НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

УКРАЇНСЬКА ФУНДАЦІЯ БЕЗПЕКОВИХ СТУДІЙ

CYBER DIGEST

Огляд подій в сфері кібербезпеки,
липень 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

Ключовою подією липня став кіберінцидент навколо продукту компанії CrowdStrike. Через недостатнє тестування чергового оновлення продукту виник supply chain інцидент, що вплинув на понад половину компаній зі списку Fortune 500. Проблеми виникли в лікарнях, були скасовані авіарейси по всьому світу – загалом інцидент стосувався 8,5 млн Windows-пристроїв (пристрої на Apple та Linux не постраждали). Реакція постраждалих компаній (Delta Air Lines) та країн (Малайзія) вже спрямована на відшкодування збитків від компаній CrowdStrike або Microsoft або від страхових установ, але перспектива цього залишається невизначеною. Ймовірним довгостроковим наслідком інциденту стане чіткіше формулювання розділів про відповідальність у контрактах з кібербезпековими хмарними організаціями та посилення регуляції хмарних сервісів з боку держав. Це доповнює процеси в ЄС, де окремі сектори, такі як аерокосмічний та оборонний, прагнуть більшого контролю за постачальниками сервісів, наполягаючи на збереженні даних європейських користувачів в межах ЄС.

США розширюють обов'язкові вимоги кібербезпеки для науково-дослідних організацій, що фінансуються федеральним бюджетом. Останній меморандум Офісу національного кібердиректора (ONCD) зобов'язує державні агентства прискорити перехід до архітектури Zero Trust, надавши стратегію протягом 120 днів, і впровадити квантово-стійке шифрування. Це доповнюється ініціативами, які передбачають розширення доступу кіберфахівців у державному секторі, зокрема шляхом зняття обмежень на посади залежно від наявності диплома про освіту.

Великобританія підтримує європейські тенденції посилення кібервимог для державного та приватного секторів. Країна готується до прийняття закону про кібербезпеку та стійкість, що зосереджуватиметься на захисті критичної інфраструктури, збільшенні повноважень регуляційних органів, посиленні звітності та запровадженні штрафів та пені для організацій, які не дотримуються встановлених стандартів кібербезпеки. Це відбувається на тлі виявлення фактів вкрай слабкої системи кібербезпеки у деяких державних інституціях, таких як Виборча комісія Великобританії, яка мала вкрай слабкі політики кіберзахисту, що дозволило зловмисникам отримати доступ до даних 40 млн британців.

Україна продовжує зміцнювати міжнародну співпрацю в галузі кібербезпеки, інтегрується до західних інституцій та ділиться своїм досвідом протистояння російській агресії у кіберпросторі. Під час третього раунду Кібердіалогу Україна-ЄС було досягнуто домовленості про поглиблення співпраці. Українська делегація поділилася досвідом протистояння кіберагресії рф та надала рекомендації партнерам щодо посилення національної кібербезпеки під час зустрічі з послами Європейського Союзу Комітету з питань політики та безпеки у Брюсселі. Фахівці Держспецзв'язку поділились досвідом протистояння кіберзагрозам на USA-Ukraine Cyber Bridge та конференції Hack the Capitol у США. IT-коаліція передала Україні мережеве обладнання та ліцензії, що підсилять потужність центрів обробки даних та кіберзахисту Міністерства оборони та Збройних сил України.

Для посилення кіберстійкості регіонів НКЦК організував перший Regional Cyber Resilience Forum у Львові, який зібрав близько 400 учасників. Мінцифра та Офіс з розвитку підприємництва та експорту запустили програму з кібердіагностики, метою якої є допомога 500 українським компаніям перевірити цифрову інфраструктуру компанії на вразливості. НКЦК, Мінветеранів та CRDF Global втретє провели навчання ветеранів за програмою реінтеграції ветеранів «Кіберзахисники», надаючи їм знання та навички у сфері кібероборони та кіберзахисту для працевлаштування у державному та приватному секторах. Держспецзв'язку також провела освітні заходи для фахівців, відповідальних за кібербезпеку в держсекторі та ОКІ.

Цього місяця кібербезпекові компанії зосередили увагу на діяльності китайської APT41. Компанія Zscaler опублікувала технічний звіт про особливості діяльності цього угрупування, Mandiant попередила про спроби APT41 проникнути в глобальний транспортний і технічний сектори, а Cisco Talos виявила зловмисну кампанію APT41, що скомпрометувала тайванський урядовий науково-дослідний інститут. Також західні кібербезпекові органи звернули увагу на діяльність APT40 (АНБ США разом з партнерами з Австралії опублікували щодо цього окреме дослідження), пов'язану зі спецслужбами КНР.

Перша світова кібервійна активно розширює ареал залучених учасників і перетворюється на глобальне, майже відкрите кіберпротиборство. В цьому протиборстві вектор наступальних заходів російських зловмисників залишається одним з ключових. В червні злам програми TeamViewer атрибутували російському угрупованню APT29. російські хакери посилили атаки на фінські сайти, зокрема група NoName здійснила численні DoS-атаки, а коаліція хакерів High Society планує атаки на НАТО, Європу, Україну та Ізраїль. Водночас західний світ активно протидіє російській кіберактивності. У липні США ліквідували російську ботоферму на основі ШІ, ввели обмеження на діяльність антивіруса «Касперського», запровадили санкції проти російських хакерів з угруповання CARR, а в Австралії затримали подружжя за підозрою в шпигунстві на користь росії. Також українська військова розвідка разом із кіберволонтерами атакувала майже сотню російських вебресурсів, а нова APT група CloudSorcerer була помічена у спробах націлитись на російські державні установи, використовуючи хмарні служби для C2 та викрадання даних.

Напруженість між Китаєм і Заходом зростає. Сторони активно обмінюються звинуваченнями у деструктивній діяльності в кіберпросторі. Німеччина звинуватила Китай у кібератаці на німецьке картографічне агентство у 2021 році, що призвело до прискорення процесів вилучення обладнання Huawei та ZTE зі своїх мереж 5G. Китай, своєю чергою, звинувачує західні країни у дезінформаційних кампаніях щодо себе, стверджуючи, що історія навколо діяльності кіберугрупування Vault Typhoon, це результат спланованої операції АНБ США, ФБР та інших американських відомств за участі розвідувальних служб країн «П’яти очей».

1. ПОДІЯ МІСЯЦЯ - КІБЕРІНЦИДЕНТ З CROWDSTRIKE

ОНОВЛЕННЯ CROWDSTRIKE, ЯКЕ ПРИЗВЕЛО ДО ГЛОБАЛЬНОГО ЗБОЮ В РОБОТІ МЕРЕЖІ, ВІРОГІДНО НЕ ПРОЙШЛО ПЕРЕВІРКУ

Звичайне оновлення широко використовуваного безпекового ПЗ від CrowdStrike, яке спричинило глобальний збій комп'ютерних систем клієнтів 19 липня, очевидно, не пройшло перевірку якості перед розгортанням. Подібні інциденти траплялися і раніше, зокрема, оновлення антивірусу McAfee у 2010 році зупинило роботу сотень тисяч комп'ютерів.

Глобальний вплив цього збою підкреслює домінування CrowdStrike: понад половина компаній зі списку Fortune 500 та багато державних органів, включно з головним агентством з кібербезпеки США та Агентством з кібербезпеки та безпеки інфраструктури, використовують програмне забезпечення компанії.

НЕВДАЛЕ ОНОВЛЕННЯ ПЗ, ЯКЕ ВІДЧУЛИ У ВСЬОМУ СВІТІ, ПІДКРЕСЛЮЄ НЕОБХІДНІСТЬ БІЛЬШОЇ ДИВЕРСИФІКАЦІЇ

Нещодавній серйозний збій у роботі IT вплинув на світову спільноту не через геополітичні конфлікти чи ворожі кібератаки, а через несправне оновлення програмного забезпечення від провідної американської кібербезпекової фірми CrowdStrike. Дефект спричинив масові збої, включаючи «синій екран смерті» у клієнтів по всьому світу, в тому числі у державних служб, авіакомпаній, лікарень та банків. Це призвело до затримки або скасування майже 3000 рейсів у США. Кіберзлочинці швидко використали ситуацію, застосовуючи шахрайство та зловмисне програмне забезпечення, посиливши наслідки.

Інцидент підкреслив ризики глобальної залежності від кількох постачальників технологій, порівнюючи його зі зломом SolarWinds у 2020 році, та наголосив на необхідності різноманітних рішень безпеки. Хоч CrowdStrike отримав похвалу за прозорість, ця подія виявила ширші вразливості в ландшафті кібербезпеці, спонукаючи заклики до законодавчих дій і переоцінку практик безпеки. Збитки від збою CrowdStrike оцінюються в приголомшливі 5,4 мільярда доларів.

ВІРУС-СТИРАЧ HANDALA, КОРИСТУЮЧИСЬ ІНЦИДЕНТОМ З CROWDSTRIKE, НАЦІЛИВСЯ НА ІЗРАЇЛЬСЬКІ ОРГАНІЗАЦІЇ

26 липня фахівці компанії Trellix повідомили про виявлений вірус-стирач Handala, спрямований невідомою хакерською групою на ізраїльські організації або ті, що взаємодіють з ними. Ланцюжок атак починається з електронного листа жертві на тему CrowdStrike, в якому йдеться про збій та пропонується «виправлення». У вкладеному PDF-файлі міститься посилання для завантаження «виправлення збою», яке запускає вірус. Наразі надійну атрибуцію зловмисної групи не проведено.

CROWDSTRIKE ВІДМІЧАЄ ПІДВИЩЕНУ АКТИВНІСТЬ ХАКЕРСЬКИХ ГРУП НА ФОНІ КІБЕРІНЦИДЕНТУ З FALCON

Протягом липня фахівці CrowdStrike відстежували підвищену активність різних хакерських груп, пов'язану з кіберінцидентом, який стався з Falcon – одним із продуктів компанії. Одним із таких прикладів стала активність неатрибутованої групи, яка 24 липня 2024 року під час спроби фішингової атаки проти однієї з німецьких організацій розповсюдила захищений паролем інсталятор під виглядом фальшивого Falcon Crash Reporter.

МАЛАЙЗІЯ ЗВЕРНУЛАСЬ ДО MICROSOFT І CROWDSTRIKE ЩОДО МОЖЛИВОСТІ ПОКРИТТЯ ЗБИТКІВ ВІД ГЛОБАЛЬНОГО ЗБОЮ

24 липня Міністр цифрових технологій Малайзії звернувся до компаній Microsoft та CrowdStrike з проханням розглянути можливість компенсації малайзійським компаніям, які зазнали збитків під час глобального технічного збою.

