НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

УКРАЇНСЬКА ФУНДАЦІЯ БЕЗПЕКОВИХ СТУДІЙ

CYBER DIGEST

Огляд подій в сфері кібербезпеки,
серпень 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

У серпні США зосередили увагу на виборчому процесі через спроби зламу інформаційних систем обох президентських команд, причому команда Трампа звинуватила іранських хакерів. Компанії Microsoft, Google і Meta також повідомили про зростання іранської кіберактивності, пов'язаної з виборами. 19 серпня Офіс директора національної розвідки (ODNI), ФБР та CISA зробили спільну заяву про посилення іранських спроб втручання у вибори США. Іран заперечив свою причетність, проте Держдепартамент США оголосив винагороду в 10 мільйонів доларів за інформацію про шістьох іранських хакерів, підозрюваних у кібератаках на системи водопостачання наприкінці 2023 року.

Європейські країни посилюють кібербезпеку, зосереджуючись переважно на поглибленні міждержавної співпраці та запровадженні стимулів на загальноєвропейському рівні. Швейцарія планує приєднатися до двох безпекових проєктів у рамках Програми постійного структурованого співробітництва ЄС (PESCO), один із яких безпосередньо стосується посилення кібербезпеки – проєкт «Федерація кіберполігонів». Водночас ENISA запустила нову програму для підтримки держав-членів ЄС, дозволяючи європейським постачальникам послуг кібербезпеки надавати відповідні послуги країнам ЄС та їхнім об'єктам критичної інфраструктури відповідно до положень Директиви NIS2. Бюджет ініціативи становить 28,3 мільйона євро.

Постквантове шифрування знову стало важливою темою в урядових та експертних дискусіях після оприлюднення NIST стандартів для трьох базових алгоритмів, стійких до квантових обчислень. Великобританія вже включила ці стандарти у свої стратегічні документи. Також дослідження RAND, опубліковане в серпні, вивчає можливості квантових обчислень і штучного інтелекту для зміцнення потенціалу Міністерства національної безпеки США. Штучний інтелект переходить до реальної імплементації: CISA призначила керівника відділу ШІ, а NSA запускає платформу автоматизованого тестування на проникнення на основі ШІ. Експерти аналізують вплив ШІ на кібербезпекові операції.

Промислові об'єкти та кібербезпека операційних технологій (OT) стали пріоритетом для урядових структур. Згідно зі звітом Censys, майже половина з 40 000 підключених до Інтернету промислових систем управління (ICS) у США є вразливими через слабкі протоколи безпеки, особливо в системах автоматизації будівель. На тлі кібератак на Halliburton та Microchip, дослідники відзначають проблеми координації між IT та OT командами у багатьох організаціях (як показує звіт Cisco, це стосується майже половини компаній). Окреме занепокоєння викликає безпека систем водопостачання: Управління звітності уряду США (GAO) закликало Агентство з охорони довкілля провести термінову комплексну оцінку ризиків у всьому секторі та розробити стратегію з урахуванням ризиків.

Україна продовжує зміцнювати міжнародні партнерства у сфері кібербезпеки. У серпні 2024 року відбулися кілька важливих подій: шостий раунд Кібердіалогу Україна–США (обговорювались питання сучасного ландшафту кіберзагроз, захист критичної інфраструктури, кіберсанкції та кібердипломатія), зустріч представників НКЦК з Посольством Японії та JICA (розглянуто можливість навчання японських колег українськими фахівцями), а також підписання Меморандуму про співпрацю у сфері кібербезпеки та кіберзахисту між Держспецзв'язку та Міністерством оборони Латвії.

CERT-UA продовжує відстежувати ворожі кібератаки з використанням електронних листів. У серпні було зафіксовано дві такі атаки. Перша використовувала тему військовополонених з Курського напрямку з розсилкою шкідливого архіву «spysok_kursk.zip», що містив шпигунські програми SPECTR і FIRMACHAGENT. Друга атака розсилала листи нібито від СБУ з файлом «Документи.zip», завантаження якого запускає шкідливу програму ANONVNC. Для протидії ворожій кіберактивності Україна вдається до пошуку інноваційних рішень. Зокрема Мінцифри та Держспецзв'язку провели Cybersecurity Innovations Hackathon, де понад 200 учасників розробляли рішення для захисту від небезпечних кіберпродуктів та модернізації кіберсистем в енергетичному секторі.

Україна, за підтримки міжнародних партнерів, активно розвиває систему підготовки кадрів у сфері кібербезпеки, акцентуючи на практичних заходах. За ініціативи НКЦК у Національному авіаційному університеті було презентовано перший національний кіберполігон Cyber Range UA. Також у Київському політехнічному інституті ім. Ігоря Сікорського відкрито «Лабораторію кібербезпеки автоматизованих систем управління». Інфраструктура лабораторії фактично дублює середовище промислової системи управління, моделюючи реальні ситуації у різних секторах, як-от: виробництво, водопостачання та комунальна сфери. У серпні відбулись кіберзмагання INCIDENT RESPONSE DAYS 3.0, в яких взяли участь 100 студентів і фахівців з кібербезпеки державного сектору.

Глобальне кіберпротистояння набирає обертів, залучаючи нових учасників. російсько-українська кібервійна залишається центральним елементом цього протиборства, проте ареал активності політично мотивованих хакерів розширюється. Міжнародні дослідники зазначають, що росія змінює фокус кібератак з українських організацій на особисті мобільні пристрої військовослужбовців і співробітників сектору безпеки. Паралельно з російсько-українським фронтом зростає активність навколо Тайваню, де кіберугруповання, ймовірно пов'язані з КНР, збільшують атаки. США або Ізраїль підозрюють в атаці на Центральний банк Ірану.

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

ENISA ПЛАНУЄ РОЗПОДІЛИТИ 28 МЛН ЄВРО НА ПІДТРИМКУ КІБЕРБЕЗПЕКИ КРАЇН-ЧЛЕНІВ ЄС

9 серпня ENISA оприлюднила нову програму, спрямовану на підвищення рівня кіберзахисту в ЄС. У рамках цієї ініціативи оголошено конкурс для європейських постачальників послуг кібербезпеки, які бажають долучитися до надання послуг країнам ЄС і їхнім об'єктам критичної інфраструктури відповідно до Директиви NIS2. Програма реалізується в межах Програми цифрової Європи (DEP), для її реалізації планується використати 28,3 млн євро.

CISA ВИПУСТИЛА «ПОСІБНИК ІЗ ПРИДБАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ДЕРЖАВНИХ ПІДПРИЄМСТВ», ЗОСЕРЕДЖЕНИЙ НА ПИТАННЯХ ЖИТТЄВОГО ЦИКЛУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

1 серпня CISA випустила «Посібник з придбання програмного забезпечення для державних підприємств» (C-SCRM), розроблений Цільовою групою з управління ризиками ланцюга постачання інформаційно-комунікаційних технологій (ICT SCRM). Цей документ надає рекомендації для державних організацій щодо придбання програмного забезпечення з метою мінімізації ризиків, пов'язаних із життєвим циклом програмного забезпечення та загрозами, які можуть виникати через компрометацію ланцюга постачання.

CISA ЗАПУСТИЛА НОВИЙ ПОРТАЛ ДЛЯ ПОКРАЩЕННЯ КІБЕРЗВІТНОСТІ

29 серпня CISA оголосила про перенесення форми звітності про кіберінциденти на новий Портал послуг (CISA Services Portal) як частину зусиль з покращення процесу звітності. Новий портал пропонує безпечну платформу з розширеними можливостями, такими як інтеграція з login.gov, збереження та оновлення звітів, можливість обміну ними з колегами або клієнтами, а також пошук і фільтрація звітів. Нова функція співпраці дозволяє користувачам брати участь у неформальних обговореннях з представниками CISA.

