націлений на вразливість D-Link, створену майже десять років тому, CVE-2015-2051. Ця вразливість дозволяє віддаленим зловмисникам виконувати довільні команди за допомогою дії GetDeviceSettings в інтерфейсі HNAP. У результаті зловмисник може створити створений HTTP-запит зі зловмисною командою, вбудованою в заголовок.

APT ГРУПА АТАКУВАЛА АМЕРИКАНСЬКИХ ДОСЛІДНИКІВ ШІ

16 травня кіберфахівці компанії Proofpoint розповіли про виявлену ними масштабну операцію невстановлених китайських зловмисників проти американських дослідників ШІ з академічного, приватного та державного секторів. Для своїх атак зловмисники використовують SugarGh0st RAT – троян віддаленого доступу.

КАТОЛИЦЬКА СИСТЕМА ОХОРОНИ ЗДОРОВ'Я ASCENSION ПОПЕРЕДЖАЄ ПРО ЗБОЇ В РОБОТІ ПІСЛЯ КІБЕРАТАКИ

8 травня одна з найбільших католицьких систем охорони здоров'я в США зіткнулася зі збоєм у своїй роботі після виявлення кібератаки.

Некомерційна організація Ascension, яка керує 140 лікарнями в 19 штатах, опублікувала повідомлення про виявлення незвичайної активності в мережевих системах і негайно почала розслідування, найнявши Mandiant і незабаром повідомивши про це правоохоронні органи. Ця атака стала ще однією в серії атак на компанії та організації у сфері охорони здоров'я, чия кібербезпека вже стала предметом пильної уваги після атаки вимагачів на UnitedHealth Group.

МЕРЕЖІ КАНАДСЬКОЇ ПРОВІНЦІЇ ПОСТРАЖДАЛИ ВІД «СКЛАДНИХ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ»

9 травня канадська провінція Британська Колумбія заявила, що виявила «складні інциденти кібербезпеки», що зачепили державні мережі. У своїй заяві прем'єр-міністр провінції Девід Ебі наголосив, що наразі немає доказів того, що була скомпрометована конфіденційна інформація. Розслідування тривають, і потрібна додаткова робота, «щоб визначити, до якої інформації міг бути доступ», сказав він. Хоча конкретна природа атаки не була з'ясована, її опис як «складної» разом з оголошенням про те, що вона стосувалася урядових мереж, швидше за все вказує на шпигунство з боку спонсорованого державою актора, який шукає політичних розвідданих.

ЗЛОМ СЛУЖБИ ШВИДКОЇ ДОПОМОГИ DOCGO РОЗКРИВ ДАНІ ПАЦІЄНТІВ

Хакери викрали особисті дані пацієнтів нью-йоркської служби швидкої допомоги DocGo, яка працює в 30 штатах США. Точна дата порушення не розголошується, але компанія заявила, що воно суттєво не вплинуло на операції чи фінансовий стан. Після злому DocGo локалізувала інцидент, розпочала розслідування за участю сторонніх експертів з кібербезпеки та повідомила правоохоронні органи. Порушення вплинуло на певну захищену медичну інформацію в бізнесі DocGo з надання швидкої допомоги в США, але не на інші бізнес-напрямки. Цей інцидент є частиною ширшої тенденції кібератак, націлених на медичні транспортні служби, з іншими помітними порушеннями, які зачіпають сотні тисяч людей.

ВЕЛИКА БРИТАНІЯ ПІДТВЕРДЖУЄ ВИТІК ДАНИХ БУХГАЛТЕРІЇ МІНІСТЕРСТВА ОБОРОНИ

7 травня уряд Великої Британії підтвердив нещодавню кібератаку на Міністерство оборони, під час якої зловмисники зламали частину платіжної мережі Збройних сил і розкрили особисті дані чинного та резервного персоналу, а також деяких ветеранів у відставці. Міністр оборони Грант Шеппс заявив, що Міністерство оборони швидко ізолювало скомпрометовану систему, відокремлену від основної мережі міністерства, якою керував підрядник. Порушення, яке вплинуло на приблизно 270 тисяч платіжних відомостей, включало імена, банківські реквізити та в деяких випадках адреси. Інцидент суттєво не вплинув на зарплати чи пенсії. Розслідування вказують на можливі помилки підрядника. І хоча крадіжка даних не підтверджена, персонал був поінформований про ризики. Підозрюється, що до атаки причетна інша держава, а ЗМІ повідомляють про причетність Китаю.

КИТАЙСЬКА APT ГРУПА ЗДІЙСНЮЄ КІБЕРШПИГУНСЬКУ ОПЕРАЦІЮ ПРОТИ КРАЇН БЛИЗЬКОГО СХОДУ, АФРИКИ ТА АЗІЇ

Фахівці кібербезпекової компанії PaloAltoNetworks 23 травня оприлюднили результати свого дослідження «Операція Diplomatic Spectre» щодо діяльності не визначеної китайської APT групи, що проводить масштабну кібершпигунську операцію проти урядових структур цілої низки країн. Її мета – збір конфіденційної та секретної інформації про дипломатичні та економічні місії, посольства, військові дії, політичні зустрічі, діяльність міністерств низки країн, а також високопосадовців цих країн. Для атак група використовує нове сімейство бекдорів TunnelSpecter і SweetSpecter (схожі за характером дії на Gh0st RAT).

НОВА СХЕМА СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ BLACK BASTA

Компанія ReliaQuest виявила, що група програм-вимагачів Black Basta проводить масову електронну розсилку спаму та голосового фішингу (вішингу) для розгортання програм-вимагачів. Атака починається, з того, що користувач отримує велику кількість спаму. Зловмисник імітує IT-підтримку, пропонуючи допомогу та інструктуючи користувача завантажити інструмент віддаленого доступу, який надає зловмиснику початковий доступ.

Компанія рекомендує організаціям проінформувати користувачів, щоб підвищити обізнаність про цю кампанію, запровадити правила прямого проксі-сервера, щоб блокувати нещодавно зареєстровані домени та налаштувати білий список застосунків лише для затверджених інструментів віддаленого моніторингу та керування (RMM).

БРИТАНСЬКА БІБЛІОТЕКА ВСЕ ЩЕ ВІДНОВЛЮЄТЬСЯ ПІСЛЯ АТАКИ RANSOMWARE У ЖОВТНІ МИНУЛОГО РОКУ

Британська бібліотека все ще намагається перебудувати свої технічні процеси після потужної кібератаки у жовтні 2023 року. Тоді хакерам вдалось викрасти близько 600 Тб інформації та знищити цілу низку серверної інфраструктури бібліотеки. Водночас у своєму виступі під час CyberUK 2024 генеральний директор Ролі Кітінг підкреслив, що ця кібератака стала причиною для глибинних змін в технічному переоснащенні бібліотеки, а також навчила її правильно комунікувати такі кіберінциденти. Хоча фізична спроможність надавати послуги відвідувачам не була порушена, однак і зараз майже не доступними залишаються численні дослідницькі сервіси, які традиційно надавала бібліотека.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

68 СВІТОВИХ ВИРОБНИКІВ ПЗ ДОБРОВІЛЬНО БУДУТЬ ДОТРИМУВАТИСЬ ВИМОГ SECURE BY DESIGN

8 травня CISA оголосило про те, що 68 провідних світових виробників програмного забезпечення добровільно взяли зобов'язання дотримуватись вимог Secure by Design (в тому числі Microsoft, GitHub, CrowdStrike, Trellix, Trend Micro). Виробники зобов'язуються дотримуватись семи конкретних цілей, які мають допомогти захистити критичну інфраструктуру США. Це містить в собі впровадження:

- багатофакторної автентифікації (MFA);
- встановлення паролі за замовчуванням;
- зменшення вразливостей; патчі безпеки;
- політику розкриття вразливостей;
- CVE;
- докази вторгнень.