КІБЕРІНЦИДЕНТ ЗІ CROWDSTRIKE ПРИЗВЕДЕ ДО НОВОГО ВИТКУ ДИСКУСІЇ ПРО КРИТИЧНІСТЬ ХМАРНИХ СЕРВІСІВ ТА ВІДПОВІДАЛЬНОСТІ СТОРІН ПІД ЧАС ІНЦИДЕНТІВ – ЕКСПЕРТ CSIS

У своєму матеріалі від 25 липня експерт аналітичного центру CSIS Дж. Льюіс аналізує можливі стратегічні наслідки кіберінциденту з CrowdStrike Falcon. Він зазначає, що попри масштабність інциденту з фінансової точки зору, його глобальний ефект є незначним. Льюіс також підкреслює проблему слабкої оцінки ризиків багатьма компаніями, які не враховують свою залежність від постачальників у ризикоорієнтованому плануванні. На його думку, ключовим наслідком цього інциденту стане активізація дискусій щодо змісту контрактів між замовниками та постачальниками хмарних послуг, зокрема в частині відповідальності сторін, а також новий виток дискусії про статус постачальників хмарних послуг як об'єктів критичної інфраструктури з відповідним державним регулюванням.

СТРАХОВІ ЗБИТКИ ВІД ЗБОЮ CROWDSTRIKE МОЖУТЬ ДОСЯГТИ 1,5 МІЛЬЯРДА ДОЛАРІВ

25 липня компанія CyberCube оприлюднила прогноз страхових наслідків від масштабного збою CrowdStrike. За їхньою оцінкою, страхові збитки можуть становити від 400 мільйонів до 1,5 мільярда доларів. Страхова компанія Parametrix оцінює страхові збитки від 540 мільйонів до 1,08 мільярда доларів США для компаній зі списку Fortune 500. Водночас рейтингове агентство Fitch повідомило, що глобальна індустрія страхування, ймовірно, уникне серйозних фінансових наслідків від цього збою.

CISA ВІДМІЧАЄ АКТИВІЗАЦІЮ ЗЛОВМИСНИКІВ, ЯКІ ХОЧУТЬ СКОРИСТАТИСЬ ІНЦИДЕНТОМ CROWDSTRIKE

26 липня CISA, у своєму огляді ситуації, пов'язаної з інцидентом CrowdStrike, зазначає, що зловмисники активно намагаються скористатися цим інцидентом у своїх інтересах. Для запобігання подібним ситуаціям CISA закликає користувачів та адміністраторів бути пильними та дотримуватися надійних заходів кібербезпеки. Зокрема, рекомендується дотримуватися вказівок лише з офіційних джерел, блокувати шкідливі домени та слідувати рекомендаціям CrowdStrike для захисту від фішингової активності.

DELTA AIR LINES БУДЕ ВИМАГАТИ КОМПЕНСАЦІЇ ЗА КІБЕРЗБІЙ CROWDSTRIKE

29 липня Delta Air Lines повідомила, що найняла юридичну фірму та вимагатиме компенсації від Microsoft та CrowdStrike через глобальний кіберзбій. Авіакомпанія, що базується в Атланті, найповільніше серед великих перевізників США відновлювалася після технічного збою, який призвів до скасування понад 6000 рейсів. Аналітики оцінюють, що вплив на прибутки Delta Air Lines може становити сотні мільйонів доларів.

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

АЕРОКОСМІЧНА ТА ОБОРОННА ПРОМИСЛОВІСТЬ ЄС ХОЧЕ ЖОРСТКІШИХ ВИМОГ ЩОДО КОМПАНІЙ-ПІДРЯДНИКІВ ХМАРНИХ ПОСЛУГ

5 липня стало відомо, що аерокосмічна та оборонна промисловість ЄС планує порушити питання щодо запровадження більш жорстких вимог до компаній-підрядників хмарних послуг у рамках Загальноєвропейської схеми сертифікації хмарної кібербезпеки (EUCS). Представники цих галузей підкреслюють, що для них це питання не цифрового суверенітету, а чіткого розуміння місця зберігання їхніх чутливих даних. Ключова ідея змін полягає в тому, що підрядники, які надають хмарні послуги на території ЄС, повинні не лише бути зареєстрованими як європейські компанії, але й розміщувати відповідну інфраструктуру на території ЄС. Це має захистити європейських споживачів від екстериторіального впливу законів країн, що не є частиною ЄС, зокрема щодо недопущення передачі даних іноземним органам.

ОФІС ПОЛІТИКИ ЩОДО НАУКИ ТА ТЕХНОЛОГІЙ (OSTP) ВИМАГАЄ ВІД НАУКОВО-ДОСЛІДНИХ УСТАНОВ БІЛЬШОЇ УВАГИ ДО ВЛАСНОЇ КІБЕРБЕЗПЕКИ

9 липня Білий дім (Офіс політики щодо науки та технологій, OSTP) опублікував меморандум, який вимагає від наукових установ, що здійснюють науково-дослідні та дослідно-конструкторські роботи за федеральні кошти (якщо таке фінансування перевищує 50 мільйонів доларів на рік), впровадити більш ефективні заходи кібербезпеки для захисту результатів досліджень від зловмисних акторів. Конкретні вимоги не вказуються, але меморандум рекомендує організаціям використовувати документи NIST.

ОФІС НАЦІОНАЛЬНОГО КІБЕРДИРЕКТОРА США ОПРИЛЮДНИВ МЕМОРАНДУМ ПРО ПРІОРИТЕТИ ІНВЕСТИЦІЙ У КІБЕРБЕЗПЕКУ

10 липня Білий дім (Офіс національного кібердиректора) опублікував нові пріоритети у сфері кібербезпеки на 2026 фінансовий рік. Пріоритети базуються на Національному плані реалізації стратегії кібербезпеки (NCSIP), який нещодавно був актуалізований до 2026 фінансового року. Документ визначає пріоритети Національної стратегії кібербезпеки США, які будуть у фокусі уваги найближчого року. Ключові зміни включають:

- оновлення вимог до впровадження Zero Trust: агентства повинні надати свої стратегії впровадження нульової довіри протягом 120 днів, включаючи документацію щодо поточного та цільового рівнів зрілості;
- покращена інтеграція державного та приватного секторів;
- розвиток кіберробочої сили: запровадження більш гнучких вимог до найму та скасування конкретних вимог до освітнього ступеня;
- активніша підготовка до постквантової криптографії: агентства мають виділити ресурси для переходу критично важливих і чутливих мереж і систем на квантово-стійку криптографію.

НІМЕЧЧИНА ПРИБЕРЕ HUAWEI ТА ZTE ЗІ СВОЇХ МЕРЕЖ 5G

11 липня уряд Німеччини оголосив про досягнення угоди з великими телекомунікаційними компаніями щодо поступового припинення використання критичних компонентів Huawei та ZTE у мобільній інфраструктурі 5G протягом п'яти років. Спершу, використання критичних компонентів китайського виробництва буде припинено в основних частинах мережі 5G до кінця 2026 року. Після цього компоненти, виготовлені китайськими виробниками, поступово виведуть з антен, ліній електропередач і веж до кінця 2029 року.

У CISA ПРИЗНАЧЕНІ НОВІ ТОП-ПОСАДОВЦІ

17 липня CISA оголосила про призначення Джеффа Гріна виконавчим помічником директора з кібербезпеки та Трента Фрейзера помічником директора із залучення зацікавлених сторін. Обидва виконували ці обов'язки до офіційного призначення. Джефф Грін, виконавчий помічник директора з кібербезпеки, раніше був старшим директором в Інституті Аспена, де керував глобальною програмою політики кібербезпеки. До роботи в Аспені він очолював відділ кіберреагування та політики в Раді національної безпеки Білого дому. Трент Фрейзер, помічник директора із залучення зацікавлених сторін, раніше був заступником помічника директора з тієї ж галузі. До приєднання до CISA він обіймав різні керівні посади в Міністерстві внутрішньої безпеки, зосереджуючись на захисті та зміцненні стійкості в середовищі вищої освіти, розвитку транскордонної транспортної інфраструктури, залученні робочої сили та управлінні програмами. Джен Істерлі також оголосила, що Бріджит Бін обійме посаду виконавчого директора в серпні 2024 року.

ВЕЛИКОБРИТАНІЯ ПЛАНУЄ ПРИЙНЯТИ ЗАКОН ПРО КІБЕРБЕЗПЕКУ ТА СТІЙКІСТЬ

24 липня британський уряд оголосив про намір винести на розгляд парламенту законопроєкт про кібербезпеку та стійкість. Очікується, що законопроєкт включатиме підвищену увагу до захисту критично важливої національної інфраструктури, збільшення повноважень регуляційних органів разом із посиленими вимогами до звітності, запровадження вищих штрафів і пені для організацій, які не дотримуються встановлених стандартів кібербезпеки. Організації будуть зобов'язані забезпечити, щоб їхні постачальники та партнери також дотримувалися та підтримували ці стандарти кібербезпеки.

ФБР ВІДПРАВЛЯЄ КІБЕРГРУПУ З 65 ОСІБ ПО ВСЬОМУ СВІТУ ДЛЯ БОРОТЬБИ З ХАКЕРАМИ

Федеральне бюро розслідувань (ФБР) нещодавно представило на своєму офіційному вебсайті Cyber Action Team (CAT). CAT складається з 65 основних членів, об'єднаних у групу швидкого реагування, яку можна розгорнути майже в будь-якій точці земної кулі протягом кількох годин. За твердженням ФБР, метою групи є відповідь на загрози та атаки, спрямовані на громадську безпеку, а також захист національної та економічної безпеки. Хоча CAT була заснована у 2005 році, ця ініціатива здебільшого залишалася поза увагою ЗМІ.

КИТАЙ ОЦІНЮЄ МОЖЛИВІСТЬ СТВОРЕННЯ НАЦІОНАЛЬНОГО ІДЕНТИФІКАТОРА КІБЕРПРОСТОРУ

29 липня стало відомо, що Міністерство громадської безпеки та Управління кіберпростору Китаю (CAC) розробляють «ідентифікатори кіберпростору» – інструмент для ідентифікації користувачів, які планують скористатися інтернет-послугами. Ідентифікатор матиме дві форми: одну у вигляді серії літер і цифр, а іншу – як облікові дані в Інтернеті. Обидві форми відповідатимуть реальній особистості громадянина, але без розкриття деталей у відкритому форматі. Платформа державних національних послуг відповідатиме за автентифікацію та видачу цих ідентифікаторів. Офіційною метою введення ідентифікатора є «захист особистої інформації громадян, регулювання публічних послуг у кіберпросторі та прискорення реалізації стратегії довіреної онлайн-ідентичності».