NCCC ВЕЛИКОБРИТАНІЇ ОПРИЛЮДНИВ НОВУ СХЕМУ СЕРТИФІКАЦІЇ – АУДИТ КІБЕРСТІЙКОСТІ

CAF це набір вимог кібербезпеки, що тісно пов'язаний із вимогами NIS Directive і стосується підтвердження стану кібербезпеки для всіх OKI Великобританії.

15 серпня Національний центр кібербезпеки Великобританії (NCCC) оголосив про запуск нової схеми сертифікації – аудиту кіберстійкості (Cyber Resilience Audit, CRA). Ця ініціатива спрямована на створення реєстру постачальників, які зможуть проводити незалежні аудити інформаційної безпеки на основі Cyber Assessment Framework (CAF). CAF – це набір вимог до кібербезпеки, тісно пов'язаний з Директивою NIS, який підтверджує стан кібербезпеки для операторів критичної інфраструктури Великобританії.

АНБ США ЗАПУСКАЄ ПЛАТФОРМУ ДЛЯ АВТОМАТИЗОВАНОГО ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ПОСТАЧАЛЬНИКІВ

5 серпня керівник АНБ США Тімоті Хо оголосив про запуск нової платформи для автоматизованого тестування на проникнення (APT Tool), розробленої Агентством на основі технологій штучного інтелекту. Платформа призначена для підвищення рівня кібербезпеки, і її основними користувачами будуть постачальники АНБ та саме агентство.

DAPRA ПІДТРИМАЛА ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ У ПЗ З ВІДКРИТИМ КОДОМ, ЩО ВИКОРИСТОВУЄТЬСЯ КРИТИЧНОЮ ІНФРАСТРУКТУРОЮ США

13 серпня стало відомо, що Агентство передових оборонних дослідницьких проєктів США (DARPA) виділило по 2 мільйони доларів сімом дослідницьким командам для пошуку вразливостей у програмному забезпеченні з відкритим кодом, яке використовується в критичній інфраструктурі США. Ці команди були відібрані з 39 претендентів під час AI Cyber Challenge – спеціалізованого заходу, спрямованого на пошук найкращих фахівців для цього завдання. Для тестування дослідникам надали реальні фрагменти коду, в яких DARPA навмисно заклала помилки для виявлення.

СІНГАПУР ОНОВИВ ГЕНЕРАЛЬНИЙ ПЛАН КІБЕРБЕЗПЕКИ ОПЕРАЦІЙНИХ ТЕХНОЛОГІЙ

20 серпня Агентство кібербезпеки Сінгапуру (CSA) оголосило про оновлення національного Генерального плану кібербезпеки операційних технологій – OT Cybersecurity Masterplan 2024. Цей план, вперше прийнятий у 2019 році, охоплює всі об'єкти критичної інфраструктури країни. Оновлення включає кілька важливих напрямків:

- удосконалення підготовки кадрів з кібербезпеки OT;
- поліпшення обміну інформацією про кіберзагрози та оптимізація процесу звітування;
- підвищення стійкості операційних технологій до ризиків через ланцюжки постачання;
- впровадження підходу Secure by Design для OT-систем.

У США ПРЕДСТАВИЛИ ЗАКОНОПРОЄКТ CYBER READY WORKFORCE ACT ДЛЯ ЗАЛУЧЕННЯ КІБЕРФАХІВЦІВ

На початку серпня сенатори Джекі Роуз і Марша Блекберн представили законопроєкт Cyber Ready Workforce Act. Цей документ передбачає створення програми державних грантів для підтримки та розширення стажувальних програм з кібербезпеки по всій країні. Відповідальність за реалізацію ініціативи покладено на Міністерство праці США. Мета законопроєкту – залучити більше фахівців у сферу кібербезпеки як у державний, так і в приватний сектор, надаючи організаціям фінансову підтримку для підвищення кваліфікації своїх працівників, включно з отриманням сертифікацій та професійних навичок.

ДЕРЖДЕПАРТАМЕНТ США ОГОЛОСИВ ВИНАГОРОДУ В 10 МЛН ДОЛАРІВ ЗА ІНФОРМАЦІЮ ПРО ІРАНСЬКИХ ХАКЕРІВ

8 серпня Держдепартамент США оголосив винагороду в розмірі 10 мільйонів доларів за інформацію про шістьох іранських хакерів, причетних до атак на промислові системи управління водопостачанням у 2023 році. До розшукуваних осіб належать Хамід Хомаюнфал, Гамід Реза Лашгарян, Махді Лашгарян, Мілад Мансурі, Мохаммад Багер Ширінкар і Реза Мохаммад Амін Саберіан. Усі вони пов'язані з Корпусом вартових ісламської революції (КВІР) Ірану, зокрема з підрозділом кіберелектронного командування. Цих хакерів, які діяли під ім'ям групи Cyber Av3ngers, звинувачують у націленні на програмований логічний контролер (PLC) Unitronics Vision, що належить муніципальній системі водопостачання Аліквіппи, Пенсільванія.

CISA ПРИЗНАЧИЛА ПЕРШОГО КЕРІВНИКА ВІДДІЛУ ШТУЧНОГО ІНТЕЛЕКТУ

1 серпня CISA оголосила про призначення Ліси Ейнштейн на посаду керівника відділу штучного інтелекту. Раніше, з 2023 року, Ейнштейн виконувала обов'язки старшого радника CISA з питань ШІ, а з 2022 року обіймала посаду виконавчого директора Консультативного комітету з кібербезпеки CISA. У новій ролі вона буде відповідати за впровадження відповідальних підходів до використання ШІ для зміцнення кібербезпеки та підтримки власників і операторів критичної інфраструктури в США у забезпеченні безпеки та надійності застосування технологій штучного інтелекту.

СЕНАТ США ЗАТВЕРДИВ ПЕРШОГО КЕРІВНИКА НАПРЯМКУ КІБЕРПОЛІТИКИ МІНІСТЕРСТВА ОБОРОНИ

2 серпня Сенат США затвердив Майкла Салмайєра на посаду помічника Міністра оборони з питань кіберполітики – нової ролі, створеної в законопроєкті про оборонну політику на 2023 фінансовий рік. Відділ кіберполітики був заснований цього року для посилення кіберспроможностей Пентагону.

Раніше Салмайєр обіймав посади головного кіберрадника армії США, директора з планування та операцій з кіберполітики в Офісі міністра оборони, а також керував проєктом кібербезпеки в Гарвардському центрі Белфера. Він зазначив, що його основним пріоритетом стане нарощення «бойової потужності» та «стійкої готовності» цифрових сил країни.

США ГОТУЮТЬСЯ ЗАБОРОНИТИ ВИКОРИСТАННЯ КИТАЙСЬКОГО ПЗ В АВТОНОМНИХ АВТОМОБІЛЯХ

5 серпня ЗМІ повідомили, що США планують накласти повну заборону використання китайського програмного забезпечення в автономних і підключених до мережі транспортних засобах. Очікується, що адміністрація Байдена запропонує заборону найближчими тижнями, і вона охоплюватиме всі транспортні засоби з рівнем автоматизації 3 та вище.

Цей крок відповідає попереднім заявам американських офіційних осіб, зокрема міністра торгівлі Джини Раймондо, про те, що китайські технології можуть становити загрозу національній безпеці США.