CISA ЗАКЛИКАЄ ВИРОБНИКІВ ТЕХНІКИ ТА ПЗ ДО БІЛЬШОЇ ВІДПОВІДАЛЬНОСТІ ПЕРЕД СОЦІАЛЬНО ВАЖЛИВИМИ ОРГАНІЗАЦІЯМИ

9 травня заступник директора CISA Клейтон Романс оприлюднив свій заклик до розробників ПЗ та техніки надавати активну безкоштовну підтримку «багатим на цілі, але бідним на кібербезпеку організаціям» (Target-Rich, Cyber-Poor Organizations). Мова йде передусім про соціально важливі установи – школи, муніципалітети та некомерційні організації, які підтримують громадське життя. На думку Романса виробники повинні захистити ці організації, адже самі розробники не доклали достатньо зусиль для того, аби зробити свої продукти повністю безпечними.

ТРИ НАЙБІЛЬШІ БРИТАНСЬКІ АСОЦІАЦІЇ СТРАХОВИКІВ ОБ'ЄДНАЛИСЬ З БРИТАНСЬКИМ NCSC ДЛЯ ПРОТИДІЇ RANSOMWARE

14 травня NCSC повідомив, що розпочав спільну роботу з трьома найбільшими страховими асоціаціями Британії – Асоціацією британських страховиків (ABI), Британською асоціацією страхових брокерів (BIBA) і Міжнародною асоціацією андеррайтингу (IUA) – задля ефективнішої боротьби з виплатами викупу. Завдяки цій співпраці вже підготовлено «Посібник для організацій, які розглядають можливість оплати в інцидентах ransomware», в якому описані необхідні кроки, до яких мають вдатись жертви ransomware для того, щоб прийняти дійсно обґрунтоване рішення, якщо виникне потреба виплати викупу.

ФАХІВЦЯМ UNIT42 ВДАЛОСЬ НАВЧИТИ ШІ СТВОРЮВАТИ ДІЄВЕ ЗЛОВМИСНЕ ПЗ

15 травня два фахівці Unit42 з PaloAltoNetworks оприлюднили результати своїх практичних досліджень щодо можливості навчити ШІ створювати дієве зловмисне ПЗ. Основний результат полягає в тому, що ШІ не лише може це робити ефективно, але він також здатний генерувати величезну кількість схожих програм, але з відмінним кодом, імітувати діяльність іншого зловмисного ПЗ (приховуючи атакуючого), а також адаптувати його для різних платформ. Все це може перевантажити діяльність дослідників кібербезпеки та послабити захист організацій.

ЕКСПЕРИМЕНТАЛЬНИЙ ХРОБАК MORRIS II МОЖЕ ВИКОРИСТОВУВАТИ ПОПУЛЯРНІ СЛУЖБИ ШІ ДЛЯ КРАДІЖКИ ДАНИХ І ПОШИРЕННЯ ШКІДЛИВОГО ПЗ

У статті йдеться про те, що дослідники створили першого відомого черв'яка генеративного ШІ, здатного поширюватися через взаємопов'язані системи ШІ та потенційно сіяти хаос у величезних масштабах.

ЯК ШТУЧНИЙ ІНТЕЛЕКТ ЗМІНИТЬ КІБЕРОПЕРАЦІЇ

Як пише для видання War on the Rocks наукова співробітниця Центру безпеки та нових технологій Джорджтаунського університету Дженні Джун, Уряд США має суперечливі погляди на вплив ШІ на кібероперації, оптимістично дивлячись на його потенціал для захисту, але обережно ставлячись до його наступальних можливостей. Швидкий розвиток штучного інтелекту створює можливості та ризики для кібербезпеки, а інструменти за допомогою ШІ змінюють методи атак і вразливості. Обрамлення впливу ШІ виключно в термінах нападу та захисту занадто спрощує проблему, оскільки ШІ змінює розподіл цілей, які можна використовувати. Кіберстратегія США повинна адаптуватися для ефективного використання ШІ при одночасному усуненні нових ризиків, зосереджуючись на посередницьких факторах, що формують його використання в кібероперaціях відповідно до інтересів США.

5. КРИТИЧНА ІНФРАСТРУКТУРА

ГЕНЕРАЛЬНИЙ ДИРЕКТОР UNITEDHEALTH ПІДТВЕРДИВ, ЩО КОМПАНІЯ ЗАПЛАТИЛА ВИКУП У РОЗМІРІ 22 МІЛЬЙОНІВ ДОЛАРІВ

1 травня Генеральний директор UnitedHealth Group Ендрю Вітті мав відповісти на багато питань під час слухань у Сенаті про реакцію компанії на руйнівну атаку ransomware на Change Healthcare. Вітті вперше підтвердив попередню інформацію про те, що компанія заплатила викуп у розмірі 22 мільйонів доларів банді програм-вимагачів BlackCat/AlphV (Вітті підкреслив, що він особисто прийняв це рішення).

Недостатні заходи кібербезпеки UnitedHealth Group були виявлені після недавньої атаки програм-вимагачів на Change Healthcare. Це упущення в основному пояснюється сервером без багатофакторної автентифікації та повільнішою, ніж очікувалося, модернізацією технології. Атака призвела до розкриття величезної кількості даних пацієнтів, тому ця проблема вимагає більш надійних стандартів кібербезпеки в галузі охорони здоров'я. Згідно зі свідченням Вітті , банда програм-вимагачів BlackCat використовувала скомпрометовані облікові дані для віддаленого доступу до порталу Change Healthcare Citrix, який увімкнув віддалений доступ до робочого столу, 12 лютого. Портал не використовував багатофакторну автентифікацію.
Опитування Американської медичної асоціації показало, що чотири з п'яти клініцистів втратили дохід через поширений характер злому Change Healthcare, причому 77% зіткнулися з перебоями в обслуговуванні.

Change Healthcare також повідомила, що втратила 872 мільйони доларів через атаку та очікує, що збитки перевищать один мільярд доларів. Також американські сенатори звинувачують керівництво UnitedHealth в тому, що ними був призначений не кваліфікований CISO – у 2023 році на цю посаду був призначений Стівен Мартін, який ніколи не обіймав посад пов'язаних з кібербезпекою.

МІЛЬЙОНИ МОДЕМІВ CINTERION МІСТЯТЬ НЕБЕЗПЕЧНУ ВРАЗЛИВІСТЬ, ЯКА ДОЗВОЛЯЄ ВИКОНУВАТИ ВІДДАЛЕНІ КОМАНДИ ЗЛОВМИСНИКІВ

13 травня Лабораторія Касперського заявила про те, що знайшла вразливість CVE-2023-47610 (оцінка CVSS 9,8) у модемах Cinterion. Проблема полягає у можливості переповнення буфера, що своєю чергою може дозволити віддаленому зловмиснику виконати довільний код у цільовій системі, надіславши спеціально створене SMS-повідомлення. Модеми Cinterion використовуються в різних системах типу «машина-машина» (M2M) і IoT, включаючи промислову автоматизацію, телематику, інтелектуальне вимірювання та продукти моніторингу охорони здоров'я.

RHEINMETALL ПІДДАЄТЬСЯ ПОСТІЙНИМ КІБЕРАТАКАМ

14 травня головний фінансовий директор Rheinmetall Дагмар Штайнерт під час щорічних зборів акціонерів повідомив, що у квітні минулого року цивільний підрозділ компанії зазнав кібератаки, яка коштувала німецькому виробнику зброї 10 мільйонів євро. Також він відмітив, що компанія піддається постійним кібератакам, що ймовірно пов'язано із її особливою роллю у постачанні озброєнь для України.