ВИБОРЧА КОМІСІЯ ВЕЛИКОЇ БРИТАНІЇ МАЄ НЕЗАДОВІЛЬНИЙ РІВЕНЬ КІБЕРБЕЗПЕКИ – ОЦІНКА УПРАВЛІННЯ ІНФОРМАЦІЙНОГО КОМІСАРА

31 липня Управління інформаційного комісара (ICO) опублікувало оцінку стану кібербезпеки окремих державних установ, включно з Виборчою комісією Великої Британії, які постраждали внаслідок кіберінциденту з Microsoft Exchange Server у 2021 році. Виявлено, що кібербезпека Виборчої комісії була вкрай низькою. Комісії знадобилося 13 місяців, щоб виявити кібератаку, значною мірою через неефективний режим виправлення в організації, який не зміг виявити численні вразливості, відомі за місяці до атаки.

Комісію також визнали винною у використанні паролів за замовчуванням та відсутності відповідної політики керування паролями. Під час перевірки виявлено, що 178 паролів були ідентичні або схожі на паролі, видані під час створення облікових записів. Як наслідок, спонсоровані Китаєм зловмисники мали доступ до імен і домашніх адрес близько 40 мільйонів британських виборців протягом 13 місяців.

ШВЕЙЦАРІЯ ЗРОБИЛА ВИКОРИСТАННЯ ПЗ З ВІДКРИТИМ КОДОМ ПРІОРИТЕТНИМ ДЛЯ ДЕРЖАВНОГО СЕКТОРА

Швейцарія прийняла «Федеральний закон про використання електронних засобів для виконання державних завдань» (EMBAG), який передбачає обов'язкове використання програмного забезпечення з відкритим кодом (OSS) в органах державного сектору. Цей закон являє собою значні зміни в державній розробці та закупівлі програмного забезпечення, спрямовані на зменшення прив'язки до постачальників, підвищення цифрової прозорості та зниження витрат на IT. EMBAG вимагає від державних органів розкривати вихідний код програмного забезпечення, сприяючи прозорості, безпеці та ефективності, за винятком випадків, пов'язаних з правами третіх сторін або питаннями безпеки.

Стаття 9 закону дозволяє державним органам пропонувати додаткові послуги, пов'язані з OSS, забезпечуючи конкурентний баланс. Розробка закону спочатку зустріла опір, але зрештою була підтримана ключовими зацікавленими сторонами, зокрема Парламентською групою цифрової сталості (Parldigi). Очікується, що EMBAG стане моделлю для інших країн, сприяючи цифровому суверенітету, інноваціям і співпраці в державному секторі.

РІШЕННЯ ВЕРХОВНОГО СУДУ США, ЙМОВІРНО, СПРИЧИНИТЬ ХАОС У КІБЕРРЕГУЛЮВАННІ

2 липня видання CSO Online повідомило, що рішення Верховного суду США у справі «Loper Bright Enterprises проти Raimondo» може кардинально змінити федеральні правила кібербезпеки, передавши остаточне схвалення регуляторних рішень від відповідних агенцій до судів. Згідно з цим рішенням, суди тепер мають останнє слово щодо тлумачення законів, виданих Конгресом. Це рішення створює невизначеність у тисячах федеральних нормативних актів, включаючи нещодавні укази адміністрації Байдена щодо кібербезпеки.

Очікується, що це призведе до численних судових позовів щодо існуючих кіберрегуляцій, потенційно спричиняючи дерегуляцію та непослідовне застосування правил у різних юрисдикціях. CSO Online зазначає, що CISO та організації повинні бути готові до потенційних труднощів у дотриманні нормативних вимог у міру розвитку правового ландшафту.

У ВЕЛИКОБРИТАНІЇ НОВИЙ УРЯД. ЩО МИ МОЖЕМО ОЧІКУВАТИ ВІД НЬОГО У КІБЕРСФЕРІ?

Видання The Record повідомляє, що від нещодавно призначеного уряду Великобританії експерти очікують «деполітизації» питань кібербезпеки. Це означає менше публічної уваги до кіберінцидентів та більше роботи для технічних фахівців. Очікується також, що питання кібербезпеки матиме нижчу пріоритетність у порівнянні з іншими питаннями безпеки та оборони. Проте деталі політики, яку проводитиме Лейбористська партія, залишаються невідомими.

ПРЕЗИДЕНТ США РОЗПОРЯДИВСЯ СТВОРИТИ КОМІСІЮ ДЛЯ РОЗСЛІДУВАННЯ МАСШТАБНОЇ РОСІЙСЬКОЇ КІБЕРАТАКИ, АЛЕ ЦЬОГО НЕ СТАЛОСЯ

Після однієї з найбільш руйнівних кібератак в історії США на урядові установи через компрометацію SolarWinds, адміністрація Байдена створила спеціальну раду для розслідування інциденту і доведення інформації до громадськості. Проте, з причин, які залишаються незрозумілими експертам, ця інформація не була оприлюднена. Публічний звіт щодо атаки на SolarWinds міг би завдати значних ударів Microsoft. Експерти вважають, що відсутність розслідування способів, якими хакери SolarWinds використовували програмне забезпечення Microsoft, позбавила Раду можливості запобігти подібним атакам у майбутньому.

ОКРУГ ІНДІАНА ПОДАВ ЗАЯВУ ПРО НАДЗВИЧАЙНУ СИТУАЦІЮ ПІСЛЯ АТАКИ ПРОГРАМ-ВИМАГАЧІВ

Кілька місцевих адміністрацій у США постраждали від атак програм-вимагачів. Зокрема, адміністрація округу Клей в штаті Індіана подала заяву про надзвичайну ситуацію після атаки, яка «призвела до неможливості надання критично важливих послуг, необхідних для щоденної роботи офісів суду округу Клей, громадських виправних установ і пробації округу Клей». Ця декларація дозволяє офіційним особам округу розподілити фінансові ресурси для постраждалих департаментів і вжити термінових заходів для вирішення проблем з операціями.

3. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

ГЛОБАЛЬНА ПОЛІЦЕЙСЬКА ОПЕРАЦІЯ ВІДКЛЮЧИЛА 600 СЕРВЕРІВ КІБЕРЗЛОЧИНЦІВ, ПОВ'ЯЗАНИХ ІЗ COBALT STRIKE

4 липня видання The Hacker News повідомило, що в рамках скоординованої операції правоохоронних органів під кодовою назвою MORPHEUS було демонтовано майже 600 серверів, які використовувалися кіберзлочинцями для атак за допомогою інструменту Cobalt Strike. За даними Європолу, операція, проведена з 24 по 28 червня, була спрямована на старіші неліцензійні версії Red Teaming Framework Cobalt Strike. З 690 позначених IP-адрес, пов'язаних зі злочинною діяльністю у 27 країнах, 590 зараз недоступні. Спільну операцію, розпочату у 2021 році, очолювало Національне агентство зі злочинності Великої Британії (NCA), за участі органів влади з Австралії, Канади, Німеччини, Нідерландів, Польщі та США, з додатковою підтримкою Болгарії, Естонії, Фінляндії, Литви, Японії та Південної Кореї.

ЧЛЕНИ АЛЬЯНСУ ДОМОВИЛИСЯ ПРО СТВОРЕННЯ ІНТЕГРОВАНОГО ЦЕНТРУ КІБЕРЗАХИСТУ НАТО

10 липня члени НАТО ухвалили рішення про створення Інтегрованого центру кіберзахисту НАТО (NICC), який покращить захист мереж НАТО та країн-членів Альянсу. Центр буде інформувати військове командування про кіберзагрози та вразливі місця, включаючи критичну цивільну інфраструктуру. NICC об'єднає цивільний і військовий персонал НАТО, країн Альянсу та експертів з промисловості, і буде базуватися у стратегічному військовому штабі НАТО в SHAPE (Бельгія).

НАТО ОПУБЛІКУВАВ РЕЗЮМЕ ПЕРЕГЛЯНУТОЇ СТРАТЕГІЇ НАТО ЩОДО ШТУЧНОГО ІНТЕЛЕКТУ (ШІ)

Альянс НАТО опублікував резюме переглянутої стратегії щодо штучного інтелекту (ШІ). Її цілями є:

- забезпечення основи для того, щоб НАТО та країни-члени могли подавати приклад і заохочувати розвиток та відповідальне використання ШІ для оборонних та безпекових цілей Альянсу;
- прискорення впровадження ШІ у розробці та наданні можливостей, підвищуючи взаємодію в межах Альянсу, включаючи надання сценаріїв використання ШІ;
- захист і контроль технологій ШІ, управління пов'язаними ризиками та захист здатності до інновацій, вирішення питань безпеки, таких як операціоналізація Принципів відповідального використання, визначених Альянсом;
- визначення та захист від загроз, пов'язаних із ворожим використанням ШІ.

АНБ США ТА АВСТРАЛІЙСЬКА ASD РОЗКРИЛИ ДЕТАЛІ ТАКТИК КИТАЙСЬКИХ КІБЕРЗЛОЧИНЦІВ

8 липня АНБ США разом з Австралійським управлінням зв'язку (ASD) та іншими відомствами опублікували консультативний документ з кібербезпеки (CSA), в якому детально описані методи, що використовуються групою APT 40 (також відомою як Kryptonite Panda, GINGHAM TYPHOON і Bronze Mohawk), пов'язаною з Міністерством державної безпеки Китайської Народної Республіки (КНР). Документ під назвою PRC MSS Tradecraft in Action може допомогти фахівцям з кібербезпеки краще зрозуміти тактики та методи цього угрупування, яке націлюється на організації в різних країнах, включаючи США та Австралію.

4. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ.

УРЯДОВОМУ ХАКЕРУ З ПІВНІЧНОЇ КОРЕЇ ВИСУНУТО ЗВИНУВАЧЕННЯ У ПРИЧЕТНОСТІ ДО КІБЕРАТАК НА ЛІКАРНІ ТА ПОСТАЧАЛЬНИКІВ МЕДИЧНИХ ПОСЛУГ США

Згідно зі звинуваченням, висунутим Департаментом юстиції США 25 липня 2024 року, хакерська група «Андаріель» використовувала кошти, отримані від медичних закладів як викуп, для фінансування крадіжки конфіденційної інформації з оборонних і технологічних установ та організацій по всьому світу, включно з урядовими установами США. Відмивання грошей здійснювалося через Китай. Звинувачення висунуто північнокорейському хакеру на ім'я Рім Йон Хьок.

CISCO TALOS ВИЯВИЛА 15 ВРАЗЛИВОСТЕЙ У БЕЗДРОТОВИХ МАРШРУТИЗАТОРАХ

10 липня компанія Cisco Talos повідомила про виявлення 15 вразливостей у програмному забезпеченні Realtek RTL819x Jungle SDK, яке використовується в деяких бездротових маршрутизаторах для малих та домашніх офісів, а також у LevelOne WBR-6013.