ЗАКОНОПРОЄКТ АВТОРСТВА РОЗВІДКИ США ПРИРІВНЮЄ ПРОГРАМИ-ВИМАГАЧІ ДО ТЕРОРИСТИЧНОЇ ЗАГРОЗИ

6 серпня видання Cyberscoop повідомило, що Комітет з розвідки Сенату США підготував законопроєкт, який прирівнює програми-вимагачі до тероризму. Ініціатива класифікує угруповання ренсомвер як «ворожих іноземних кіберактерів», а країни, які їх підтримують, як «державних спонсорів програм-вимагачів», що підпадають під санкції. Законопроєкт також надає розвідувальній спільноті США більше повноважень для боротьби з кіберзлочинцями, підвищуючи ренсомвер до одного з пріоритетів національної розвідки.

Критики зазначають, що більшість країн, ймовірно, визнаних спонсорами ренсомверу, як-от росія та Північна Корея, вже під санкціями, тому вплив нових заходів може бути обмеженим. Крім того, законопроєкт може не врахувати мінливу та децентралізовану природу ренсомвер-груп, які часто розпадаються та відновлюються під різними назвами. Попри це, законопроєкт підкреслює ескалацію загрози ренсомвер та готовність США агресивно боротися з нею.

NIST ОПРИЛЮДНИВ ТРИ СТАНДАРТИ АЛГОРИТМІВ ДЛЯ ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ

14 серпня Національний інститут стандартів і технологій (NIST) опублікував три нові криптографічні алгоритми:

- **ML-KEM** (на основі CRYSTALS-Kyber) – для безпечного обміну криптографічними ключами;
- **ML-DSA** (відомий як CRYSTALS-Dilithium) – для створення та перевірки цифрових підписів;
- **SLH-DSA** (відомий як Sphincs+) – алгоритм цифрового підпису без збереження стану.

Деякі державні установи, як-от Національний центр кібербезпеки Великобританії (NCCC), вже почали оновлювати свої документи/рекомендації, зокрема публікуючи Білу книгу щодо постквантової криптографії, яка служить дорожньою картою для поступового впровадження постквантового шифрування у всіх секторах економіки. Приватні компанії, такі як Palo Alto Networks, також почали заявляти про підтримку нових алгоритмів у своїх продуктах.

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

КОМІТЕТ ООН ОДНОГОЛОСНО ПІДТРИМАВ ГЛОБАЛЬНИЙ ДОГОВІР ПРО КІБЕРЗЛОЧИННІСТЬ

9 серпня Організація Об'єднаних Націй ухвалила перший глобальний договір про кіберзлочинність, ініційований росією, який створює міжнародну правову базу для боротьби з кіберзлочинами та забезпечення доступу до даних. Після трьох років переговорів договір був одноголосно схвалений спеціальним комітетом ООН і восени буде винесений на голосування Генеральної Асамблеї для остаточного затвердження.

Хоча договір спрямований на боротьбу з глобальною кіберзлочинністю, її критикують правозахисні організації та технологічні компанії, які стверджують, що в ній відсутні адекватні гарантії для запобігання зловживанням цифровим спостереженням і доступом до даних. Проте держави-члени ООН досягли компромісу, вважаючи, що навіть недосконалий договір кращий, ніж його відсутність. Ця глобальна угода відрізняється від попередніх регіональних угод, таких як Будапештська конвенція тим, що представляє ширший консенсус.

БРИТАНІЯ ТА ФРАНЦІЯ ОБГОВОРЯТЬ ЗЛОВЖИВАННЯ КОМЕРЦІЙНИМИ ІНСТРУМЕНТАМИ КІБЕРВТОРГНЕННЯ

12 серпня видання The Record повідомило, що Велика Британія та Франція планують розпочати консультації щодо проблеми поширення та безвідповідального використання комерційних інструментів кібервторгнення, таких як шпигунське ПЗ. Ці консультації відбуватимуться в рамках ініціативи Pall Mall Process і залучатимуть представників держав, індустрії та громадянського суспільства для розробки належних практик використання таких інструментів. Ініціатива, започаткована в лютому за підтримки великих компаній, таких як Apple і Microsoft, має на меті встановити ширші стандарти для комерційних кіберінструментів злому. Проте експерти наголошують, що узгодження різних поглядів на інструменти кібервторгнення буде складним процесом.

ПІВДЕННА КОРЕЯ І США ПРОВЕЛИ СПІЛЬНІ НАВЧАННЯ ДЛЯ ПРОТИДІЇ ФІЗИЧНИМ ТА КІБЕРЗАГРОЗАМ З БОКУ ПІВНІЧНОЇ КОРЕЇ

З 19 по 29 серпня США та Південна Корея провели спільні навчання Ulchi Freedom Shield, спрямовані на підвищення готовності до реагування на збройні та кіберзагрози з боку Північної Кореї. Навчання включали різні сценарії, зокрема глушіння GPS, кібератаки та інші потенційні ворожі дії, з метою зміцнення спільної оборони обох країн.

ШВЕЙЦАРІЯ ПРИЄДНАЄТЬСЯ ДО ДВОХ БЕЗПЕКОВИХ ПРОЄКТІВ ЄС У РАМКАХ PESCO

21 серпня Швейцарія оголосила про плани приєднатися до двох проєктів у рамках Програми постійного структурованого співробітництва ЄС (PESCO), один з яких зосереджений на посиленні кібербезпеки – «Федерація кіберполігонів». Цей проєкт ЄС спрямований на об'єднання потенціалу країн для спільних кібернавчань, використання кіберполігонів та створення ефективної мережі взаємодії між фахівцями з кібербезпеки.

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

FBI ТА CISA: RANSOMWARE НЕ ВПЛИНЕ НА БЕЗПЕКУ ТА СТІЙКІСТЬ СИСТЕМ ГОЛОСУВАННЯ ТА ПІДРАХУНКУ ГОЛОСІВ

15 серпня ФБР і CISA випустили спільну заяву в рамках інформаційної кампанії щодо кіберзагроз під час виборів 2024 року. У заяві наголошується, що атаки програм-вимагачів (ransomware) не зможуть вплинути на безпеку та надійність процесів голосування та підрахунку голосів. Хоча такі атаки можуть спричинити локальні затримки в роботі державних чи місцевих мереж, вони не загрожують точності виборчого процесу. Виборчі органи використовують багаторівневі системи безпеки для захисту голосування та підрахунку від потенційних кібератак.

КОМАНДА ТРАМПА ЗАЯВИЛА ПРО КІБЕРАТАКУ З БОКУ ІРАНСЬКИХ ХАКЕРІВ

10 липня передвиборча команда Дональда Трампа повідомила про злам їхніх мереж іранськими хакерами. Це твердження було частково підтверджено компаніями Microsoft і Google, які заявили про спроби хакерської групи APT42, ймовірно пов'язаної з Іраном, атакувати кампанії обох політичних таборів, включаючи команду Каміли Гарріс. Meta також підтвердила можливі спроби зламу акаунтів WhatsApp, що належать посадовцям адміністрацій президента Джо Байдена та колишнього президента Трампа, і пов'язала ці атаки з тією ж групою. 19 серпня Офіс директора національної розвідки (ODNI), ФБР та CISA випустили спільну заяву, у якій підтвердили зростання хакерської активності з боку Ірану, спрямованої на вибори в США. Іран, своєю чергою, заперечив свою причетність до цих атак.