70% СИСТЕМ ВОДОПОСТАЧАННЯ США МАЮТЬ КРИТИЧНІ КІБЕРВРАЗЛИВОСТІ

17 травня Агентство з охорони навколишнього середовища США (EPA) видало попередження, щоб окреслити заходи, до яких мають вдатись учасники сектору для захисту систем питної води від кіберзагроз. Перевірки, проведені EPA з вересня 2023 року, виявили, що понад 70% систем водопостачання не повністю відповідають Закону про безпечну питну воду. Перевірки виявили, що деякі системи мають критичні кібервразливості, включно з тими, що викликані використанням паролів за замовчуванням і систем автентифікації, які можна легко зламати. «Агентство збільшить кількість запланованих перевірок і, якщо це доцільно, вживатиме цивільних і кримінальних заходів», – заявили в EPA.

США ПОБОЮЮТЬСЯ, ЩО ПІДВОДНІ КАБЕЛІ ВРАЗЛИВІ ДО ШПИГУНСТВА З БОКУ КИТАЙСЬКИХ РЕМОНТНИХ КОРАБЛІВ

19 травня видання Wall Street Journal повідомило, що офіційні особи США попередили телекомунікаційні компанії про потенційні ризики для безпеки від китайських ремонтних суден, які працюють на підводних кабелях. Занепокоєння в основному викликає Центр SBSS, контрольована державою китайська компанія, чиї судна приховували своє місцеперебування, можливо, ставлячи під загрозу безпеку кабелів, які передають як комерційні, так і військові дані. Компанії з Кремнієвої долини, такі як Google і Meta, володіють багатьма з цих кабелів і покладаються на іноземні компанії для їх обслуговування. Зосередження уваги адміністрації Байдена на цих ризиках є частиною ширших зусиль протидії діяльності Китаю в західній частині Тихого океану. Попри запевнення, що прогалини в даних трекерів можуть бути спричинені технічними проблемами, США і надалі обережно ставляться до наслідків для безпеки від участі Китаю в ремонті кабелю. Речник МЗС Китаю Мао Нін назвав ці звинувачення «абсолютно безпідставними та такими, що являють собою недоброзичливе паплюження китайських компаній».

ROCKWELL AUTOMATION ЗАКЛИКАЄ КЛІЄНТІВ ВІДКЛЮЧИТИ ICS ВІД ІНТЕРНЕТУ

22 травня гігант промислової автоматизації Rockwell Automation попросив клієнтів вжити «негайних» заходів і перевірити, чи будь-які пристрої, які не призначені спеціально для публічного підключення, мають доступ до мережі Інтернет. В матеріалі Rockwell згадуються кілька серйозних вразливостей (знайдених і виправлених за останні роки), зокрема CVE-2021-22681, CVE-2022-1159, CVE-2023-3595 і CVE-2023-3596, CVE-2023-46290, CVE-2024-21914, CVE -2024-21915 і CVE-2024-21917. Експлуатація цих вразливостей може дозволити хакерам проводити DoS-атаки, підвищувати привілеї, змінювати налаштування і навіть проводити атаки у стилі Stuxnet.

АВСТРАЛІЯ ПОДАЛА ПОЗОВ ПРОТИ ОПЕРАТОРА OPTUS, ЯКИЙ ЗАЗНАВ МАСШТАБНОЇ КІБЕРАТАКИ У ВЕРЕСНІ 2022 РОКУ

22 травня Австралійський медіа-регулятор повідомив, що подає позов проти телекомунікаційного оператора Optus через кібератаку, з якою Optus зіткнувся у вересні 2022 року. У результаті інциденту була розкрита особиста інформація клієнтів, зокрема домашні адреси, паспорти та номера телефонів.

ЗЛАМ ПРИСТРОЇВ МОНІТОРИНГУ ПІДКРЕСЛЮЄ КІБЕРЗАГРОЗУ ІНФРАСТРУКТУРІ СОНЯЧНОЇ ЕНЕРГЕТИКИ

Японські ЗМІ нещодавно повідомили про те, що під час, можливо, першої публічно підтвердженої кібератаки на інфраструктуру сонячної електромережі зловмисники встановили контроль над 800 пристроями віддаленого моніторингу SolarView Compact, виготовленими виробником електроніки промислового керування Contec, на об'єктах виробництва сонячної енергії, щоб застосувати їх у крадіжках банківських рахунків. Атака привертає увагу до нової загрози кібербезпеці, що її становить швидко зростаючий сонячний компонент енергосистеми.

НЕВСТАНОВЛЕНІ ХАКЕРИ У ЖОВТНІ 2023 РОКУ ЗМОГЛИ ПОРУШИТИ ДОСТУП ДО ІНТЕРНЕТУ В НИЗЦІ ШТАТІВ СЕРЕДНЬОГО ЗАХОДУ США

30 травня дослідники кібербезпеки з Lumen Technologies розкрили деталі кібератаки невстановлених хакерів проти телекомунікаційного обладнання американських телекомоператорів у жовтні 2023 року. За даними Lumen Technologies кіберінцидент (про який досі не повідомлялось) вивів з ладу понад 600 тисяч інтернет-роутерів. Хакери встановили шкідливе програмне забезпечення, яке в період з 25 по 27 жовтня порушило доступ до Інтернету в багатьох штатах Середнього Заходу. Хоча жертва кібератаки прямо не вказується, але швидше за все мова йде про арканзаського інтернет-провайдера Windstream.

ФРАНЦУЗЬКА ЛІКАРНЯ CHC-SV ВІДМОВИЛАСЯ ПЛАТИТИ ВИКУП ВИМАГАЧАМ LOCKBIT

1 травня французька лікарня Hôpital de Cannes – Simone Veil (CHC-SV) повідомила, що отримала вимогу сплатити викуп від Lockbit 3.0. Атаку на лікарню було здійснено у квітні, і вона призвела до серйозних порушень у її роботі. Лікарня передала вимогу поліції та ANS-SI, і відмовилася від сплати, заявивши, що у разі злиття викрадених даних, попередить своїх клієнтів. Наступного дня стало відомо, що нападники оприлюднили інформацію, яку, за їх твердженням, вони викрали у лікарні.

6. АНАЛІТИЧНІ ОЦІНКИ

УРЯДОВІ СТРУКТУРИ США МАЙЖЕ НА 90% ВИКОНАЛИ УКАЗ ПРЕЗИДЕНТА США 14028 «ПОКРАЩЕННЯ КІБЕРБЕЗПЕКИ КРАЇНИ»

На початку травня Управління звітності уряду Сполучених Штатів оприлюднила оцінку стану виконання Указу Президента США від 2021 року № 14028 «Покращення кібербезпеки країни». Указ покладав на три державні структури – CISA, NIST та Офіс з управління та бюджету (OMB) – 55 задач, що мали сприяти поліпшенню кібербезпеки країни. Відповідно до оцінки Управління звітності США, було виконано 49 з 55 поставлених задач. Не виконані задачі стосуються: аналізу бюджетів витрат на досягненні цілей цього Указу Президента США, розробку та поширення серед урядових агенцій порядку закупки «критичного ПЗ», надання пропозицій щодо покращення управління сферою кібербезпеки, оцінку можливостей федеральних установ для впровадження EDR, забезпечення процесу обліку (журналювання) доступу.

ЛЮДСЬКИЙ ФАКТОР ЗАЛИШАЄТЬСЯ ДЖЕРЕЛОМ МАЙЖЕ 70% КІБЕРІНЦИДЕНТІВ – ЗВІТ VERIZON

17-й щорічний звіт Verizon Business досліджує майже 30 458 інцидентів безпеки, а також 10 626 підтверджених порушень у 2023 році. З проаналізованих порушень понад дві третини (68%) включали не зловмисний людський фактор – тобто інциденти пов'язані з інсайдерськими помилками або людьми, які потрапили на схеми соціальної інженерії. Цей відсоток залишається таким же, як і минулого року, що свідчить про те, що людський фактор залишається серйозною проблемою.

ВСЕ БІЛЬШЕ КОМПАНІЙ СТИКАЮТЬСЯ З АТАКАМИ ЧЕРЕЗ ЛАНЦЮЖКИ ПОСТАЧАННЯ ПЗ

У травневому звіті Ponemon Institute встановлено, що 59% організацій зазнавали атак на ланцюжок постачання програмного забезпечення, причому 54% із респондентів зазнали такої атаки протягом минулого року. Це опитування було проведено серед 1278 фахівців з IT та кібербезпеки, з яких майже половину становили менеджери, директори та керівники вищої ланки. З цих організацій 50% знадобилося понад місяць, щоб відреагувати на інцидент.