ГРУПА ЗАГРОЗ VELVET ANT, ПОВ'ЯЗАНА З КИТАЄМ, ВИКОРИСТОВУЄ CISCO ZERO-DAY

Компанія Sygnia виявила, що пов'язана з Китаєм група використовувала вразливість CVE-2024-20399 як вразливість «нульового дня» і поділилася деталями з Cisco. Група загроз під назвою Velvet Ant успішно експлуатувала цю вразливість для виконання команд у базовій операційній системі пристроїв Cisco Nexus. Це призвело до використання раніше невідомого спеціалізованого шкідливого програмного забезпечення, яке дозволяло групі загроз дистанційно підключатися до скомпрометованих пристроїв Cisco Nexus, завантажувати додаткові файли та виконувати код на цих пристроях.

ІНДОНЕЗІЯ РОЗПОЧАЛА ПРОЦЕС ВІДНОВЛЕННЯ ДАНИХ ПІСЛЯ RANSOMWARE

12 липня влада Індонезії повідомила про початок процесу відновлення даних, які були зашифровані групою Brain Cipher у червні 2024 року. Спочатку хакери вимагали викуп у розмірі 8 мільйонів доларів, але пізніше відмовилися від цієї вимоги та передали ключ для розшифрування безкоштовно.

ELDORADO RANSOMWARE: НОВА ЗОЛОТА ІМПЕРІЯ КІБЕРЗЛОЧИННОСТІ?

Дослідники з Group-IB описують програмне забезпечення-вимагач як послугу (RaaS) під назвою Eldorado, яке з'явилося в березні 2024 року. Це зловмисне програмне забезпечення націлене на системи як Windows, так і Linux. За інформацією BleepingComputer, Eldorado вже заявило про 16 жертв, більшість з яких знаходяться у США, і діють у секторах нерухомості, освіти, охорони здоров'я та виробництва.

ДЕРЖАВНІ СПЕЦСЛУЖБИ ІРАНУ ЗНАЧНО АКТИВІЗУВАЛИ СВОЮ ХАКЕРСЬКУ ДІЯЛЬНІСТЬ ПРОТИ ІЗРАЇЛЮ – CHECKPOINT

Згідно зі звітом ізраїльської кібербезпекової компанії Checkpoint, іранська група загроз MuddyWater, пов'язана з Міністерством розвідки та безпеки (MOIS), значно активізувала свою діяльність в Ізраїлі з початку війни між Ізраїлем та ХАМАС. Ця активність аналогічна діям групи проти цілей у Саудівській Аравії, Туреччині, Азербайджані, Індії та Португалії.

Зловмисники регулярно використовують фішингові листи, надіслані зі зламаних організаційних облікових записів електронної пошти, що призводить до розгортання легітимних інструментів віддаленого керування, таких як Atera Agent та Screen Connect. Нещодавні кампанії MuddyWater також призвели до розгортання нового, раніше незадокументованого спеціально створеного бекдора під назвою BugSleep, який використовується для націлювання на організації в Ізраїлі.

ЗЛАМ OPENAI 2023 РОКУ ВИКЛИКАЄ ЗАНЕПОКОЄННЯ ЩОДО НАЦІОНАЛЬНОЇ БЕЗПЕКИ

На початку минулого року приватний хакер отримав доступ до внутрішніх систем обміну повідомленнями OpenAI, викравши деталі про дизайн ChatGPT, що викликало побоювання щодо можливих порушень з боку держав-супротивників. За інформацією SC Media, серед супротивників США зростає інтерес до ChatGPT, включаючи державних хакерів з росії, Китаю, Ірану та Північної Кореї.

OpenAI повідомила про інцидент своїм співробітникам і правлінню у квітні 2023 року, але не повідомила громадськість або правоохоронні органи, оскільки вважала, що хакер не мав зв'язків з іноземними урядами. Ілля Колоченко, генеральний директор ImmuniWeb, підкреслив значну загрозу з боку державних кіберзлочинців, які націлюються на постачальників штучного інтелекту для викрадення інтелектуальної власності та комерційної інформації, потенційно впроваджуючи бекдори для контролю або руйнування компаній ШІ.

ХАКЕРИ ВИКРАЛИ В AT&T «МАЙЖЕ ВСІ» ЖУРНАЛИ ВИКЛИКІВ ЗА ШІСТЬ МІСЯЦІВ

За кілька днів було повідомлено, що злам даних AT&T був здійснений американським хакером, який проживає в Туреччині. Телекомунікаційний гігант заплатив викуп у розмірі $370,000, щоб переконатися, що викрадена інформація буде видалена. Як повідомляє Bloomberg, така відносно невелика сума пояснюється тим, що хакери не усвідомили цінність викраденої інформації.

ГЛИБОКЕ ЗАНУРЕННЯ В ОНОВЛЕНИЙ АРСЕНАЛ КИТАЙСЬКОГО ДЕРЖАВНОГО УГРУПОВАННЯ APT41

11 липня компанія Zscaler опублікувала технічний звіт про нещодавно виявлений завантажувач зловмисного програмного забезпечення DodgeBox, пов'язаний із загрозою APT41, яка діє в Китаї. DodgeBox використовується для встановлення нового бекдору під назвою MoonWalk, який використовує Google Drive для командно-контрольного зв'язку. Друга частина звіту стосується власне бекдору MoonWalk.

MANDIANT ПОПЕРЕДЖАЄ, ЩО КИТАЙСЬКА ХАКЕРСЬКА ГРУПА APT41 ПРОНИКАЄ В ГЛОБАЛЬНИЙ ТРАНСПОРТНИЙ І ТЕХНІЧНИЙ СЕКТОРИ

Дослідники з Mandiant відзначають масштабне відновлення атак зловмисного програмного забезпечення з боку плідної китайської урядової хакерської групи APT41, яка була залучена до зломів організацій у секторах доставки, логістики, технологій та автомобільної промисловості в Європі та Азії.

За інформацією Mandiant, більшість скомпрометованих організацій знаходяться у Великобританії, Італії, Іспанії, Туреччині, Тайвані та Таїланді. APT41 вдалося проникнути в ці організації та підтримувати тривалий несанкціонований доступ, починаючи з 2023 року.

У технічному звіті Mandiant зазначається, що APT41 (також відома як Barium, Wicked Panda та Winnti) також проводить розвідувальні дії проти подібних організацій у таких країнах, як Сінгапур, що вказує на потенційне розширення кола їхніх цілей.

APT41 АТАКУВАЛА УРЯДОВИЙ ТАЙВАНСЬКИЙ ДОСЛІДНИЦЬКИЙ ІНСТИТУТ

31 липня експерти Cisco Talos виявили зловмисну кампанію, яка скомпрометувала тайванський урядовий науково-дослідний інститут. Атака розпочалась ще в липні 2023 року і включала доставку зловмисного програмного забезпечення ShadowPad, Cobalt Strike та інших спеціалізованих інструментів для посткомпрометаційних дій. Інститут спеціалізується на обчислювальних і пов'язаних технологіях. Зловмисники намагалися зібрати паролі користувачів, отримати дані про програмне забезпечення, яке використовується в інституті, та викрасти численні файли.

4,3 МІЛЬЙОНА ОСІБ ПОСТРАЖДАЛИ ВІД ВИТОКУ ДАНИХ HEALTHEQUITY

Американська компанія HealthEquity, яка займається фінансовими технологіями та надає бізнес-послуги у сфері небанківських заощаджень, повідомила 4,3 мільйона осіб про компрометацію їхньої особистої та медичної інформації внаслідок витоку даних стороннього постачальника. Серед викрадених даних є номери соціального страхування та інформація про платіжні картки. Витік стався 25 березня і, за словами компанії, вимагав проведення глибокого технічного розслідування.

ІДЕНТИФІКОВАНО ПОНАД 250 МОБІЛЬНИХ ЗАСТОСУНКІВ, ЩО Є «ЗЛИМИ ДВІЙНИКАМИ» ЗАКОННИХ ПРОГРАМ

Команда Satori Threat Intelligence Team виявила масштабну операцію з рекламного шахрайства під назвою Konfety, яка передбачає створення «злих двійників» легітимних програм у Google Play Store. Використовуючи CarmelAds SDK, кіберзлочинці створюють програми-приманки, які виконують рекламне шахрайство та перенаправляють користувачів на сайти зі зловмисним ПЗ. Ці програми-приманки безпосередньо не здійснюють шахрайство, але поширюються через рекламні кампанії, що призводить до встановлення шкідливих розширень браузера, моніторингу вебпошуку та завантаження зловмисного коду на пристрої користувачів. Виявлено понад 250 таких застосунків.

Хоча сам SDK не є зловмисним, його використовували для відтворення реклами, стороннього завантаження файлів APK та підключення до командно-контрольних серверів. Цей новий вектор атаки, ймовірно, використовується кількома загрозливими суб'єктами. Операція підкреслює постійну проблему зловмисної реклами та необхідність суворіших заходів безпеки з боку рекламних мереж, а також кращої освіти кінцевих користувачів щодо безпеки мобільних застосунків.

ФРАНЦІЯ РОЗПОЧАЛА МАСШТАБНУ ОПЕРАЦІЮ З БОРОТЬБИ З КІБЕРШПИГУНСТВОМ НАПЕРЕДОДНІ ОЛІМПІАДИ

Французька влада розпочала масштабну операцію з видалення шкідливого програмного забезпечення зі своїх комп'ютерних систем, зосереджену на програмах, пов'язаних зі шпигунством. Ця «дезінфекція» триватиме кілька місяців і спрямована на шкідливе ПЗ PlugX, яке відоме своєю асоціацією з китайськими державними хакерськими групами та поширюється через USB-флеш-накопичувачі. PlugX інфікувало щонайменше 3000 пристроїв у Франції та кілька мільйонів у всьому світі.

Завдяки командно-контрольному серверу, пов'язаному з PlugX, конфіскованому компанією з кібербезпеки Sekoia, було виявлено зараження у понад 170 країнах. Рішення Sekoia для дистанційної дезінфекції використовується у Франції та інших країнах. Сотні пристроїв, насамперед у Франції та інших європейських країнах, вже були продезінфіковані. Ця операція підкреслює міжнародні зусилля в боротьбі зі складною кіберзлочинністю, особливо напередодні Олімпійських ігор.

STARGAZER GOBLIN СТВОРИВ 3000 ПІДРОБЛЕНИХ ОБЛІКОВИХ ЗАПИСІВ GITHUB ДЛЯ ПОШИРЕННЯ ЗЛОВМИСНОГО ПЗ

Користувач, відомий як Stargazer Goblin, здійснив атаку типу Distribution-as-a-Service на платформі Github, використовуючи приблизно 3000 підроблених облікових записів. Вважається, що ця мережа була створена ще у 2022 році, хоча прямих доказів її існування до липня 2023 року немає. Мережа виявилася стійкою до спроб її закриття, оскільки облікові записи витримали спроби блокування. Виявлення цієї складної мережі відбувається на тлі посилення атак на платформу та її користувачів.