У DARKWEB ВИСТАВИЛИ НА ПРОДАЖ 2,9 МІЛЬЯРДА ЗАПИСІВ ПЕРСОНАЛЬНИХ ДАНИХ АМЕРИКАНЦІВ

8 квітня стало відомо, що компанія National Public Data, яка займається перевіркою репутації громадян у Флориді, стала жертвою хакерської групи USDoD. В результаті кібератаки в DarkWeb опинились 2,9 мільярда записів персональних даних американських громадян, загальний обсяг яких становить 277,1 ГБ. Як з'ясувалося, дані зберігалися у незашифрованому вигляді, а компанія тривалий час не повідомляла про злам. Крім того, вона не мала дозволу від власників даних на їхнє зберігання. У зв'язку з цим вже подано позов на відшкодування збитків проти компанії.

ХАКЕРИ ЗЛОВЖИВАЮТЬ БЕЗКОШТОВНИМ TRYCLOUDFLARE, ЩОБ РОЗМІСТИТИ ЗЛОВМИСНЕ ПЗ ДЛЯ ВІДДАЛЕНОГО ДОСТУПУ – PROOFPOINT

У своєму звіті, дослідники компанії наголошують, що зловмисники мають фінансову мотивацію, змінюють тактику, техніку та процедури, щоб покращити ефективність та уникнути виявлення, але на сьогодні компанія не готова атрибутувати їх діяльність якійсь з відомих загроз. Дослідження триває.

1 серпня видання Bleeping Computer повідомило, що дослідники компанії Proofpoint виявили зростаючу активність зловмисників, які зловживають сервісом Cloudflare Tunnel у кампаніях із розповсюдження шкідливого програмного забезпечення, яке зазвичай доставляє трояни віддаленого доступу (RAT). У своєму звіті Proofpoint зазначає, що зловмисники мають фінансову мотивацію, постійно адаптують свою тактику, техніки та процедури для підвищення ефективності атак і уникнення виявлення. Проте на сьогодні компанія не готова атрибутувати їх діяльність якійсь з відомих загроз. Дослідження триває.

ХАКЕРИ, ПОВ'ЯЗАНІ З КИТАЄМ, ЗЛАМАЛИ ІНТЕРНЕТ-ПРОВАЙДЕРА ДЛЯ ПОШИРЕННЯ ОНОВЛЕНЬ ШКІДЛИВОГО ПЗ

5 серпня видання The Hacker News повідомило, що компанія Volexity виявила діяльність китайської хакерської групи Evasive Panda, яка у середині 2023 року скомпрометувала неназваного інтернет-провайдера (ISP). Метою атаки було розповсюдження оновлень зловмисного ПЗ серед цільових компаній, що свідчить про новий рівень складності в тактиках цієї групи. Технічні деталі доступні у блозі компанії.

НОВА АТАКА SLUBSTICK ПІДВИЩУЄ НЕБЕЗПЕКУ ВРАЗЛИВОСТЕЙ ЯДРА LINUX

5 серпня видання Security Week повідомило, що дослідники з Технологічного університету Граца в Австрії представили нову техніку експлуатації ядра Linux під назвою SLUBStick. Ця техніка значно підвищує небезпеку вразливостей у системі керування пам'яттю (купі). SLUB-Stick демонструє високу ефективність, досягаючи успіху у понад 99% випадків, що робить його набагато небезпечнішим порівняно з іншими крос-кеш-атаками, які мають показник успіху близько 40%.

СПЛЕСК АТАК ПРОГРАМ-ВИМАГАЧІВ MAGNIBER ВПЛИВАЄ НА ДОМАШНІХ КОРИСТУВАЧІВ У ВСЬОМУ СВІТІ

Нова хвиля атак рансомверу Magniber активно націлюється на домашніх користувачів по всьому світу, шифруючи їхні пристрої та вимагаючи викуп у розмірі від 1000 до 5000 доларів. Запущений у 2017 році як наступник програми-вимагача Cerber, Magniber використовує різні методи зараження, включаючи експлуатацію вразливостей Windows, підроблені оновлення програмного забезпечення та злом ПЗ.

З 20 липня 2024 року значно зросла кількість жертв, які звертаються за допомогою після зараження через злом програмного забезпечення або генератори ключів. Magniber шифрує файли, додаючи випадкові розширення, та залишає записку про викуп з інструкціями щодо оплати через сайт Tor. На сьогодні не існує безкоштовних інструментів для розшифрування файлів, зашифрованих останніми версіями цього рансомверу.

PROOFPOINT ВИЯВИЛА НОВУ КІБЕРШПИГУНСЬКУ КАМПАНІЮ VOLDEMORT

29 серпня компанія Proofpoint опублікувала дослідження щодо кібершпигунської кампанії Voldemort. Невстановлений зловмисний суб'єкт використовує шкідливе програмне забезпечення Voldemort для збору розвідувальних даних з уражених систем. Дослідники відзначили поєднання сучасних тактик, технік і процедур (TTP) з нестандартними методами, такими як використання Google таблиць для командування та керування (C2) і зовнішніх ресурсів для зберігання файлів пошуку. Кампанія починається з фішингових листів, що імітують повідомлення податкових органів таких країн, як США, Велика Британія, Франція, Німеччина, Італія, Індія та Японія.

БАНДА ПРОГРАМ-ВИМАГАЧІВ ВИКОРИСТОВУЄ НОВЕ ПЗ SHARPRHINO ДЛЯ АТАК НА IT-ФАХІВЦІВ

Згідно зі звітом Quorum Cyber, міжнародна група програм-вимагачів Hunters International розпочала атаки на IT-фахівців за допомогою нового трояна віддаленого доступу (RAT) на базі C#, відомого як SharpRhino. Цей шкідливий інструмент використовується для проникнення у корпоративні мережі. Hunters International застосовує нову тактику, створюючи фальшиві вебсайти, що імітують легальні інструменти для мережевого сканування з відкритим кодом, намагаючись зламати облікові записи IT-працівників із підвищеними привілеями.

ВРАЗЛИВІСТЬ GITHUB ARTIPACKED НАРАЖАЄ РЕПОЗИТОРІЇ НА ПОТЕНЦІЙНЕ ПОГЛИНАННЯ

У звіті Palo Alto Networks Unit 42, опублікованому 13 серпня, повідомляється про виявлення нової вразливості в артефактах GitHub Actions під назвою ArtiPACKED. Ця вразливість може бути використана для захоплення репозиторіїв та отримання доступу до хмарних середовищ організацій.

КІБЕРАТАКА ПОРУШИЛА ВИРОБНИЧІ ОПЕРАЦІЇ MICROCHIP TECHNOLOGY

21 серпня видання Help Net Security повідомило про кібератаку на американського виробника напівпровідників Microchip Technology, яка порушила бізнес-операції компанії, включаючи роботу деяких виробничих потужностей та виконання замовлень.

Підозрілу активність виявили 17 серпня 2024 року, а 19 серпня компанія підтвердила, що неавторизована сторона скомпрометувала кілька серверів, що спричинило перебої в роботі. Microchip Technology ізолювала постраждалі системи та залучила фахівців з кібербезпеки для розслідування. Хоча повний масштаб атаки ще не визначений, неясно, чи була вона пов'язана з програмами-вимагачами або крадіжкою даних. Інцидент підкреслює зростаючу вразливість виробників напівпровідників до кіберзагроз.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

РИНОК КІБЕРСТРАХУВАННЯ В США ЗАЛИШАЄТЬСЯ ПРИБУТКОВИМ, АЛЕ РИЗИКИ ЗРОСТАЮТЬ

30 серпня у матеріалі SecurityIntelligence аналізується поточний стан ринку кіберстрахування в США. Хоча ринок залишається прибутковим, ризики продовжують зростати, а маржинальність поступово зменшується. Основною проблемою для страхових провайдерів є масштаб і складність кіберінцидентів, у яких вони повинні повністю покривати збитки. Відомий бізнесмен Воррен Баффет зазначив, що страхові агенти часто підписують нових комерційних клієнтів без належної оцінки кіберризиків, що створює ризикові умови для провайдерів, якщо вимоги підпадають під дію полісів, а витрати виходять з-під контролю.