КОМПАНІЇ ГОТОВІ ПОВІДОМЛЯТИ ДЕРЖАВНІ ОРГАНИ ПРО ВИПАДКИ RANSOMWARE, АЛЕ НЕ ОТРИМУЮТЬ ЕФЕКТИВНОЇ ПІДТРИМКИ ВІД НИХ – ДОСЛІДЖЕННЯ SOPHOS

На початку травня кібербезпекова компанія Sophos провела дослідження за участі 2974 організацій, які постраждали від ransomware. Один з висновків дослідження – компанії, які повідомляють про інциденти, не отримують ефективної допомоги від державних структур, які були повідомлені про ситуацію. Так 100% компаній у Швейцарії повідомили урядові структури про такі інциденти, але допомогу отримали лише 49%. Ця ситуація характерна для майже всіх європейських країн – середній показник компаній, які отримали допомогу становить близько 55-57%. Значно краща ситуація у Близькосхідному регіоні: в Індії 70% отримали і поради, і допомогу з розслідуванням, у Сінгапурі цей показник становить 69%, а у Південній Африці – 68%.

КИТАЙ ЗАЛИШАЄТЬСЯ НАЙБІЛЬШ АКТИВНОЮ КІБЕРЗАГРОЗОЮ ДЛЯ США

2 травня було оприлюднено звіт національної розвідки США. Китай залишається найбільш активною кіберзагрозою для США. Нещодавно CISA виявила, що китайські кіберактори зосередилися на атаках критичної інфраструктури США. CISA повідомила, що виявила китайські вторгнення в авіаційному та енергетичному секторах, а також секторі водопостачання та телекомунікацій. Ключовими цілями атак є малі та середні підприємства, що надають критичні послуги.

КОНФЕРЕНЦІЯ RSAC 2024 БУЛИ МАЙЖЕ ПОВНІСТЮ ПРИСВЯЧЕНА ТЕМІ ШІ

З 6 по 9 травня у Сан-Франциско відбулась щорічна найбільша конференція з кібербезпеки RSA. В огляді заходу від Security Intelligence підкреслено, що майже весь захід був присвячений різним аспектом застосування ШІ у сфері кібербезпеки – як для захисту від кібератак, так і для зловмисного використання. Загалом цьому було присвячено понад 100 різних сесій, в тому числі проблематиці «тіньового IT» – використання персоналом компанії IT-рішень, які не були погоджені IT-підрозділами. Наразі ця проблема стає актуальною для використання співробітниками ChatGPT чи інших схожих моделей генеративного ШІ, коли дані компанії (часто – конфіденційні) можуть використовуватись співробітниками на сторонньому ресурсі.

АРГУМЕНТИ НА КОРИСТЬ МАЙБУТНІХ КІБЕРЗБРОЙНИХ СИЛ США

Поточний метод призначення персоналу для кібероперацій в армії США є неефективним і відрізняється між родами військ, що спричиняє проблеми з наймом, навчанням і утриманням. Система, що існує, подібна до ситуації, коли людина має невідповідну кваліфікацію для непов'язаних ролей, як-от коли капітан армії, який має лише кібердосвід, керує піхотною ротою, тобто кіберекспертиза в системі не відповідає потребам для виконання завдань. Пропоноване рішення полягає у створенні нового виду збройних сил, присвяченого кіберпростору. Це забезпечить цілеспрямований набір, навчання та утримання кваліфікованого кіберперсоналу, подібно до створення Космічних сил для космічних операцій. Ця нова гілка буде вирішувати унікальні вимоги та виклики створення кіберсил, якими існуючі служби не змогли адекватно керувати через конкуруючі пріоритети.

ОПЕРАЦІЇ ПРОГРАМ-ВИМАГАЧІВ СТАЮТЬ МЕНШ ПРИБУТКОВИМИ

Як пише видання HelpNetSecurity, платежі на користь операторів рансомвер зменшилися, попри збільшення кількості атак, завдяки покращенню кіберстійкості, діям правоохоронних органів і наявності дешифраторів. За даними фірми Chainalysis, що займається аналізом блокчейнів, у 2023 році кількість атак програм-вимагачів, пов'язаних із платежами, зменшилася на 46%. Зусилля правоохоронних органів, такі як збій роботи ботнету Qakbot у 2023 році та проникнення до LockBit у 2024 році, підірвали довіру та порушили діяльність у спільнотах програм-вимагачів. Крім того, афера з виходом групи ALPHV/BlackCat, яка раніше захопила 30% усіх платежів рансомвер, ще більше дестабілізувала екосистему програм-вимагачів. Ця тенденція відображає зростаюче небажання жертв платити викуп і підкреслює важливість постійних скоординованих зусиль між приватним сектором і правоохоронними органами для протидії загрозам програм-вимагачів.

74% CISO ВВАЖАЮТЬ, ЩО ЛЮДИ Є НАЙБІЛЬШОЮ ВРАЗЛИВІСТЮ ЇХНЬОЇ КОМПАНІЇ

21 травня Proofpoint поширив результати свого великого дослідження, що включало опитування 1600 CISO компаній, в яких є не менше 1000 співробітників. 74% CISO вважають, що людська помилка є найбільшою кібервразливістю для їх організацій. Показово, що цей показник істотно зріс у порівнянні з минулими опитуваннями: 60% у 2023 році та 56% у 2022 році. Також 86% опитаних вважають, що їхні співробітники розуміють свою роль у захисті бізнесу від кіберзагроз.

ОФІЦІЙНІ ОСОБИ США КАЖУТЬ, ЩО КИТАЙСЬКІ ОПЕРАЦІЇ НАЗАВЖДИ ЗМІНИЛИ ЛАНДШАФТ КІБЕРЗАГРОЗ

Попри зусилля з ліквідації китайської хакерської операції Volt Typhoon, яка проникла в критично важливу інфраструктуру США, федеральні чиновники визнають, що ця кампанія остаточно змінила ландшафт кіберзагроз. Зосереджений на дестабілізації та суспільній паніці, особливо під час конфліктів, Volt Typhoon уособлює перехід від традиційного шпигунства до більш зловісних намірів Пекіна. Кампанія була виявлена Microsoft і потрапила до кола уваги громадськості завдяки Міністерству юстиції. Вона використовувала домашні та офісні маршрутизатори, щоб надати уряду Китаю доступ до даних. ФБР і АНБ підкреслюють складність і наполегливість таких операцій, підкреслюючи підвищену вразливість через застарілі, але функціональні пристрої в мережах США.

ЗВІТ ESET ПРО ДІЯЛЬНІСТЬ APT ЗА ЧЕТВЕРТИЙ КВАРТАЛ 2023 – ПЕРШИЙ КВАРТАЛ 2024

У звіті ESET про діяльність APT за четвертий квартал 2023 – перший квартал 2024 підсумовуються помітні дії окремих APT груп, які були задокументовані дослідниками ESET з жовтня 2023 року до кінця березня 2024 року. Окреслені операції є репрезентативними для ширшого кола загроз, які досліджувала компанія протягом цього періоду та ілюструють ключові тенденції та розробки, і містять лише частину розвідувальних даних про кібербезпеку, наданих клієнтам приватних звітів ESET APT.