КІБЕРАТАКА ВРАЗИЛА НЕКОМЕРЦІЙНУ ОРГАНІЗАЦІЮ ДОНОРСТВА КРОВІ ONEBLOOD

31 липня CNN повідомила, що некомерційна організація з донорства крові OneBlood, яка обслуговує сотні лікарень на південному сході США в Алабамі, Флориді, Джорджії, Північній і Південній Кароліні, стала жертвою кібератаки. Кілька джерел, знайомих із ситуацією, повідомили, що інцидент розслідується як потенційна атака програмного забезпечення-здирника. Поки OneBlood оговтувалася від інциденту, організація вручну маркувала продукти крові, повідомляє CNN.

5. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

CISA ВИПУСТИЛА ПОСІБНИК З ОПЕРАТИВНОЇ БЕЗПЕКИ ДЛЯ ОФІЦІЙНИХ ОСІБ, ЯКІ ЗАЙМАЮТЬСЯ ВИБОРАМИ

5 липня CISA опублікувала «Посібник з оперативної безпеки для посадових осіб з питань виборів». Цей посібник спрямований на посилення безпеки виборчої інфраструктури, надаючи детальний огляд оперативної безпеки (OPSEC) у контексті виборів. У ньому підкреслюються потенційні ризики та пропонуються практичні заходи для їх пом'якшення.

КАНАДСЬКИЙ ЦЕНТР КІБЕРБЕЗПЕКИ ПОВІДОМИВ ПРО ВРАЗЛИВІСТЬ В ПРОТОКОЛІ RADIUS

9 липня Канадський центр кібербезпеки оголосив про виявлення вразливості в протоколі RADIUS (CVE-2024-3596). Ця вразливість може дозволити зловмиснику пройти аутентифікацію або відмовити в ній легальним користувачам. Проблема пов'язана з відсутністю автентифікації та перевірки цілісності в протоколі RADIUS. Зловмисник може використати слабкий криптографічний хеш MD5 та підробити відповіді на аутентифікацію від сервера RADIUS. RADIUS – популярний мережевий протокол для автентифікації, авторизації та обліку, що використовується для управління доступом до мереж, включаючи хмарні сервіси.

CISA ОПУБЛІКУВАЛА КОНСУЛЬТАЦІЮ ЩОДО ДІЙ ЧЕРВОНОЇ КОМАНДИ ПІД ЧАС ОЦІНКИ ОРГАНІЗАЦІЇ FCEB США

11 липня CISA оприлюднила документ «Операції червоної команди CISA проти федеральної цивільної організації виконавчої гілки влади». У цій консультації з кібербезпеки (CSA) детально описані ключові тактики, методи та процедури (TTP) червоної команди, а також пов'язана з цим діяльність. CSA надає рекомендації, які допоможуть керівникам та фахівцям з кібербезпеки покращити їхні можливості у сфері кібербезпеки, виявлення загроз, реагування та пошуку.

6. КРИТИЧНА ІНФРАСТРУКТУРА

LOCKBIT ЗАЯВЛЯЄ ПРО КІБЕРАТАКУ НА НАЙБІЛЬШУ ЛІКАРНЮ ХОРВАТІЇ

2 липня видання The Record повідомило, що група програм-вимагачів LockBit взяла на себе відповідальність за кібератаку на найбільшу хорватську лікарню KBC Zagreb, яка порушила роботу IT-систем і змусила перейти до ручних операцій. Атака вплинула на обслуговування пацієнтів, особливо на служби екстреної допомоги та радіологічну службу, і призвела до перенаправлення пацієнтів в інші лікарні. Хоча LockBit стверджував, що отримав доступ до конфіденційних даних, хорватські офіційні особи не підтвердили жодних вимог викупу чи крадіжки даних. Розслідування триває. Ця атака є частиною ширшого сплеску кібератак на хорватські інституції, включаючи нещодавні цільові атаки на кілька державних вебсайтів, здійснені групою NoName057(16), пов'язаною з росією.

MICROSOFT ВИЯВИЛА КРИТИЧНІ НЕДОЛІКИ В ROCKWELL AUTOMATION PANELVIEW PLUS

Корпорація Microsoft виявила дві вразливості в системі Rockwell Automation PanelView Plus, які можуть бути використані віддаленими неавтентифікованими зловмисниками для виконання довільного коду та ініціювання відмови в обслуговуванні (DoS).

CDK GLOBAL ЗАПЛАТИЛА ВИКУП У 25 МЛН ДОЛАРІВ RANSOMWARE ГРУПІ BLACKSUIT

12 липня стало відомо, що компанія CDK Global, чиє програмне забезпечення використовується для функціонування більш ніж половини всіх автосалонів у США, заплатила викуп у розмірі 25 мільйонів доларів групі BlackSuit, яка займається програмами-вимагачами, для відновлення своїх систем. Кібератака проти CDK Global розпочалася 19 червня, і лише в середині липня компанія змогла відновити своє функціонування.

SIEMENS ВИПРАВИЛО НЕДОЛІКИ ПРОДУКТУ POWER GRID, ЩО ДОЗВОЛЯЛИ РОЗГОРТАТИ БЕКДОР

24 липня компанія Siemens повідомила про підготовку виправлень для кількох потенційно серйозних вразливостей, що впливають на деякі її продукти для електромереж Sicam. Мова йде про Sicam A8000, який є віддаленим терміналом (RTU) для телеконтролю та автоматизації в енергетичному секторі, а також Sicam Enhanced Grid Sensor (EGS) і його програмне забезпечення Sicam 8.

Одна з вразливостей (CVE-2024-37998) класифікована як «критична» і дозволяє зловмиснику скинути пароль облікових записів адміністратора без знання поточного пароля, якщо ввімкнена функція автоматичного входу. Інша вразливість (CVE-2024-39601), класифікована як «середньої серйозності», дозволяє віддаленому автентифікованому зловмиснику або неавтентифікованому зловмиснику з фізичним доступом знизити версію мікропрограми пристрою до версії, яка містить відому вразливість.

ЗАПАСИ КРОВІ В БРИТАНІЇ ВПАЛИ ДО «БЕЗПРЕЦЕДЕНТНО НИЗЬКОГО РІВНЯ» ЧЕРЕЗ КІБЕРАТАКУ

Як повідомила BBC 25 липня, Національна служба охорони здоров'я Великобританії попередила про зниження запасів крові до небезпечного рівня після того, як сотні записів на здачу крові були скасовані через кібератаку в червні. Національна служба охорони здоров'я закликала лікарні обмежити використання крові групи О, оскільки її запаси впали значно нижче мінімальних вимог. Дефіцит частково пояснюється кібератакою на фірму Synnovis минулого місяця, а також іншими сезонними факторами.

ЗЛОВМИСНЕ ПЗ ПОРУШИЛО ТЕПЛОПОСТАЧАННЯ У ЛЬВОВІ

Dragos опублікувала звіт про новий штам зловмисного програмного забезпечення, що використовується проти систем індустріального контролю (ICS). У січні 2024 року це ПЗ порушило роботу енергокомпанії у Львові, призвівши до дводенної втрати опалення в 600 багатоквартирних будинках під час мінусових температур. Зловмисне ПЗ, яке Dragos назвала FrostyGoop, є «першим специфічним для ICS зловмисним програмним забезпеченням, що використовує зв'язок Modbus для впливу на операційні технології (OT)». Dragos підозрює, що зловмисне ПЗ отримало доступ до систем ICS через невідому вразливість у зовнішньому маршрутизаторі Mikrotik.

КІБЕРАТАКИ НА СУДНОПЛАВСТВО ЗРОСТАЮТЬ НА ТЛІ ГЕОПОЛІТИЧНОЇ НАПРУЖЕНОСТІ

Судновласники, порти та інші морські організації зіткнулися з щонайменше 64 кіберінцидентами у 2023 році, як виявили дослідники з Нідерландського університету прикладних наук НХЛ Стенден на основі звітів компаній, ЗМІ та академічних досліджень. Для порівняння, за попередні десять років було зареєстровано лише три такі інциденти, а у 2003 році — жодного. Понад 80 відсотків кібератак з 2001 року були пов'язані з відомими загрозами, походження яких пов'язане з росією, Китаєм, Північною Кореєю або Іраном.

7. АНАЛІТИЧНІ ОЦІНКИ

РИНОК КІБЕРСТРАХУВАННЯ ОПИНИВСЯ ПЕРЕД ВИКЛИКОМ, ПОВ'ЯЗАНИМ З ПОЛІПШЕННЯМ КІБЕРБЕЗПЕКИ ОРГАНІЗАЦІЙ

1 липня компанія Howden у своєму звіті зазначила низку тенденцій, пов'язаних із ринком кіберстрахування. Основна з них полягає в тому, що ставки на кіберстрахування знижуються в усьому світі, оскільки компанії стають більш ефективними у пом'якшенні загроз від кіберзлочинності. Попри зростання кількості атак програм-вимагачів останніми роками, у 2023/24 роках на ринку кіберстрахування відбулося двозначне зниження цін.

РОСІЙСЬКИЙ FIN7 ПРОДАЄ СВОЄ ЗЛОВМИСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ЩО РУЙНУЄ EDR – SENTINELONE

18 липня компанія з кібербезпеки SentinelOne оприлюднила свій звіт про діяльність російської хакерської групи FIN7. Згідно зі звітом, FIN7 активно продає програмне забезпечення AvNeutralizer, яке дозволяє ефективно вимикати засоби захисту кінцевих точок (EDR), групам, що займаються поширенням програм-вимагачів (ransomware). Ціна на AvNeutralizer коливається від 4 000 до 15 000 доларів США, і дані свідчать про сплеск активності потенційних клієнтів на початку 2023 року.

CISCO TALOS СИСТЕМАТИЗУВАВ ОСНОВНІ TTP RANSOMWARE ГРУП

10 липня експерти кібербезпекової компанії Cisco Talos випустили посібник, присвячений діяльності найактивніших груп, що займаються програмами-вимагачами (ransomware). У документі проаналізовано типові тактики, методи та процедури (TTP) цих груп, а також те, як вони використовують ці методи. Крім того, посібник містить рекомендації щодо найбільш ефективних тактик захисту від дій зловмисників.

СПЕЦІАЛІЗАЦІЯ В МЕЖАХ КІБЕРВІЙСЬК Є БІЛЬШ ЕФЕКТИВНИМ ШЛЯХОМ ЇХ ПОБУДОВИ НІЖ МАКСИМАЛЬНО УНІВЕРСАЛІЗАЦІЯ ЇХ УЧАСНИКІВ

25 липня в аналітичному матеріалі «Кібервійська не є єдиним рішенням» досліджується специфічний підхід Міністерства оборони США до кіберфахівців, яких міністерство розглядає як універсальних спеціалістів, здатних виконувати захисні, наступальні та розвідувальні місії, а за потреби – займатися питаннями радіоелектронної боротьби. Автор зазначає, що цей багаторічний підхід є неефективним і потребує змін у процесі створення кібервійськ, оскільки у сфері кібербезпеки важливою є більш вузька спеціалізація.