РОЗБІЙНИЙ ШІ (ROGUE AI) ЯК СТРАТЕГІЧНА ЗАГРОЗА: ОЦІНКА TRENDMICRO

Вони пропонують виділити три види таких зловмисних ШІ: зловмисний
15 серпня фахівці компанії TrendMicro опублікували звіт про можливі загрози, пов'язані з концепцією «Розбійного ШІ» (Rogue AI) – систем штучного інтелекту, які можуть діяти проти інтересів своїх творців, користувачів або людства. TrendMicro виділяє три типи таких загроз:

- зловмисний ШІ, що використовується кіберзлочинцями для компрометації інших систем;
- випадковий розбійник, що виникає через людські помилки в розробці, коли ШІ дає неправильні результати на основі коректних даних;
- підривний ШІ, який зазнає вторгнення в легітимні системи управління ШІ, внаслідок чого починає функціонувати некоректно.

Ці загрози вимагають посилення заходів безпеки на всіх етапах розробки та використання штучного інтелекту.

ПОХМІЛЛЯ ВІД ШІ НАСТАЛО, І ЦЕ – КІНЕЦЬ ПОЧАТКУ

Після року ажіотажу навколо штучного інтелекту, ринок переходить у фазу корекції, особливо для таких гігантів, як Nvidia, Microsoft та Google. Як часто буває з новими технологіями, перший досвід впровадження не відповідає високим очікуванням. Проте ШІ продовжить розвиватися, рухаючись до глибшого розуміння та інтеграції в бізнес.

Попри потенціал генеративного ШІ, його недетермінований характер і високі витрати стримують масове впровадження. ШІ розглядається більше як вдосконалення існуючих інструментів, ніж їхня заміна. В секторах, як-от кібербезпека та підтримка клієнтів, ШІ демонструє перспективи, але вимагає суворого контролю та управління ризиками. Попри спад початкового ажіотажу, штучний інтелект залишається важливою технологією, що потребує обережного впровадження для мінімізації ризиків та максимізації користі.

ЗАГРОЗА ВИТОКІВ ДАНИХ ЧЕРЕЗ НЕМАРКОВАНІ НАБОРИ В GENAI ЗРОСТАЄ

22 серпня фахівці TrendMicro опублікували звіт, що наголошує на проблемі неструктурованих корпоративних даних при використанні генеративного штучного інтелекту (GenAI). Все більше компаній інтегрують GenAI для оптимізації процесів, використовуючи свої корпоративні набори даних для його навчання. Проте багато з цих наборів даних залишаються немаркованими, часто у формі скріншотів, що підвищує ризик випадкових витоків конфіденційної інформації.

5. КРИТИЧНА ІНФРАСТРУКТУРА

МІСТО КОЛУМБУС, ОГАЙО, РОЗСЛІДУЄ МОЖЛИВИЙ ВИТІК ДАНИХ ПІСЛЯ АТАКИ ПРОГРАМ-ВИМАГАЧІВ

Адміністрація міста Колумбус, штат Огайо, розслідує ймовірний витік конфіденційної муніципальної інформації після кібератаки, за яку відповідальність взяла хакерська група Rhysida. 1 серпня Rhysida заявила, що під час атаки 18 липня викрала 6,5 терабайта даних, що містять інформацію екстрених служб, доступ до міських камер та інші конфіденційні відомості. Зловмисники вимагають викуп у розмірі 1,9 мільйона доларів за не викриття даних.

НАФТОПРОМИСЛОВА КОМПАНІЯ США HALLIBURTON ПОСТРАЖДАЛА ВІД КІБЕРАТАКИ

21 серпня стало відомо, що одна з провідних нафтопромислових компаній США, Halliburton, зазнала кібератаки. Хоча деталі інциденту залишаються обмеженими, повідомляється, що атака вплинула на певні системи компанії.

ЗДІЙСНЕНО КІБЕРАТАКУ НА ВИРОБНИКА МІКРОСХЕМ MICROCHIP

17 серпня компанія Microchip Technology, один з провідних виробників напівпровідників і оборонний підрядник США, повідомила про виявлення несанкціонованого доступу до своїх серверів та порушення бізнес-операцій. Хоча деталі інциденту не розголошуються, відомо, що атака призвела до зниження виробничих потужностей компанії. Продукція Microchip активно використовується Міністерством оборони США, а також в автомобільній та аерокосмічній галузях.

ХАКЕРИ США ВИЯВИЛИ ВРАЗЛИВОСТІ В МАШИНАХ ДЛЯ ГОЛОСУВАННЯ, АЛЕ ЧАСУ НА ЇХ ВИПРАВЛЕННЯ ОБМАЛЬ

8 серпня видання Politico повідомило, що на конференції DEF CON у Лас-Вегасі американські хакери виявили прогалини в безпеці обладнання для президентських виборів США. Хоча злом, здатний зірвати вибори, є малоймовірним, експерти висловлюють занепокоєння, що будь-яка вразливість може бути використана для підриву довіри до результатів. Водночас очільниця CISA запевняє, що цього року кібербезпека виборчих процесів перебуває на найвищому рівні.

АГЕНТСТВО З ОХОРОНИ НАВКОЛИШНЬОГО СЕРЕДОВИЩА США ПОВИННЕ ПРИДІЛИТИ БІЛЬШЕ УВАГИ КІБЕРРИЗИКАМ ДЛЯ СИСТЕМ ВОДОПОСТАЧАННЯ

Згідно з новим звітом Управління звітності уряду США (GAO), Агентство з охорони навколишнього середовища (EPA) має терміново вирішити питання зростаючих кіберризиків для систем водопостачання та водовідведення. GAO зазначає, що інші федеральні агентства вже оцінювали ризики кібербезпеки в цьому секторі, тоді як EPA не провело повної оцінки та не розробило стратегію для управління кіберризиками. Звіт містить як причини виникнення, так і рекомендації для виправлення ситуації.

DRAGOS ПОВІДОМЛЯЄ, ЩО АТАКИ ПРОГРАМ-ВИМАГАЧІВ НА ПРОМИСЛОВІ СЕКТОРИ ЗРОСТАЮТЬ, ПІДВИЩУЮЧИ РИЗИК ДЛЯ ОТ-МЕРЕЖ

Кібербезпекова компанія Dragos повідомила про суттєве зростання атак програм-вимагачів у другому кварталі 2024 року. Хакерські угруповання адаптували свої стратегії, змінили бренди та почали використовувати нові тактики й вразливості. Попри втручання правоохоронних органів, кількість інцидентів з використанням рансомверу майже подвоїлася порівняно з першим кварталом, найбільше постраждав виробничий сектор. У звіті підкреслюється, що хоча атаки поки що не були спрямовані безпосередньо на системи керування промисловими процесами (ICS) або операційні технології (OT), взаємозв'язок між IT і OT-системами підвищує ризик збоїв, які можуть вплинути на роботу OT.