КИТАЙ МОЖЕ ГОТУВАТИ МАСШТАБНІ КІБЕРАТАКИ ПРОТИ ТАЙВАНЮ ЗАВДЯКИ ОТРИМАНИМ ДАНИМ ПРО ZERO-DAY ВРАЗЛИВОСТІ

29 травня фахівці Booz Allen Hamilton оприлюднили звіт «Розуміння китайської кіберстратегії щодо Тайваню», в якій дають опис як поточного ландшафту кіберзусиль КНР, так і можливих стратегічних задач, які переслідує КНР щодо Тайваню. Серед висновків аналітиків – Китай може використати накопичену інформацію завдяки законодавству 2021 року про розкриття інформації про нульовий день аби атакувати інформаційні системи Тайваню вразливостями нульового дня.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

НКЦК ПОСИЛЮЄ ВЗАЄМОДІЮ З КОНСУЛЬТАТИВНОЮ МІСІЄЮ ЄВРОПЕЙСЬКОГО СОЮЗУ

Секретар РНБО України Олександр Литвиненко 20 травня 2024 року зустрівся з Головою Консультативної місії Європейського Союзу Рольфом Холмбо. Під час зустрічі сторони обговорили співпрацю у підтримці загального процесу реформ в Україні на шляху до членства в ЄС, а також конкретні напрямки підтримки РНБО та безпекової архітектури України.
Розвиток кібербезпекових спроможностей є одним із важливих напрямів підтримки України з боку КМЄС. Одним із пріоритетів залишається практична взаємодія з Національним координаційним центром кібербезпеки задля ефективної розбудови національної системи кібербезпеки України та обміну досвідом з країнами ЄС.

ЗА СПРИЯННЯ НКЦК У КИЄВІ ВІДБУЛАСЬ ПЕРША НАУКОВО-ПРАКТИЧНА МІЖНАРОДНА КОНФЕРЕНЦІЯ З ПИТАНЬ КІБЕРДИПЛОМАТІЇ

Міністр закордонних справ України Дмитро Кулеба у своєму зверненні до підкреслив, що сучасна Україна вже закріпила в світі роль новатора і має шанс посісти провідне місце у світовому кіберпросторі. «Безперечно, це робить нашу державу невід'ємною частиною європейської та євроатлантичної систем безпеки».

Заступник Секретаря РНБО України Сергій Демедюк зазначив, що нещодавні офіційні заяви наших партнерів НАТО та ЄС щодо атрибутування кібератак до російських хакерів свідчать про усвідомлення міжнародної спільноти щодо злочинів рф, які вчиняються проти їхніх країн та населення. «Зараз необхідно разом будувати стратегії для прогнозованого та постійного посилення колективної кіберстійкості, що є важливим кроком у забезпеченні безпеки як на національному, так і на міжнародному рівні», – сказав він.

Під час заходу спікери визначили кібердипломатію як важливий інструмент для підтримки стабільності в кіберпросторі, обговорили необхідність його захисту та розглянули питання ролі штучного інтелекту в кібердипломатії, його впливу на ухвалення стратегічних рішень у міжнародних відносинах. Окрему увагу учасники заходу приділили дискусії щодо протидії російській дезінформації та інформаційній війні.

ЕСТОНІЯ ПЕРЕДАСТЬ УКРАЇНІ ЗАСОБИ ДЛЯ ПІДСИЛЕННЯ СПРОМОЖНОСТЕЙ У КІБЕРПРОСТОРІ В МЕЖАХ ІТ КОАЛІЦІЇ

Заступниця міністра оборони України Катерина Черногоренко зустрілась із заступником командувача Кіберкомандування Сил оборони Естонії Міхкелем Тікком та керівницею департаменту кіберполітики і координаторкою ІТ коаліції з боку Міністерства оборони Естонії Лаурою Оолуп у Києві. Сторони обговорили подальшу співпрацю щодо впровадження проєктів в межах коаліцій.

У межах візиту естонська делегація провела низку зустрічей з кіберфахівцями Міністерства оборони України та Збройних сил України. Партнери окремо відзначили професійність українських фахівців та підтвердили готовність і надалі надавати експертну допомогу з питань кібербезпеки.

НАТАЛІЯ ТКАЧУК ВЗЯЛА УЧАСТЬ У ЩОРІЧНІЙ ASIAN LEADERSHIP CONFERENCE

Керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України, секретар НКЦК Наталія Ткачук взяла участь у Asian Leadership Conference, що відбулася з 22 по 23 травня у Сеулі. Вона розповіла про досягнення України у розбудові національної системи кібербезпеки, поділилася унікальним досвідом із протидії кібератакам рф як складової повномасштабного військового вторгнення, наголосила на важливості міжнародної підтримки України та необхідності об'єднувати зусилля між державами для протидії кіберзагрозам.

«Україна та Південна Корея мають багато спільного: корейці пережили гіркий досвід війни, який нині переживає Україна, але спромоглися відновити країну, перетворивши її на одного з лідерів азійського регіону у сфері новітніх технологій та кібербезпеки. І для нас це приклад, що надихає. Аналогічна ціль стоїть і перед нашою державою й Україна вже має позитивні досягнення», – підкреслила Секретар НКЦК.

СЕРГІЙ ДЕМЕДЮК ЗАКЛИКАВ ДО ФОРМУВАННЯ НА МІЖНАРОДНОМУ РІВНІ ЄДИНОГО ПОНЯТІЙНОГО АПАРАТУ СФЕРИ КІБЕРОБОРОНИ

На міжнародному рівні слід формувати єдину термінологію ключових кібербезпекових понять. На цьому 30 травня під час засідання Національного кластера кібербезпеки акцентував заступник Секретаря РНБО України Сергій Демедюк. «Нам необхідно формувати єдину термінологію ключових кібербезпекових понять. російські хакери відкрито демонструють свої атаки на об'єкти критичної інфраструктури іноземних держав, втручаються у внутрішньополітичні процеси. А світ, на жаль, мовчить. Тож зараз нам потрібно ініційовувати процеси щодо формування певної ідеології щодо кібероборони під час війни».

Секретар НКЦК Наталія Ткачук наголосила на необхідності розбудови прозорої та дієвої національної нормативно-правової бази, зокрема й щодо проведення кібероперацій. Також у ході діалогу було обговорено питання щодо воєнних злочинів у кіберпросторі, зокрема, сучасні правові підходи та прогалини, механізми міжнародного стримування та реагування на воєнні дії в кіберпросторі, а також ключові потреби та рішення у секторі освіти та науки у сфері кібербезпеки.

ЗАСТУПНИК МІНІСТРА ЗАКОРДОННИХ СПРАВ АНТОН ДЕМЬОХІН ЗДІЙСНИВ РОБОЧИЙ ВІЗИТ ДО СПОЛУЧЕНИХ ШТАТІВ АМЕРИКИ

У травні заступник міністра закордонних справ з питань цифрового розвитку, цифрових трансформацій і цифровізації Антон Демьохін здійснив робочий візит до США. Виступаючи на конференції з кібербезпеки RSA 2024 у Сан-Франциско він підкреслив, що Україна перебуває в епіцентрі великої війни як у фізичному, так і кіберпросторі, що потребує максимального висвітлення на найбільших світових майданчиках. Також він взяв участь у Глобальному круглому столі ООН міністерського рівня зі зміцнення спроможностей у сфері кібербезпеки, провів низку двосторонніх та багатосторонніх зустрічей з іноземними партнерами з державного та приватного секторів, а також неурядових організацій. Крім того, український дипломат провів ряд двосторонніх зустрічей високопосадовцями Сінгапуру, США та представниками ООН та CRDF Global.

ФАХІВЦІ CERT-UA ВЗЯЛИ УЧАСТЬ В КОНФЕРЕНЦІЇ З КІБЕРБЕЗПЕКИ RSA 2024

Фахівець CERT-UA Назар Тимошик поділився зі світовою спільнотою експертів передовим українським досвідом протистояння російській агресії в кіберпросторі. У панельній дискусії про еволюцію кіберзагроз з боку росії протягом війни спікери обговорили нові тенденції та методи, які застосовують ворожі хакери. Він закликав учасників конференції використовувати досвід України для виявлення вразливостей своїх організацій до подібних загроз та розробки стратегій протистояння та захисту цифрових ресурсів.