ЯК ЗБОЇ MFA ВИКЛИКАЮТЬ 500% ЗРОСТАННЯ ВТРАТ ВІД ПРОГРАМ-ВИМАГАЧІВ

Середній платіж кіберзлочинцям-вимагачам різко зріс, збільшившись на понад 500% – з 400 тисяч у 2023 році до 2 мільйонів доларів у 2024 році, згідно зі звітом Sophos «State of Ransomware 2024». Згідно з даними RISK & INSURANCE, середня сума викупу зросла з 1,4 мільйона у 2022 році до 20 мільйонів доларів у 2023 році, а виплати зросли з 335 тисяч до 6,5 мільйонів доларів.

Це різке зростання відображає зростаючу складність кібератак і вразливості в застарілих методах безпеки, особливо в застарілій багатофакторній автентифікації (MFA). Крім того, генеративний штучний інтелект дозволяє кіберзлочинцям створювати дуже переконливі фішингові атаки. У статті розглядаються причини збільшення платежів вимагачам, обмеження застарілої MFA та потреба у впровадженні рішень MFA наступного покоління.

ОГЛЯД КІБЕРЗАГРОЗ, З ЯКИМИ ЗІШТОВХУЄТЬСЯ НАТО ВІД MANDIANT

9 липня компанія Mandinat оприлюднила власну оцінку кіберзагроз, з якими стикається Альянс та його члени. Серед основних загроз виділено:

- кібершпигунство, переважно з боку російської APT29 та китайських APT груп;
- руйнівні кібератаки, здійснювані російською APT44, хактивістами та кіберзлочинцями;
- дезінформація та інформаційні операції, пов'язані з діяльністю структур Пригожина, Ghost-writer/UNC1151, COLDRIVER;

Війна росії проти України посилила ці загрози, які також продовжують зростати самостійно.

ФІНАНСУВАННЯ КІБЕРБЕЗПЕКИ РІЗКО ЗРОСЛО У ДРУГОМУ КВАРТАЛІ 2024 РОКУ – ЗВІТ PINPOINT SEARCH GROUP

У звіті Pinpoint Search Group про фінансування кібербезпеки за 2-й квартал 2024 року виявлено незначне збільшення кількості транзакцій порівняно з 2-м кварталом 2023 року, але суттєве зростання загальної суми зібраного фінансування – на 71% порівняно з 1,9 мільярда доларів минулого року. Зростання обсягів фінансування з року в рік є позитивним показником для галузі, яка зазнала значних змін протягом останнього року.

APT45: ЦИФРОВА ВІЙСЬКОВА МАШИНА ПІВНІЧНОЇ КОРЕЇ – MANDIANT

У своєму новому звіті компанія Mandiant повідомляє, що APT45 є давнім північнокорейським кібероператором, який проводить шпигунські кампанії з 2009 року та поступово розширив свою діяльність до фінансово вмотивованих операцій, включаючи розробку та розгортання програм-вимагачів. Це відрізняє його від інших північнокорейських операторів.

Кластери активності, пов'язані з APT45, мають унікальну генеалогію сімейств зловмисних програм, відмінну від тих, що використовуються іншими північнокорейськими групами, такими як TEMP.Hermit та APT43. Серед угруповань, що діють з Корейської Народно-Демократичної Республіки (КНДР), APT45 найчастіше націлюється на критичну інфраструктуру. Діяльність цієї групи відображає геополітичні пріоритети режиму.

ЕКСПЕРТ АНАЛІТИЧНОГО ЦЕНТРУ CSIS ОПРИЛЮДНИВ ІНФОРМАЦІЙНУ ДОВІДКУ ЩОДО КІБЕРПОТЕНЦІАЛУ ASEAN

16 липня Юлія Брок, експерт аналітичного центру CSIS, оприлюднила інформаційну довідку про діючі та заплановані кіберініціативи АСЕАН (Асоціація держав Південно-Східної Азії). Довідка містить огляд існуючої Стратегії кібербезпеки АСЕАН, заходи боротьби з кіберзлочинністю, ініціативи з розвитку кіберпотенціалу країн-членів АСЕАН, а також питання обміну інформацією про кіберінциденти та навчання.

8. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

ЄВРОПЕЙСЬКИЙ СОЮЗ ТА УКРАЇНА ПРОВЕЛИ ТРЕТІЙ РАУНД КІБЕРДІАЛОГУ У БРЮССЕЛІ

Сторони домовилися про поглиблення співпраці у сфері кібербезпеки на тлі російського вторгнення та переговорів про вступ України до ЄС. Учасники діалогу підтвердили свою прихильність рамкам ООН щодо відповідальної поведінки держав у кіберпросторі, обговорили зміни в ландшафті кіберзагроз, останні законодавчі зміни, посилення кібердипломатії, а також заходи з розбудови кіберстійкості. Вони також домовилися посилити обмін інформацією щодо ситуативної обізнаності та використання режиму кіберсанкцій в рамках Інструментарію ЄС з кібердипломатії.

ЄС підкреслив свою готовність продовжувати підтримувати Україну у зміцненні її кіберстійкості, взаємодії та реагуванні на кіберзагрози, особливо щодо критичної інфраструктури та мереж. Сторони обговорили можливість України скористатися Резервом кібербезпеки ЄС та організувати додаткові тренінги для українських цивільних і військових установ. Також домовилися про проведення четвертого раунду Кібердіалогу у 2025 році.

НКЦК ОРГАНІЗУВАВ ПЕРШИЙ REGIONAL CYBER RESILIENCE FORUM У ЛЬВОВІ

24-25 липня у Львові відбувся перший Regional Cyber Resilience Forum. Цього разу навколо теми важливості посилення кібербезпеки у регіонах України об'єдналися представники держави та бізнесу, кіберком'юніті, технологічні компанії, провідні українські та міжнародні експерти галузі. Загалом впродовж двох днів форуму відбулося три панельні дискусії та понад 30 доповідей експертів та воркшопів, які охоплювали широкий спектр тем. Захід зібрав близько 400 учасників офлайн та онлайн. Також у рамках форуму відбулися регіональні командно-штабні навчання (ТТХ), у яких взяли участь представники Львівської ОВА та міської адміністрації, основних суб'єктів кібербезпеки України та об'єктів критичної інфраструктури регіону.

Regional Cyber Resilience Forum: Lviv організовано НКЦК та CRDF Global в Україні за підтримки Державного департаменту США та у співпраці зі Службою безпеки України, Державною службою спеціального зв'язку та захисту інформації України, Львівською обласною державною адміністрацією, Львівським державним університетом безпеки життєдіяльності ДСНС України.

ІТ-КОАЛІЦІЯ ПЕРЕДАЛА УКРАЇНІ МЕРЕЖЕВЕ ОБЛАДНАННЯ НА ПОНАД 2 МІЛЬЙОНИ ЄВРО

ІТ-коаліція, завдяки внескам Люксембургу та Данії, передала Україні мережеве обладнання та допоміжні ліцензії загальною вартістю понад 2 мільйони євро. Це обладнання посилить потужність центрів обробки даних та кіберзахисту Міністерства оборони та Збройних сил України.

Раніше ІТ-коаліція, яку очолюють Естонія та Люксембург, передала Збройним силам України ноутбуки, монітори та інше комунікаційне обладнання вартістю 900 тисяч євро. Загалом, на потреби розбудови ІТ-інфраструктури для Міністерства оборони та Сил оборони України, ІТ-коаліція вже передала допомоги на понад 5 мільйонів євро у межах внесків Великобританії, Данії, Литви, Латвії, Люксембургу та двосторонньої допомоги з боку Канади.

УКРАЇНА ПОДІЛИЛАСЬ З ПОСЛАМИ ЄС СВОЇМ ДОСВІДОМ ПРОТИСТОЯННЯ КІБЕРАГРЕСІЇ РФ

3 липня 2024 року представники НКЦК, на чолі з керівником служби з питань інформаційної та кібербезпеки Апарату РНБО України, секретарем НКЦК Наталією Ткачук, зустрілися з послами Європейського Союзу Комітету з питань політики та безпеки у Брюсселі. Захід, організований за підтримки Постійного представництва Естонії при ЄС, мав на меті поглибити розуміння поточних викликів та можливостей у сфері кібербезпеки в Україні серед послів ЄС. Українська делегація поділилася досвідом протистояння кіберагресії рф та надала рекомендації партнерам щодо посилення національної кібербезпеки. Наталія Ткачук зазначила, що зустріч є важливим кроком у зміцненні співпраці між Україною та ЄС у сфері кібербезпеки, наголосивши на необхідності посилення колективної кібероборони Європи через залучення українського досвіду.

МІНЦИФРА ТА ОФІС З РОЗВИТКУ ПІДПРИЄМНИЦТВА ТА ЕКСПОРТУ ЗА ПІДТРИМКИ USAID ЗАПУСТИЛИ ПРОГРАМУ З КІБЕРДІАГНОСТИКИ БІЗНЕСУ

Програми допоможе 500 українським компаніям скористатися безоплатними послугами з діагностики цифрової інфраструктури від кібербезпекових компаній. Загальний фонд програми — 1,5 мільйона доларів. Послуги з кібердіагностики допоможуть малим та середнім підприємствам перевірити цифрову інфраструктуру компанії на вразливості. Представники бізнесу зможуть безоплатно скористатися однією з трьох послуг:

- тест на проникнення;
- тест безпеки застосунку;
- оцінка вразливостей інформаційного середовища.

Для того, щоб отримати одну з трьох безоплатних послуг з кібердіагностики, необхідно: зареєструватися в спеціальному розділі порталу Дія.Бізнес, визначити послугу та взяти участь в аукціоні, засвідчити договір на порталі цифровим підписом та домовитися з надавачем послуг про дату проведення кібердіагностики.

ФАХІВЦІ ДЕРЖСПЕЦЗВ'ЯЗКУ ПОДІЛИЛИСЬ ДОСВІДОМ ПРОТИСТОЯННЯ КІБЕРЗАГРОЗАМ НА USA-UKRAINE CYBER BRIDGE ТА КОНФЕРЕНЦІЇ HACK THE CAPITOL У США

Представники Держспецзв'язку України взяли участь у заходах USA-Ukraine Cyber Bridge та конференції Hack the Capitol у Вашингтоні. В рамках USA-Ukraine Cyber Bridge, який організувала компанія CYBER RANGES, експерти з кібербезпеки у Вашингтоні та Києві заслухали доповіді представників Агентства кібербезпеки та захисту інфраструктури (CISA) та міжнародної організації MITRE. Крім того, учасники заходу взяли участь у панельних дискусіях та практичному тренінгу на основі сценаріїв, розроблених фахівцями CERT-UA, а також у конференції Hack the Capitol.