ПРОМИСЛОВІ СИСТЕМИ УПРАВЛІННЯ, ПІДКЛЮЧЕНІ ДО ІНТЕРНЕТУ, Є ВРАЗЛИВИМИ ДО АТАК

Згідно зі звітом кібербезпекової компанії Censys, майже половина з 40 000 підключених до Інтернету промислових систем управління (ICS) у США, особливо в секторі автоматизації будівель, є вразливими через слабкі протоколи безпеки. Багато з цих пристроїв, які працюють у мережах таких провайдерів, як Verizon і Comcast, використовують застарілі протоколи автоматизації без належної автентифікації. Понад 80% людино-машинних інтерфейсів (HMI) працюють у бездротових мережах, що робить їх вразливими для кібератак.

У звіті також зазначається, що багато систем водопостачання та водовідведення (WWS) мають незахищений доступ до HMI, що часто пов'язано з недостатньою обізнаністю та обмеженими ресурсами власників. Особливу загрозу створюють інтерфейси вебадміністрування, які використовують облікові дані за замовчуванням. Нещодавні кібератаки з боку державних суб'єктів, таких як Іран, Китай і росія, підкреслюють нагальну потребу в посиленні заходів безпеки, включаючи впровадження VPN, брандмауерів і надійної автентифікації.

ПОРТ СІЕТЛА ТА АЕРОПОРТ СІЕТЛ-ТАКОМА ПОСТРАЖДАЛИ ВІД ІМОВІРНОЇ КІБЕРАТАКИ

24 серпня Порт Сіетла, який включає міжнародний аеропорт Сіетл-Такома (Сі-Так), повідомив про «можливу кібератаку», яка порушила роботу його вебсайтів та телефонних систем. Збої почалися вранці 24 серпня і тривали до наступного дня. Аеропорт порадив мандрівникам використовувати застосунки авіакомпаній та планувати додатковий час на поїздки. Попри інцидент, робота аеропорту не була припинена. Атака відбулася на тлі зростаючої уваги до кібербезпеки в портах після нещодавнього указу адміністрації Байдена.

6. АНАЛІТИЧНІ ОЦІНКИ

41% IT ТА OT КОМАНД У ПРОМИСЛОВИХ КОМПАНІЯХ ПРАЦЮЮТЬ ОКРЕМО НАД ПИТАННЯМИ КІБЕРБЕЗПЕКИ – ЗВІТ CISCO

На початку серпня компанія Cisco оприлюднила звіт про стан промислових мереж великих компаній, заснований на опитуванні 1000 респондентів з 17 країн. Дослідження охопило організації з 20 секторів, включаючи виробництво, енергетику, комунальні послуги та транспорт. Одним із ключових висновків є низький рівень взаємодії між IT та OT командами, які відповідають за кібербезпеку: 41% опитаних підтвердили, що ці команди працюють окремо. Водночас 46% вважають, що впровадження систем штучного інтелекту може сприяти кращій координації між IT та OT. Щодо пріоритетів інвестицій, 31% респондентів назвали пристрої з підтримкою ШІ, а 30% – рішення для кібербезпеки.

ФРАНЦІЯ СТВОРИЛА ЕФЕКТИВНУ СИСТЕМУ КІБЕРЗАХИСТУ ПІД ЧАС ОЛІМПІЙСЬКИХ ІГОР – ОЦІНКА SECURITYINTELLIGENCE

23 серпня видання SecurityIntelligence підбило підсумки зусиль Франції у протидії кіберзагрозам під час проведення Олімпійських ігор. Незважаючи на 140 спроб кібератак, зафіксованих французьким агентством кібербезпеки ANSSI, зловмисникам не вдалося вплинути на захід. Успіх забезпечили такі заходи, як впровадження програми кіберпильності, переведення ANSSI у стан підвищеної готовності з постійним моніторингом, а також широке застосування штучного інтелекту для громадської безпеки, зокрема для виявлення загублених предметів через системи відеонагляду. Важливу роль відіграла й тісна співпраця з міжнародними партнерами, організована ще до початку змагань.

ШІ ТА КВАНТОВІ ОБЧИСЛЕННЯ МОЖУТЬ ЗНАЧНО ПІДВИЩИТИ ЕФЕКТИВНІСТЬ DHS – ЗВІТ RAND CORP

27 серпня експерти RAND Corp оприлюднили аналіз, який підкреслює потенційний вплив штучного інтелекту та квантових обчислень на діяльність Міністерства національної безпеки США (DHS). Серед ключових напрямів, на які ці технології матимуть найбільший вплив, зазначено кібербезпеку, криптографію та захист критичної інфраструктури. Це пов'язано як з розвитком захисних дій DHS (передусім CISA), так і посиленням спроможностей зловмисних акторів завдяки цим технологіям.

UNIT 42 ОПУБЛІКУВАВ ЗВІТ ПРО ОСНОВНІ ВЕКТОРИ КІБЕРАТАК У 2024 РОЦІ

7 серпня підрозділ кібербезпеки Palo Alto Networks, Unit 42, презентував «Звіт про реагування на інциденти у 2024 році». У звіті детально розглянуто основні вектори кібератак та надано рекомендації щодо їх пом'якшення. Документ вказує, що динаміка дослідження векторів кібератак свідчить про істотне зростання вразливостей ПЗ (38,6% у 2024 році) в якості основного вектора за період з 2021 по 2023 рік. Також суттєво зросло використання вкрадених облікових даних – до 20,5%. Водночас відзначено значне зниження частки атак, заснованих на фішингу та brute force.

ІРАН НАЦІЛЕНИЙ НА ВИБОРИ В США 2024 РОКУ – ЗВІТ MICROSOFT

8 серпня Microsoft оприлюднила звіт, у якому висвітлюється активність іранських хакерів, спрямована на вплив на вибори в США 2024 року. У звіті зафіксовано щонайменше чотири випадки, коли іранські угруповання намагалися втрутитися у виборчий процес. Це включає злам поштових скриньок учасників виборчих штабів обох кандидатів, а також спроби поляризувати американське суспільство через створення фейкових сайтів і новин за допомогою штучного інтелекту.

ЯК ФІШИНГОВІ АТАКИ ШВИДКО АДАПТУЮТЬСЯ ДО ПОТОЧНИХ ПОДІЙ – ДОСЛІДЖЕННЯ EGRESS

Згідно з дослідженням компанії Egress, у 2023 році 94% компаній постраждали від фішингових атак, що на 40% більше порівняно з попереднім роком. Однією з причин цього зростання є використання штучного інтелекту, особливо генеративного ШІ, який спрощує створення шкідливих електронних листів, контенту для фішингових кампаній і навіть діпфейків. ШІ також допомагає генерувати шкідливе програмне забезпечення, яке зловмисники використовують для зараження систем своїх жертв.

Іншим чинником зростання фішингових атак є «фішинг як послуга» (PhaaS), що дозволяє зловмисникам наймати професіоналів для проведення фішингових кампаній. Ця послуга робить атаки доступними навіть для людей з мінімальними технічними навичками, що сприяє подальшому зростанню кількості атак.

КІЛЬКІСТЬ DDOS-АТАК ЗРОСЛА НА 46% У ПЕРШІЙ ПОЛОВИНІ 2024 РОКУ – ЗВІТ GCORE RADAR

Згідно з даними звіту Gcore Radar, кількість DDoS-атак у першій половині 2024 року зросла на 46% порівняно з попереднім роком. Це суттєво вплинуло на індустрії ігор та технологій, які стали основними мішенями для зловмисників. Хакери застосовують дедалі більш витончені методи, що підкреслює важливість впровадження надійних і оперативних захисних стратегій у найбільш уразливих секторах.