УКРАЇНА ТА ПОЛЬЩА ПІДПИСАЛИ МЕМОРАНДУМ ПРО СПІВПРАЦЮ У СФЕРІ ЦИФРОВІЗАЦІЇ

Віцепрем'єр-міністр з розвитку інновацій, освіти, науки та технологій — Міністр цифрової трансформації Михайло Федоров та Віцепрем'єр-міністр — Міністр цифровізації Польщі Кшиштоф Гавковський підписали меморандум про співпрацю у сфері цифровізації. У фокусі спільної роботи Польщі та України — співпраця у сфері цифрових технологій та інновацій, розвиток IT-індустрії, штучного інтелекту, електронного урядування, розвитку Дії та mObywatel тощо. Також Віцепрем'єри обговорили підтримку у сфері захисту критичної інформації та державних реєстрів.

СБУ СПІЛЬНО З ФБР ТА ПАРТНЕРАМИ З ЄС ВИКРИЛА МІЖНАРОДНУ МЕРЕЖУ ХАКЕРІВ, ЯКІ РОЗРОБЛЯЛИ ВІРУСИ-ВИМАГАЧІ ДЛЯ АТАК НА АМЕРИКАНСЬКІ ТА ЄВРОПЕЙСЬКІ КОМПАНІЇ

Служба безпеки та ФБР спільно з правоохоронними органами Великої Британії та ЄС провели масштабну спецоперацію у 8 країнах Європи. У результаті спільних дій викрито понад 30 учасників транснаціональних хакерських угруповань, які займалися розробкою та розповсюдженням зловмисного програмного забезпечення, зокрема, «Pikabot», «System BC», «Bumblebee», «Smokeloader» та «IcedID».

За матеріалами міжнародного розслідування, зловмисники «зламували» мережі відомих компаній, а потім продавали доступ до цих мереж іншим хакерам. Серед них і російські угруповання «BlackBasta», «Revil» та «Conti». Задокументовано десятки фактів вимагання грошей з представників західних корпорацій на загальну суму в декілька десятків мільйонів доларів США. Паралельно у 8 країнах Євросоюзу та Північної Америки правоохоронці вилучили понад 90 серверів та заблокували понад 1000 доменів, які використовували хакери.

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ РОЗПОЧАЛО СПІВПРАЦЮ З ПРОГРАМОЮ РОЗВИТКУ ОБОРОННИХ СТАРТАПІВ DEFENCE BUILDER ACCELERATOR (DBA)

Мета співпраці — спільна допомога розробникам для створення технологічних рішень під запит Сил оборони і швидкої доставки їх на фронт. У межах програми Defence Builder Accelerator до 15 оборонних стартапів впродовж 4 місяців будуть створювати систему менеджменту команди, оформлювати юридичну та фінансову структуру, ефективніше залучати інвестиції. Також учасники акселератора отримають доступ до тестувань на полігоні та швидкий зворотний зв'язок щодо застосування своїх розробок з поля бою.

Участь у програмі братимуть розробники оборонних технологій, які вже мають мінімально життєздатний продукт (MPV) або прототип (TRL4) у напрямках БПЛА, наземних та водних роботизованих комплексів, кібербезпеки, сенсорів тощо.

В УКРАЇНІ ВІДБУВСЯ DIGITAL POWER SUMMIT 2024

Під час форуму, CDTO ОВА та цифрові лідери громад поспілкувалися з представниками уряду, обговорили пріоритетні проєкти 2024 року та які цифрові рішення можна ініціювати у своїх громадах та регіонах. Серед ключових тем – цифрові інструменти у освітній, медичній, соціальній та фінансовій сферах, цифрова економіка і цифрові послуги, кібербезпека та кіберстійкість, розвиток людського капіталу та державні програми для цього та естонський досвід із розвитку цифрової трансформації у малому місті.

ФАХІВЦІ ДЕРЖСПЕЦЗВ'ЯЗКУ ВЗЯЛИ УЧАСТЬ У 12-Й КОНФЕРЕНЦІЇ EU MITRE ATT&CK COMMUNITY WORKSHOPS

Фахівці Держспецзв'язку взяли участь у 12-й конференції EU MITRE ATT&CK Community Workshops, яка проходила 17 травня. Українські кіберзахисники виступили онлайн на одній сцені з фахівцями від Єврокомісії, корпорації MITRE, Центру Кібербезпеки Бельгії та Центру Протидії Кіберзагрозам Люксембургу. Ці центри заснували та активно розвивають платформу MISP, яка є де-факто стандартом обміну індикаторами про кібератаки як в Україні, так і в ЄС.

Участь у цій конференції також стала для Держспецзв'язку можливістю поділитися досвідом з іншими фахівцями з кібербезпеки з усього світу, дізнатися про останні тенденції щодо кіберзагроз і методів протидії їм та покращити свої навички використання MITRE ATT&CK для кіберзахисту України.

КІБЕРПОЛІЦЕЙСЬКИЙ ВЗЯВ УЧАСТЬ У ЗАСІДАННІ ФОРУМУ БЕЗПЕКИ РОЗРАХУНКІВ І КРЕДИТІВ

Фахівець Департаменту кіберполіції підполковник Олександр Ульяненков під час виступу на ФБРіК наголосив на важливості розвитку механізмів обміну інформацією між банківськими та платіжними установами для ефективної протидії шахрайству. «Впровадження нових технологічних рішень демонструє прагнення до інновацій та постійного вдосконалення методів боротьби з кіберзлочинністю», – сказав він.

На Форумі делегати від 39 організацій обговорили взаємодію між банківськими та платіжними установами на базі оновленої системи обміну інформацією між Департаментом кіберполіції, банківськими організаціями та ЄМА.

ДЕРЖСПЕЦЗВ'ЯЗКУ РОЗПОЧИНАЄ ЕКСПЕРИМЕНТАЛЬНИЙ ПРОЄКТ З ДЕКЛАРУВАННЯ ВІДПОВІДНОСТІ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Кабінет Міністрів України прийняв постанову «Про реалізацію експериментального проєкту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації». Координатором проєкту буде Державна служба спеціального зв'язку та захисту інформації України.

Мета проєкту – модернізувати процеси впровадження комплексної системи захисту інформації (КСЗІ) з використанням кращих світових стандартів безпеки, зокрема NIST 800-53 (США). Після закінчення експерименту Держспецзв'язку прозвітує Уряду про результати та запропонує внести відповідні зміни до законодавчих та інших нормативно-правових актів для підвищення рівня захисту державних інформаційних ресурсів та адаптації систем до нових кіберзагроз. Строк реалізації – до 2 років.

В УКРАЇНІ СТАРТУВАЛА ІНФОРМАЦІЙНА КАМПАНІЯ З ПЛАТІЖНОЇ БЕЗПЕКИ #КІБЕРБЕЗПЕКАФІНАНСІВ

Національний банк України разом з Державною службою спеціального зв'язку та захисту інформації України із 30 травня 2024 року розпочав Всеукраїнську інформаційну кампанію з платіжної безпеки #КібербезпекаФінансів. Її мета – поліпшити обізнаність громадян про платіжну безпеку та сформувати навички із захисту фінансових даних у віртуальному просторі.

Інформаційна кампанія триватиме до кінця вересня 2024 року у всіх регіонах України. В межах кампанії Національний банк запустив спеціальну вебсторінку (лендинг) «Кібербезпека фінансів» із детальною інформацією про кампанію та правила поведінки у віртуальному просторі.