НКЦК, МІНВЕТЕРАНІВ ТА CRDF GLOBAL В УКРАЇНІ ВТРЕТЄ ПРОВЕЛИ НАВЧАННЯ ВЕТЕРАНІВ ЗА ПРОГРАМОЮ РЕІНТЕГРАЦІЇ «КІБЕРЗАХИСНИКИ»

У межах програми «Кіберзахисники» ветерани протягом п'яти місяців здобували знання та навички у сфері кібероборони та кіберзахисту для подальшого працевлаштування у державному та приватному секторах України. Навчання завершилось проведенням змагань з кібербезпеки (CTF) та урочистою церемонією нагородження випускників.

Метою проєкту є надання безкоштовної комплексної підтримки ветеранам та ветеранкам на їхньому шляху до нових кар'єрних можливостей у сфері кібербезпеки. Навчальна програма включала теоретичні та практичні заняття, інтенсивне вивчення англійської мови, професійні консультації щодо кар'єрного розвитку та психосоціальну підтримку.

За час роботи проєкту «Кіберзахисники» понад 100 ветеранів та ветеранок успішно завершили навчання, що дозволило їм суттєво покращити свої теоретичні знання та практичні навички у сфері кібербезпеки. Завдяки цьому вони стали більш конкурентоспроможними на ринку праці як у державному, так і в приватному секторах.

ДЕРЖСПЕЦЗВ'ЯЗКУ ПРОВЕЛА СЕМІНАР ДЛЯ ДЕРЖСЛУЖБОВЦІВ, ВІДПОВІДАЛЬНИХ ЗА КІБЕРБЕЗПЕКУ В ДЕРЖОРГАНАХ ТА НА ОКІ

Держспецзв'язку провела практичний семінар для вищих посадовців держави та фахівців, відповідальних за кібербезпеку в держорганах та на об'єктах критичної інфраструктури. Захід, організований спільно з Нацагентством з питань держслужби, Вищою школою публічного управління та за підтримки проєкту EU4PAR 2, залучив 50 представників з 35 держструктур. Учасники поглибили знання щодо оцінки захищеності інформаційно-комунікаційних систем, реєстрів інформаційно-комунікаційних систем та об'єктів критичної інформаційної інфраструктури, отримати навички пошуку та виявлення вразливостей, впровадження програм BugBounty. Це четвертий семінар з кібербезпеки цього року, що вже підвищив кваліфікацію 400 осіб.

ДЕРЖСПЕЦЗВ'ЯЗКУ ПРОВЕЛА НАВЧАННЯ З КІБЕРБЕЗПЕКИ ДЛЯ МІНОБОРОНИ ТА ІНШИХ ДЕРЖАВНИХ СТРУКТУР

У травні та червні Держспецзв'язку провела навчання з кібербезпеки для держслужбовців категорій «Б» та «В» Секретаріату Кабінету Міністрів України, Міністерства Оборони України, Верховного Суду та Державної служби України з питань праці. Участь взяли близько 200 фахівців. Спеціалісти CERT-UA навчали учасників розпізнавати ознаки кібератак, запобігати їм та нейтралізувати наслідки. Навчання спрямовані на зміцнення кіберзахисту України.

В УКРАЇНІ ВПЕРШЕ ПЕРЕВІРИЛИ КІБЕРБЕЗПЕКУ СИСТЕМИ DELTA ЗА СТАНДАРТАМИ РІВНЯ НАТО

Бойова система DELTA успішно пройшла перевірку інформаційної безпеки, підтвердивши відповідність своєї комплексної системи захисту інформації (КСЗІ) встановленим вимогам. Незалежну перевірку здійснила одна з провідних міжнародних консалтингових компаній, а діагностика кібербезпеки тривала півтора місяця.

У ході перевірки було проаналізовано 162 заходи захисту інформації, які використовуються в системі DELTA. Система, побудована на сучасних технологіях, відповідає вимогам щодо кіберзахисту за стандартами НАТО. Наступним кроком є введення системи DELTA в експлуатацію Силами оборони. Очікується, що система отримає широке розповсюдження у бойових підрозділах, забезпечуючи технологічну перевагу над ворогом.

УКРАЇНСЬКА РОЗВІДКА РАЗОМ ІЗ КІБЕРВОЛОНТЕРАМИ АТАКУВАЛА МАЙЖЕ СОТНЮ РОСІЙСЬКИХ ВЕБРЕСУРСІВ

15 липня 2024 року волонтерська хакерська спільнота спільно з кіберфахівцями ГУР МО України здійснила масштабну кібератаку на близько 100 вебресурсів у росії. Метою атаки було знищення внутрішньої інформації компаній, які обслуговують клієнтів з державного сектору росії, що причетні до ведення війни проти України. Зокрема, ураження зазнали – MITgroup, «Пермський завод промобладнання», «Об'єднані кранові технології» та «РУМОС-ЛАДА».

Внаслідок кібератаки, зовнішній вигляд уражених вебресурсів був змінений: замість звичних розділів на сайтах з'являлась лише свиняча голова і код помилки «404».

CERT-UA ПОПЕРЕДЖАЄ ПРО ФІШИНГОВІ АТАКИ З МЕТОЮ ВИКРАДЕННЯ ПОШТОВИХ АКАУНТІВ UKR.NET

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA зафіксувала протягом липня атаки хакерського угруповання UAC-0102. Вони мали на меті викрадення облікових записів поштового сервісу UKR.NET працівників державних органів, військовослужбовців, а також співробітників українських підприємств та організацій.

Зловмисники розсилали електронні листи з архівами, які містять HTML-файл. Після відкриття файлу користувачі потрапляли на фішинговий сайт, що імітує сторінку UKR.NET, де їхні логіни та паролі передавались злочинцям, а на комп'ютер завантажувався документ для відвернення уваги. Більше інформації на сайті CERT-UA: https://cert.gov.ua/article/6280183

ЗАФІКСОВАНО СПЛЕСК АКТИВНОСТІ БІЛОРУСЬКИХ ХАКЕРІВ

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA зафіксувала сплеск активності білоруського хакерського угруповання UAC-0057 з 12 по 18 липня. Зловмисники поширювали документи з макросами для запуску шкідливого ПЗ PICASSOLOADER, що встановлювало бекдор Cobalt Strike Beacon. Тематика файлів-приманок стосувалась фінансово-економічних показників, оподаткування та реформ місцевого самоврядування, включаючи проєкт «HOVERLA», що реалізується за підтримки Агентства США з міжнародного розвитку (USAID). Більше інформації на сайті CERT-UA: https://cert.gov.ua/article/6280159

ХАКЕРИ ВИКОРИСТАЛИ ШКІДЛИВИЙ МАКРОС У WORD-ДОКУМЕНТІ ДЛЯ АТАКИ НА НАУКОВО-ДОСЛІДНУ УСТАНОВУ УКРАЇНИ

CERT-UA дослідила кібератаку угруповання UAC-0063 на українську науково-дослідну установу, що сталась 8 липня 2024 року. Зловмисники отримали доступ до облікового запису електронної пошти співробітника та розіслали шкідливий макрос у Word-документі, що призвело до встановлення програм HATVIBE та CHERRYSPY. Ці програми надали хакерам несанкціонований доступ до комп'ютерів. У процесі дослідження було виявлено, що атаки з використанням схожих засобів також могли відбуватися проти Міністерства оборони Республіки Вірменія.

Є підстави асоціювати цю злочинну активність з угрупуванням APT28 (UAC-0001), що афілійоване з військовою розвідкою рф. Детальніше про технічну сторону та індикатори загроз читайте на сайті CERT-UA.

CERT-UA ЗАФІКСУВАЛА НОВІ КІБЕРАТАКИ НА УКРАЇНСЬКІ ОБОРОННІ ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ ТЕМИ ЗАКУПІВЕЛЬ БПЛА

Хакери, видаючи себе за державних працівників, розсилають електронні листи з ZIP-файлом, що містить PDF-документ із посиланням. Переходячи за посиланням, користувач завантажує шкідливу програму GLUEEGG, яка встановлює легітимний інструмент віддаленого доступу ATERA. Це надає зловмисникам контроль над комп'ютером жертви.

Ворожа активність відстежується за ідентифікатором UAC-0180. Це угруповання активно атакує співробітників оборонних підприємств та Сил оборони України, постійно оновлюючи арсенал різноманітних шкідливих програм, але їх зловмисна діяльність не обмежується Україною. Дізнайтесь більше про деталі інциденту на сайті CERT-UA: https://cert.gov.ua/article/6280099

В УКРАЇНІ СУДИТИМУТЬ ЗЛОЧИННУ ГРУПУ, ЯКА ПРИВЛАСНИЛА ПОНАД 6 МЛН ГРИВЕНЬ З РАХУНКІВ ПІДПРИЄМСТВ І ВИКРАЛИ СВОГО СПІЛЬНИКА

В Україні викрили злочинну групу, яка викрадала кошти з банківських рахунків провідних промислових підприємств України. Зловмисники використовували шкідливе програмне забезпечення для отримання віддаленого доступу до фінансових операцій компаній, завдаючи збитків на суму понад 6 млн грн. В результаті конфлікту всередині групи, двоє членів викрали свого спільника, вимагаючи його частку «доходу». Поліція затримала злочинців, і тепер їм загрожує до 12 років ув'язнення з конфіскацією майна.

КІБЕРПОЛІЦІЯ ВИКРИЛА ГРУПУ ШАХРАЇВ, ЯКІ ОШУКАЛИ ДЕСЯТКИ ЛЮДЕЙ ЗА СХЕМОЮ «ДРУГ ПРОСИТЬ У БОРГ»

Кіберполіція Прикарпаття викрила групу шахраїв, які зламували облікові записи в соцмережах та розсилали повідомлення від імені власників із проханням позичити гроші. Схему організували троє жителів Запорізької області та один мешканець Прикарпаття, які діяли з серпня 2023 по січень 2024 року. Шахраї ошукали півсотні людей, отримавши кошти на підконтрольні банківські рахунки. Обвинуваченим загрожує до п'ятнадцяти років позбавлення волі.