ОГЛЯД ЛАНДШАФТУ ЗАГРОЗ У СЕРЕДИНІ 2024 РОКУ – ЗВІТ QUALYS

Згідно зі звітом компанії Qualys, на середину 2024 року кібербезпековий ландшафт характеризується такими ключовими загрозами:

- кількість зареєстрованих загальних вразливостей (CVE) зросла на 30%, досягнувши 22 254 порівняно з 17 114 у 2023 році, що підкреслює зростаючу проблему безпеки та потребу в покращенні заходів кібербезпеки;
- У 2024 році 0,91% вразливостей (204 випадки) були використані для реальних атак, що вимагає посилення цілеспрямованих заходів кіберзахисту;
- основні загрози включають використання загальнодоступних програм для початкового доступу та експлуатацію віддалених служб для латерального пересування в мережах;
- зафіксовано збільшення на 10% повторного використання старих CVE, що вказує на потребу в систематичному усуненні вже виявлених вразливостей.

CROWDSTRIKE РОЗКРИЛА ПРИЧИНУ ГЛОБАЛЬНИХ ЗБОЇВ СИСТЕМИ

Компанія з кібербезпеки CrowdStrike опублікувала детальний аналіз причини збою оновлення свого програмного забезпечення Falcon Sensor, який спричинив пошкодження мільйонів пристроїв Windows по всьому світу. Деталі доступні у звіті за посиланням: https://www.crowdstrike.com/blog/channel-file-291-rca-available/

ПОСИЛЕННЯ ТИСКУ: НОВІ ТАКТИКИ ПРОГРАМ-ВИМАГАЧІВ – АНАЛІЗ SOPHOS X-OPS

Компанія Sophos X-Ops опублікувала дослідження, яке виявило дедалі агресивніші тактики, що використовуються бандами програм-вимагачів для примушення жертв до сплати викупу. Окрім традиційних погроз опублікувати викрадені дані та інформувати клієнтів і ЗМІ про порушення, зловмисники застосовують нові методи:

- використання легітимних організацій, таких як ЗМІ, регуляторів та навіть правоохоронні органи, щоб посилити тиск на жертв;
- залучення постраждалих клієнтів і співробітників до вимог компенсації або судових процесів проти компаній, надаючи контактні дані генеральних директорів або власників бізнесу;
- використання викрадених даних для виявлення порушень законодавства або фінансових розбіжностей, що може завдати шкоди репутації;
- оператори програм-вимагачів критикують і висміюють жертв, намагаючись зобразити себе добродійниками;
- зловмисники все частіше публікують надзвичайно конфіденційні дані, включаючи медичні дані, зображення оголеного тіла та, в одному випадку, особисті дані доньки генерального директора тощо.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

В КИЄВІ ВІДБУВСЯ ШОСТИЙ РАУНД КІБЕРДІАЛОГУ УКРАЇНА–США

Учасники Діалогу обговорили сучасний ландшафт кіберзагроз, захист критичної інфраструктури, кіберсанкції та кіберуправління. Україна та США розглянули питання співпраці в кібердипломатії, боротьбі з кіберзлочинністю, інноваціях у сфері кібербезпеки, а також безпеки та конкурентоспроможності українських ІТ та телекомунікацій. Також обговорили шляхи надання кібердопомоги Україні, включаючи Талліннський механізм.

Заступник Секретаря РНБО Сергій Демедюк зазначив, що росія є однією з найбільших загроз як для України, так і для західних країн. Тому посилення співпраці, особливо в обміні аналітичною розвідкою кіберзагроз, між Україною та США є надзвичайно важливим для підвищення ситуаційної обізнаності та ефективності спільної протидії кіберзагрозам. Він також підкреслив необхідність створення в Україні Центру компетенції з кіберстійкості та висловив вдячність за підтримку США в зміцненні кібербезпеки України.

ЗА ІНІЦІАТИВИ НКЦК В УКРАЇНІ РОЗПОЧАВ РОБОТУ ПЕРШИЙ ВІТЧИЗНЯНИЙ КІБЕРПОЛІГОН CYBER RANGE UA

23 серпня в Національному авіаційному університеті відбулася презентація першого національного кіберполігону Cyber Range UA – віртуального середовища для емуляції інфраструктур та кібератак. Платформа дозволяє кільком десяткам кіберспеціалістів одночасно вчитись реагувати на інциденти в умовах, максимально наближених до реальних.

Кіберполігон наразі містить 15 сценаріїв і їх кількість буде постійно збільшуватися. Спочатку тренування проходитимуть представники державних установ, критичної інфраструктури та студенти НАУ. Платформа також буде доступна для приватних компаній та інших навчальних закладів, сприяючи обміну досвідом і взаємодії між різними секторами та суб'єктами забезпечення кібербезпеки для вдосконалення національної системи кібербезпеки.

Cyber Range UA – це спільний проєкт Національного координаційного центру кібербезпеки при РНБО України, Національного авіаційного університету та компанії Cyber Unit Technologies. Кіберполігон створено за підтримки CRDF Global в Україні та Державного департаменту США.

УРЯД ПІДТРИМАВ ЗАКОНОПРОЄКТ ПРО ЗАБОРОНУ ВИКОРИСТАННЯ РОСІЙСЬКИХ ПРОГРАМ

Уряд підтримав законопроєкт про заборону використання санкційних електронних ресурсів для посилення кіберзахисту. Законопроєкт, розроблений Держспецзв'язку за дорученням Ради національної безпеки і оборони України, посилює санкційне законодавство щодо переліку цифрових продуктів, створених російськими компаніями або будь-якими представниками країн, які мають стосунок до діяльності країн-агресорів чи терористичних організацій. Під заборону також потраплять сайти та сервіси, що становлять загрозу національній безпеці та належать або контролюються особами чи організаціями, щодо яких застосовано санкції.

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ ПРЕДСТАВИЛО НОВУ ПЛАТФОРМУ АРМІЯ+

Міністерство оборони України представило застосунок Армія+, який дозволяє подавати електронні рапорти, зменшуючи паперову роботу. Застосунок має 11 видів рапортів, згрупованих у чотири типи: «На відпустку», «На допомогу», «Направлення» і «Видача направлення». Рапорти можна подати за кілька хвилин, а підказки допоможуть заповнити їх правильно. Рапорти надсилаються на підпис за допомогою унікального номера військовослужбовця – Армія ID. Армія+ також містить опитування, завдяки яким держава зможе дізнатися думку військових з будь-яких питань, а самі військовослужбовці зможуть впливати на реальні зміни у Силах оборони України. Застосунок вже доступний у Play Market та App Store.

В КПІ ІМ. ІГОРЯ СІКОРСЬКОГО ВІДКРИЛИ НАВЧАЛЬНУ «ЛАБОРАТОРІЮ КІБЕРБЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ КЕРУВАННЯ»

Найсучасніша лабораторія допоможе 200 майбутнім та наявним операторам, відповідальним за критичну інфраструктуру, вдосконалити навички та знання для зменшення та усунення вразливостей в автоматизованих системах керування.

Інфраструктура лабораторії фактично дублює середовище промислової системи управління, моделюючи реальні ситуації у різних секторах, як-от: виробництво, водопостачання та комунальна сфери. Це полегшує проведення практичних експериментів і розширює можливості для навчання. Ініціативу реалізували за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України».