ФАХІВЦІ CERT-UA ПІДГОТУВАЛИ АНАЛІТИЧНИЙ ЗВІТ «РОСІЙСЬКІ КІБЕРОПЕРАЦІЇ» H2 '2023

Фахівці команди CERT-UA підготували аналітичний звіт «російські кібероперації» H2 '2023. Цей звіт ґрунтується на всебічному аналізі кіберзагроз, виявлених протягом другого півріччя 2023 року, та розкриває нові тенденції в поведінці ворожих хакерів. Серед тенденцій другої половини 2023 року – підвищений інтерес ворожих хакерів до українського телекомунікаційного сектору. Це можна вважати певною ескалацією у спробах утримати ініціативу та присутність на українських об'єктах інформаційної інфраструктури. Більше – читайте в аналітичному звіті «російські кібероперації» H2'2023:

UA: https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=64621&embedded=true&a=bi

EN: https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=64622&embedded=true&a=bi

CERT-UA ПОПЕРЕДИЛА ПРО ЦІЛЕСПРЯМОВАНІ АТАКИ З ВИКОРИСТАННЯМ ПРОГРАМИ ВІДДАЛЕНОГО ДОСТУПУ SUPEROPS RMM

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA попередила про діяльність кіберзловмисників, які використовують легітимну програму для віддаленого управління комп'ютерами SuperOps RMM з метою отримання несанкціонованого доступу до інформаційних систем українських організацій.

Було зафіксовано та проаналізовано кібератаки, в ході яких жертвам надсилалися електронні листи з посиланням на Dropbox, де містився виконуваний файл (.SCR) розміром близько 33 МБ. При запуску цього файлу на комп'ютері жертви відбувається завантаження, декодування та виконання шкідливого Python-коду, який своєю чергою запускає легітимну програму SuperOps RMM. Це надавало зловмисникам несанкціонований віддалений доступ до комп'ютера жертви.

Подібні кібератаки здійснюються з лютого – березня 2024 року та мають доволі широку географію. Описаний кластер кіберзагроз відстежується за ідентифікатором UAC-0188.

CERT-UA ПОПЕРЕДЖАЄ ПРО ЗБІЛЬШЕННЯ КІЛЬКОСТІ КІБЕРАТАК ПРОТИ БУХГАЛТЕРІВ

CERT-UA попередила про значне зростання кількості кібератак, пов'язаних з діяльністю фінансово мотивованого угруповання UAC-0006. З 20 травня 2024 року фахівці зафіксували дві масштабні кампанії з розповсюдження шкідливого програмного забезпечення SMOKE-LOADER. Наразі бот-мережа UAC-0006 налічує декілька сотень заражених комп'ютерів. Існує висока ймовірність, що найближчим часом зловмисники активізують шахрайські схеми з використанням систем дистанційного банківського обслуговування.

КІБЕРПОЛІЦЕЙСЬКІ ВИКРИЛИ ШАХРАЯ, ЯКИЙ ОШУКАВ ВІЙСЬКОВОСЛУЖБОВЦЯ

Зловмисник отримав доступ до банківського рахунку військового та привласнив його гроші. Фігуранту повідомили про підозру, йому загрожує покарання у вигляді позбавлення волі на строк від 5 до 8 років. Слідчі дії тривають. Також поліцейські встановлюють й інших можливих потерпілих.

8. ПЕРША СВІТОВА КІБЕРВІЙНА

ВЕЛИКА БРИТАНІЯ СПІЛЬНО З СОЮЗНИКАМИ ВИКРИЛИ ОСОБУ РОСІЙСЬКОГО ЛІДЕРА КІБЕРЗЛОЧИННОЇ ГРУПИ LOCKBIT

7 травня Великобританія, США та Австралія викрили та ввели санкції проти російського лідера кіберзлочинної групи LockBit Дмитра Хорошева. Будь-які його активи будуть заморожені, а поїздки – заборонені. Також було оголошено винагороду у 10 млн доларів за інформацію, що призведе до затримання злочинця.

НА MONOBANK ЗДІЙСНЕНО ПОТУЖНУ DDOS-АТАКУ

1 травня у застосунку Монобанку виникали проблеми із доступом. Наступного дня його співзасновник Олег Гороховський повідомив, що на банк було здійснено потужну DDoS-атаку.

У 2024 РОЦІ РОСІЙСЬКА КІБЕРЗАГРОЗА ДЕМОНСТРУЄ НОВИЙ РІВЕНЬ АГРЕСІЇ ТА МАНЕВРЕНОСТІ – НАЦІОНАЛЬНИЙ КІБЕРДИРЕКТОР США Г. КОКЕР

14 травня Національний кібердиректор США Гаррі Кокер, виступаючи CYBERUK 2024 підкреслив, що «розвиток цифрової солідарності є ключовим елементом кібербезпеки, оскільки кіберзагрози стають дедалі серйознішими». Виразним прикладом, на його думку, є Україна, яка з 2022 року успішно протистоїть російським кібератакам на критичну інфраструктуру. Однак російська загроза еволюціонує: «у 2024 році кіберзагрози з боку росії демонструють новий рівень агресії та маневреності. Відтак підвищення безпеки мереж та комунікацій є критичним для успіху України на полі бою».

ЗАЯВА ПІВНІЧНОАТЛАНТИЧНОЇ РАДИ ЩОДО НЕЩОДАВНЬОЇ ГІБРИДНОЇ ДІЯЛЬНОСТІ РОСІЇ

На початку травня НАТО та ЄС забили на сполох через російських хакерів і гібридну діяльність, яка зачепила принаймні сім країн Європи. Йшлося про дії, які стосувалися пов'язаних з росією акторів, які брали участь у різних «диверсіях, актах насильства, кібервтручанні, кампаніях з дезінформації та інших гібридних операціях» у Чехії, Естонії, Німеччині, Латвії, Литві, Польщі та Великобританії.

Як результат, 2 травня НАТО видав заяву, в якій наголошується, що «Дії росії не перешкодять членам Альянсу продовжувати підтримувати Україну». «Ми засуджуємо поведінку росії», – йдеться в заяві та додається: «Ми діятимемо індивідуально та колективно, щоб протистояти цим діям, і продовжуватимемо тісно координувати свою роботу».

УРЯД КОСОВА СТИКНУВСЯ З КІБЕРАТАКАМИ, ЯКІ ПІДТРИМУЄ КРЕМЛЬ

Нещодавно російські хакери атакували державні вебсайти в Косово. Станом на 10 травня кілька вебсайтів були тимчасово недоступні через розповсюджений інцидент відмови в обслуговуванні. «Атака була здійснена російськими хакерами у відповідь за нашу підтримку України військовою технікою», — заявив речник уряду місцевим ЗМІ.

РОСІЙСЬКА ГРУПА FLYINGYETI НАМАГАЛАСЬ АТАКУВАТИ УКРАЇНСЬКИХ ГРОМАДЯН

31 травня безпекова команда сервісу Cloudflare повідомила, що зупинила спробу проведення масштабної атаки російським угрупуванням FlyingYeti проти українських користувачів. Хоча традиційно атаки цієї групи спрямовані проти сил оборони України, однак цього разу у фокусі уваги були громадяни, які відчувають фінансові складнощі та покладаються на соціальні виплати від держави. Для фішингової атаки, яка планувалась групою з січня 2024 року, планувалось використати фішинговий сайт на GitHub та ресурси Cloudflare Worker.

9 ТРАВНЯ УКРАЇНСЬКІ ТА РОСІЙСЬКІ ХАКЕРИ ОБМІНЯЛИСЯ АТАКАМИ НА ТЕЛЕБАЧЕННЯ

Під час святкування Дня перемоги 9 травня, що є одним з найбільших пропагандистських свят у рф, російські видання повідомили, що невідомі хакери зламали ефір телепровайдера «Уфанет» в Башкортостані та Оренбурзькій, Омській й Іркутській областях. Замість параду на красній площі глядачам показували кадри пов'язані з війною в Україні. росіяни своєю чергою зламали супутниковий ефір каналів групи StarLightMedia та «Інтер» в Україні та запустили трансляцію параду в москві на красній площі.