9. ПЕРША СВІТОВА КІБЕРВІЙНА

У ЗЛОМІ TEAMVIEWER ОФІЦІЙНО ЗВИНУВАЧУЮТЬ РОСІЙСЬКИХ КІБЕРШПИГУНІВ

1 липня видання Security Week повідомило, що TeamViewer підтвердив, що нещодавня хакерська атака на системи компанії була здійснена російською кібершпигунською групою APT29, також відомою як Midnight Blizzard. Ця група відзначається потужними атаками на важливі організації, такі як Microsoft. Спочатку повідомлялося, що злам не вплинув на середовище продукту, платформу підключення TeamViewer або дані клієнтів. Однак 4 липня компанія повідомила, що APT29 змогла скопіювати дані каталогу співробітників, включаючи імена, корпоративну контактну інформацію та зашифровані паролі для внутрішнього IT-середовища компанії. Водночас TeamViewer зазначив, що злам, здається, було локалізовано.

РОСІЯ ЗАБОРОНИЛА СВОЇМИ ВІЙСЬКОВОСЛУЖБОВЦЯМИ КОРИСТУВАТИСЬ МОБІЛЬНИМИ ТЕЛЕФОНАМИ НА ЛІНІЇ ЗІТКНЕННЯ

24 липня російський парламент ухвалив закон, який посилює покарання для військовослужбовців за особисте використання інтернет-пристроїв. Закон класифікує володіння пристроями, що дозволяють військовослужбовцям зберігати або надсилати відео, фотографії чи геолокаційні дані в Інтернеті, як злочин, який карається триманням під вартою до 15 днів. Закон також забороняє передачу будь-якої інформації, яка може бути використана для ідентифікації російських військ та їхнього місцеперебування.

РОСІЙСЬКІ ХАКЕРИ ПОСИЛИЛИ АТАКИ НА ФІНСЬКІ САЙТИ

На початку липня численні фінські сайти стали жертвами DoS-атак, які, за даними Центру кібербезпеки, здійснює російська хакерська група NoName. Об'єктами цих кібератак стали, зокрема, Міністерство фінансів, Податкова служба, банк Osuuspankki та мережеві служби Гельсінкі.

APPLE ВИДАЛЯЄ VPN-ПРОГРАМИ З РОСІЙСЬКОГО APP STORE ПІД ТИСКОМ УРЯДУ

4 липня 2024 року Apple видалила численні програми віртуальної приватної мережі (VPN) з свого App Store у росії на вимогу роскомнадзору. Це видалення стосувалося мобільних застосунків від 25 постачальників послуг VPN, серед яких Hidemy.name VPN, Le VPN, NordVPN, PIA VPN, Planet VPN, Proton VPN і Red Shield VPN, як повідомляють Інтерфакс і MediaZona. Варто зазначити, що NordVPN вже закрила всі свої російські сервери у березні 2019 року. Red Shield VPN розкритикувала дії Apple, зазначивши: «Дії Apple, мотивовані бажанням зберегти доходи від російського ринку, активно підтримують авторитарний режим. Це не тільки безрозсудно, але й є злочином проти громадянського суспільства».

КИТАЙ ВІДКИДАЄ ЗВИНУВАЧЕННЯ У ДІЯЛЬНОСТІ VOLT TYPHOON І ЗВИНУВАЧУЄ АЛЬЯНС «П'ЯТЬ ОЧЕЙ» В КОМПАНІЇ ДЕЗІНФОРМАЦІЇ

19 липня було опубліковано спільний звіт під назвою Lie to Me: A Secret Disinformation Campaign Targeting, підготовлений низкою китайських організацій у сфері кібербезпеки, зокрема Національним центром екстреного реагування на комп'ютерні віруси, Національною інженерною лабораторією технологій захисту від комп'ютерних вірусів і постачальником послуг безпеки 360 Digital Security Group. У звіті стверджується, що вся інформація, яка поширювалася про групу Vault Typhoon в останні місяці, є результатом кампанії з дезінформації, організованої АНБ США, ФБР та іншими урядовими відомствами США, зокрема Міністерствами юстиції, оборони, внутрішньої безпеки та енергетики, за участю розвідувальних служб країн «П'яти очей».

ПОЛКОВНИК ЦАХАЛ ПОВІДОМЛЯЄ ПРО ВІДБИТТЯ 3 МЛРД КІБЕРАТАК З ОСЕНІ 2023 РОКУ

Один з командувачів Армії оборони Ізраїлю (ЦАХАЛ), полковник Рахелі Дембінський, повідомив, що з осені минулого року ЦАХАЛ зазнав близько 3 мільярдів кібератак. Дембінський зазначив, що багато з цих атак спрямовані на критично важливі військові функції, зокрема на обмін інформацією між сухопутними силами. Значна частина цих кібератак пов'язана з політично мотивованими хакерськими групами, які намагаються приєднатися до боротьби проти Ізраїлю у війні.

ПІВНІЧНОКОРЕЙСЬКА КІБЕРГРУПА ПРОВОДИТЬ ГЛОБАЛЬНУ ШПИГУНСЬКУ КАМПАНІЮ З МЕТОЮ ПРОСУВАННЯ ВІЙСЬКОВИХ І ЯДЕРНИХ ПРОГРАМ ПІВНІЧНОКОРЕЙСЬКОГО РЕЖИМУ

25 липня ФБР США спільно з партнерами випустило консультаційний документ з кібербезпеки, в якому висвітлено діяльність кібершпигунства, пов'язану з 3-м бюро Головного розвідувального управління Корейської Народно-Демократичної Республіки (КНДР), яке базується в Пхеньяні та Сінуюджу. Третє бюро включає спонсоровану державою кібергрупу КНДР, таку як Andariel, Onyx Sleet, DarkSeoul, Silent Chollima та Stonefly/Clasiopa. Ця група націлена на оборонні, аерокосмічні, ядерні та інженерні організації з метою отримання конфіденційної та секретної технічної інформації, а також інтелектуальної власності. Учасники 3-го бюро фінансують свою діяльність через ransomware, націлений на установи охорони здоров'я США.

НІМЕЧЧИНА ЗВИНУВАТИЛА КИТАЙ У КІБЕРАТАЦІ НА КАРТОГРАФІЧНЕ АГЕНТСТВО У 2021 РОЦІ

31 липня Німеччина звинуватила Китай у причетності до кібератаки в 2021 році на федеральне картографічне агентство, викликавши посла Пекіна в Берліні для подання офіційної скарги. Метою атаки було шпигунство. Хакерам вдалося скомпрометувати кінцеві пристрої приватних осіб та компаній. Федеральне агентство картографії та геодезії Німеччини (BKG) відіграє важливу роль для організацій, пов'язаних із критичною інфраструктурою.

НОВА ГРУПА APT CLOUDSORCERER НАЦІЛЕНА НА ДЕРЖАВНІ УСТАНОВИ РОСІЇ

Раніше незадокументована група APT, що отримала назву CloudSorcerer, була помічена в атаках на російські державні установи, використовуючи хмарні служби для командування та контролю (C2) і викрадання даних.

Компанія Kaspersky, яка виявила цю активність у травні 2024 року, заявила, що механізм, розроблений зловмисниками, подібний до CloudWizard, але має відмінності у вихідному коді шкідливого ПЗ. Атаки використовують інноваційну програму збору даних і низку тактик ухилення для приховування слідів.

МІНІСТЕРСТВО ЮСТИЦІЇ США ЛІКВІДУВАЛО РОСІЙСЬКУ БОТОФЕРМУ НА ОСНОВІ ШІ

9 липня Міністерство юстиції США повідомило, що російська державна новинна мережа RT розробила, а федеральна служба безпеки керувала ботофермою, підсиленою штучним інтелектом, для поширення дезінформації з метою розпалювання розбрату в Сполучених Штатах та інших країнах. Міністерство юстиції оголосило про арешт двох доменних імен і обшук у 968 облікових записах соціальних мереж у зв'язку з цією операцією. Директор ФБР Крістофер Рей зазначив, що це перший випадок, коли США зруйнували роботу ботоферми, «підсиленої ШІ».

KASPERSKY ЗАЛИШАЄ РИНОК США ПІСЛЯ ЗАБОРОНИ З БОКУ МІНІСТЕРСТВА ТОРГІВЛІ

російський постачальник засобів безпеки Kaspersky оголосив про вихід з американського ринку майже через місяць після того, як Міністерство торгівлі США оголосило про заборону продажу його програмного забезпечення через ризики для національної безпеки. Також передбачається, що внаслідок цього у США буде звільнено до 50 співробітників компанії.

США ЗАПРОВАДИЛИ САНКЦІЇ ПРОТИ РОСІЙСЬКИХ ХАКЕРІВ УГРУПОВАННЯ CARR

Міністерство фінансів США оголосило про введення санкцій проти двох керівників кіберзлочинного угруповання Cyber Army of russia Reborn (CARR), яке здійснює атаки на об'єкти критичної інфраструктури по всьому світу.

КІБЕРАТАКА НА EVOLVE BANK РОЗКРИЛА ДАНІ 7,6 МІЛЬЙОНІВ КЛІЄНТІВ

9 липня Evolve Bank and Trust повідомив генерального прокурора штату Мен про кібератаку, яка на початку цього року торкнулася щонайменше 7,6 мільйонів його клієнтів. Атаку здійснила російська група, що займається програмами-вимагачами, Lockbit. Повний масштаб нападу поки невідомий, оскільки слідство триває. У заяві не вказано, які саме типи даних були скомпрометовані, але банк раніше підтвердив, що імена, номери соціального страхування, реквізити банківських рахунків і контактна інформація клієнтів персональних банківських послуг були доступні.

РЯДОВУ АВСТРАЛІЙСЬКИХ СИЛ ОБОРОНИ І ЇЇ ЧОЛОВІКА ЗВИНУВАЧУЮТЬ У ШПИГУНСТВІ НА КОРИСТЬ РОСІЇ

Федеральне правоохоронне агентство стверджує, що сімейна пара вступила в змову з метою отримання конфіденційної інформації після того, як жінка поїхала до росії під час тривалої відпустки у 2023 році. За даними правоохоронців, вона доручила своєму чоловікові, який залишився в Австралії, увійти до її офіційного робочого облікового запису, отримати доступ до певної інформації та надіслати її на її особистий електронний аккаунт, поки вона перебувала за кордоном.

НАЙБІЛЬШИЙ ХАКЕРСЬКИЙ АЛЬЯНС ПЛАНУЄ АТАКУВАТИ НАТО, ЄВРОПУ, УКРАЇНУ ТА ІЗРАЇЛЬ

23 липня видання CyberNews повідомило, що коаліція хакерів High Society, до складу якої входить близько 20 кіберугруповань, включаючи проросійські групи, такі як «Кіберармія росії» та UserSec, об'єднується з іншою хакерською групою, «Союзом 7 жовтня», щоб створити нову коаліцію під назвою «Священна Ліга». Хактивісти стверджують, що коаліція нараховує 70 активних хакерських груп, хоча список кіберугруповань, опублікований на каналі зв'язку «Священної Ліги», включає 55 учасників. Все спілкування на каналі здійснюється англійською та російською мовами. Альянс заявив, що його діяльність є відповіддю на арешт іспанським урядом членів групи NoName.