ПІДТРИМУВАНИЙ КРЕМЛЕМ APT28 НАЦІЛЕНИЙ НА ПОЛЬСЬКІ ІНСТИТУЦІЇ У МАСШТАБНІЙ КАМПАНІЇ ШКІДЛИВИХ ПРОГРАМ

8 травня польська команда реагування на комп'ютерні надзвичайні ситуації CERT Polska повідомила, що спостерігала масштабну кампанію зловмисного програмного забезпечення, спрямовану на державні установи Польщі. На основі технічних показників і схожості з атаками, описаними в минулому (наприклад, на українські організації), кампанію можна пов'язати з APT28, який пов'язаний з гру рф. Мета атаки – збір інформації.

РОСІЙСЬКІ ХАКЕРИ ОТРИМАЛИ ДОСТУП ДО САЙТУ ПОЛЬСЬКОГО АГЕНТСТВА ПРЕСИ (PAP) І РОЗМІСТИЛИ ТАМ ФЕЙКОВУ СТАТТЮ

28 травня на сайті Польського агентства преси (PAP) з'явилась стаття про те, що поляки будуть мобілізовані для боротьби в Україні. У статті стверджувалося, що Туск планує оголосити часткову військову мобілізацію 1 липня: «Двісті тисяч польських громадян, як колишніх військових, так і штатних цивільних, будуть призвані на обов'язкову військову службу. Всі призвані будуть відправлені в Україну», – йшлось у статті. PAP видалило статтю через кілька хвилин після її публікації, додавши, що «джерело тексту не є Польське агентство преси». Потім стаття з'явилася вдруге, а потім знову була видалена. 31 травня польський уряд заявив, що поява цього матеріалу, ймовірно, є російською кібератакою.

РОСІЯ ДЕДАЛІ ЧАСТІШЕ ПЕРЕШКОДЖАЄ УКРАЇНІ У ВИКОРИСТАННІ ПОСЛУГ STARLINK

Як пише видання New York Times, росія застосовує передову технологію для втручання в роботу супутникового інтернет-сервісу Ілона Маска Starlink. Це призвело до нових збоїв у роботі сервісу на північній лінії фронту. Starlink був критично важливим для української армії з перших днів війни з росією, адже за його допомогою вони можуть швидко спілкуватися та ділитися інформацією про несподіваний наступ та обмінюватися повідомленнями. Погіршення якості сервісу Starlink становлять серйозну загрозу для України, якій часто вдавалося перехитрити російську армію за допомогою передового зв'язку та інших технологій, але вона тримала оборону проти нового просування росії.

ФАЙЛ НЕ ЗНАЙДЕНО: РОСІЯ ЛАМАЄ ДОКАЗИ СВОЇХ ВОЄННИХ ЗЛОЧИНІВ

Як пише видання War on the Rocks, поки війна в Україні триває, президент росії владімір путін використовує кібервійну, щоб переписати історію конфлікту та уникнути післявоєнного правосуддя. російські хакери атакують українські бази даних і бази даних Міжнародного кримінального суду, щоб модифікувати або видалити докази воєнних злочинів. Ця тактика спрямована на те, щоб допомогти російським злочинцям уникнути судового переслідування, що відображає ширшу стратегію росії щодо використання кібератак для приховування своїх звірств. Цифрова маніпуляція доказами воєнних злочинів, у тому числі потенційне використання дипфейків, ускладнює прагнення до справедливості. Щоб протистояти цьому, посилені заходи кібербезпеки, покращене збереження доказів компаніями соціальних мереж і проактивне запобігання кіберзломам мають вирішальне значення для забезпечення підзвітності та доброчесності в трибуналах щодо воєнних злочинів.

«РОСІЙСЬКІ» ХАКЕРИ ЗІПСУВАЛИ СОТНІ МІСЦЕВИХ БРИТАНСЬКИХ НОВИННИХ САЙТІВ

11 травня група, яка оголошує себе «першокласними російськими хакерами», зіпсувала сотні вебсайтів місцевих і регіональних британських газет. На сайтах видань, що належать Newsquest Media Group, група опублікувала екстрену новину під назвою «ПЕРВОКЛАССНАЯ АТАКА РОСІЙСЬКИХ ХАКЕРІВ». Те, що постраждало так багато заголовків Newsquest, свідчить про те, що центральна або спільна система керування вмістом могла бути зламана, але зараз немає жодних доказів того, що хакери насправді були росіянами.

РОСІЙСЬКІ АКТОРИ ВИКОРИСТОВУЮТЬ ЗАКОННІ СЕРВІСИ ДЛЯ АТАКИ З КІЛЬКОМА ШКІДЛИВИМИ ПРОГРАМАМИ

Як повідомляє Recorded Future, в рамках нової кіберкампанії російськомовні актори зловживали легальними інтернет-сервісами, такими як GitHub і FileZilla, для розгортання кількох варіантів шкідливого ПЗ. Серед іншого, йдеться про розгортання Atomic macOS Stealer (AMOS), поточна версія якого здатна заразити Mac як на базі Intel, так і на базі ARM. Ця кампанія є унікальною, частково через кількість різних сімейств зловмисного ПЗ, а також залежність зловмисника від легальних інтернет-сервісів і спільної інфраструктури C2.

BLUEDELTA ВІД ГРУ НАЦІЛЕНА НА КЛЮЧОВІ МЕРЕЖІ В ЄВРОПІ В РАМКАХ БАГАТОСТУПЕНЕВИХ ШПИГУНСЬКИХ КАМПАНІЙ

Insikt Group відстежує розвиток операційної інфраструктури BlueDelta гру, що націлюється на мережі по всій Європі за допомогою зловмисного ПЗ Headlace для викрадення інформації і вебсторінок, які збирають облікові дані. BlueDelta розгортала інфраструктуру Headlace у три окремі етапи з квітня по грудень 2023 року, використовуючи фішинг, скомпрометовані інтернет-сервіси та живучи завдяки використанню наземних двійкових файлів для отримання інформації. Сторінки збору облікових даних були націлені на Міністерство оборони України, європейську транспортну інфраструктуру та азербайджанський аналітичний центр, відображаючи ширшу російську стратегію впливу на регіональну та військову динаміку.

9. РІЗНЕ

ПІВНІЧНІЙ КОРЕЇ ВДАЛОСЬ ВІДМИТИ 147,5 МЛН ДОЛАРІВ У КРИПТОВАЛЮТІ

14 травня були повідомлені окремі деталі закритого звіту спостерігачів ООН, що опікуються питанням дотримання санкцій. За їх даними, уряду Північної Кореї вдалось через платформу віртуальної валюти Tornado Cash відмити 147,5 млн доларів. У 2022 році США ввели санкції проти Tornado Cash через звинувачення в підтримці Північної Кореї. У 2023 році двох співзасновників звинуватили у сприянні відмиванню грошей на суму понад один мільярд доларів США, зокрема для кіберзлочинної групи, пов'язаної з Північною Кореєю. Всього ж за період 2017-2024 Північна Корея вкрала криптоактивів на суму 3,6 млрд доларів.

HORIZON3.AI ПРЕДСТАВЛЯЄ СЕРВІС З ПІДТРИМКОЮ ШІ ДЛЯ ПРИШВИДШЕННЯ ВИЗНАЧЕННЯ ПРІОРИТЕТІВ І ВИПРАВЛЕННЯ ВРАЗЛИВОСТЕЙ

Компанія Horizon3.ai представила службу швидкого реагування на своїй платформі тестування на проникнення на основі NodeZero SaaS, яка має на меті проактивно запобігати зловмисним атакам, шляхом швидкого усунення критичних вразливостей, виявлених в IT-середовищах. Сервіс поєднує досвід ШІ та людей, щоб швидко оцінювати та визначати пріоритети вразливостей, окрім тих, що перераховані NVD, автоматично перевіряючи на можливість використання. Використовуючи штучний інтелект для швидкості аналізу та людське мислення для оцінки критичності, платформа Horizon3 виявляє вразливості та розробляє безпечні експлойти, забезпечуючи автономне виконання для перевірки можливості використання. З акцентом на швидке реагування, сервіс надає організаціям корисну інформацію для ефективного захисту своєї інфраструктури.