ІННОВАЦІЙНА СИСТЕМА DELTA УСПІШНО ВПРОВАДЖЕНА У ВСІ СИЛОВІ СТРУКТУРИ УКРАЇНИ

Екосистема інноваційних продуктів для ведення бойових дій DELTA, розроблена Міністерством оборони, продемонструвала високу ефективність на полі бою і вже введена в експлуатацію для усіх підрозділів сектору безпеки і оборони України. Рішення було ухвалено на ставці Верховного Головнокомандувача ЗСУ.

Міністр оборони Рустем Умєров повідомив, що система DELTA вже допомогла знищити ворожу техніку на суму понад 15 мільярдів доларів. Він також наголосив, що спільно з партнерами, зокрема Держспецзв'язку та СБУ, було модернізовано заходи безпеки для забезпечення ефективного використання DELTA.

Система DELTA, розроблена Центром інновацій Міноборони, пройшла аудит і відповідає сучасним стандартам комплексної системи захисту інформації. Цьогоріч вона пройшла успішні тестування п'яти різних стандартів взаємосумісності, а також інтегрувалась з польською системою управління артилерійським вогнем TOPAZ та відпрацювала складні сценарії збору даних про розташування власних сил і дружніх підрозділів.

ПРЕДСТАВНИКИ НКЦК ЗУСТРІЛИСЬ З ПОСОЛЬСТВОМ ЯПОНІЇ ТА JICA

Заступник Секретаря РНБО України та Керівника НКЦК Сергій Демедюк, керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Наталія Ткачук та керівник управління забезпечення діяльності НКЦК Сергій Прокопенко 19 серпня провели робочу зустріч з представниками Посольством Японії в Україні та Японського агентства міжнародного співробітництва (JICA). Під час зустрічі було обговорено результати співпраці у сфері кібербезпеки, зокрема масштабні кібернавчання Hackwave, які було проведено минулого року НКЦК спільно з JICA.

Також на запит японської сторони розглянули можливість проведення навчальних заходів українськими фахівцями для японських колег, з урахуванням унікального досвіду України у протидії кіберагресії в умовах повномасштабного воєнного вторгнення. Сторони також визначили подальші кроки для поглиблення співробітництва, зокрема розвиток Національної системи кібербезпеки, навчання та впровадження передових технологій.

ДЕРЖСПЕЦЗВ'ЯЗКУ ТА МІНІСТЕРСТВО ОБОРОНИ ЛАТВІЇ ПІДПИСАЛИ МЕМОРАНДУМ ПРО СПІВПРАЦЮ У СФЕРІ КІБЕРБЕЗПЕКИ ТА КІБЕРЗАХИСТУ

У рамках візиту делегації Міністерства оборони Латвійської Республіки до України було підписано Меморандум про взаєморозуміння між Міністерством оборони Латвії та Адміністрацією Держспецзв'язку України. Документ передбачає обмін інформацією про кіберінциденти, проведення спільних навчань та тренінгів, реалізацію спільних проєктів із досліджень у сфері кібербезпеки та кіберзахисту, а також обмін досвідом та кращими практиками з питань протидії кіберзагрозам.

НКЦК ПРОВІВ КІБЕРЗМАГАННЯ INCIDENT RESPONSE DAYS 3.0

Національний координаційний центр кібербезпеки при РНБО України за підтримки CRDF Global в Україні 22-23 серпня 2024 року провів дводенні кіберзмагання INCIDENT RESPONSE DAYS 3.0. У заході взяли участь близько сто студентів та фахівців з кібербезпеки державного сектору, які об'єдналися у 21 команду.

Метою змагань було підвищення кваліфікації спеціалістів та вдосконалення їх професійних навичок шляхом виконання завдань, наближених до реальних кіберінцидентів. Учасники розслідували інциденти, збирали артефакти та аналізували зловмисне програмне забезпечення, працюючи за унікальним сценарієм на національному кіберполігоні Cyber Range UA.

НА CYBERSECURITY INNOVATIONS HACKATHON СТВОРИЛИ РІШЕННЯ ДЛЯ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ І МОНІТОРИНГУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Cybersecurity Innovations Hackathon зібрав понад 200 учасників, які протягом восьми днів розробляли інноваційні рішення для захисту від небезпечних кіберпродуктів та модернізації кіберсистем в енергетичному секторі. У заході взяли участь розробники, фахівці з кібербезпеки та представники стартапів. Команди працювали над проєктами в трьох напрямах:

- технології із кібербезпеки на базі штучного інтелекту, машинного навчання, Big Data, захист промислових систем та розробка спеціальних проєктів.
- розробка рішень для захисту та покращення систем керування промисловими процесами в енергетичному секторі.
- розробка реального проєкту для замовника від партнера хакатону.

Переможцями хакатону стали команди A42, CyberForce та Fix It. Вони отримають менторську підтримку від Проєкту USAID «Кібербезпека критично важливої інфраструктури України» для подання на грантові програми, а також резидентство на пів року в першому інноваційному парку UNIT.City.

ГУР РОЗПОВІВ ПРО КІБЕРОПЕРАЦІЮ, ЯКА ПАРАЛІЗУВАЛА РОЗРОБНИКА ЯДЕРНОЇ ЗБРОЇ В РФ

Кіберфахівці ГУР МОУ разом з хакерською групою BO Team заявили про те, що успішно атакували підприємство, що розробляє ядерну зброю у Снєжинську (Челябінська область). Внаслідок атаки було виведено з ладу сервери та мережеве обладнання єдиного провайдера «Вега», залишивши без зв'язку та інтернету майже на тиждень стратегічні підприємства міста, включно з ВНИИТФ – розробником ядерних боєприпасів.

Внаслідок кібероперації отримано персональні дані працівників та документи заводу, що під санкціями. Це допоможе виявити механізми обходу санкцій і причетних осіб. Місцеві пабліки повідомляють про можливий зрив держоборонзамовлення рф.

НА ЧЕРНІГІВЩИНІ КІБЕРПОЛІЦЕЙСЬКІ ЛІКВІДУВАЛИ МЕРЕЖУ ШАХРАЙСЬКИХ КОЛ-ЦЕНТРІВ

Зловмисники видавали себе за співробітників банків і за допомогою спеціальних програм отримували доступ до банківських рахунків громадян. Шахраї створили бот у месенджері, через який заманювали жертв і змушували їх розкривати реквізити банківських карток. Використовуючи отриману конфіденційну інформацію, зловмисники незаконно проникали в інтернет-банкінг і переказували кошти на свої рахунки.

Загальні збитки від цих дій склали понад 5,4 мільйона гривень. Наразі триває досудове розслідування. Зловмисникам загрожує до восьми років позбавлення волі.

НА ХАРКІВЩИНІ СУДИТИМУТЬ ЧЛЕНІВ ЗЛОЧИННОГО УГРУПОВАННЯ, ЯКІ ПРИВЛАСНЮВАЛИ ОБЛІКОВІ ЗАПИСИ КОРИСТУВАЧІВ ІНТЕРНЕТУ

Кіберполіцейські викрили трьох членів організованої злочинної групи, які займалися викраденням облікових записів у соціальній мережі Instagram. У березні 2024 року оперативники встановили, що зловмисники використовували метод брутфорсу для підбору паролів із застосуванням спеціального програмного забезпечення. Після зламу акаунтів, фігуранти продавали отримані дані на даркнеті.

Правоохоронці завершили розслідування і направили до суду обвинувальний акт за фактами несанкціонованого втручання в роботу електронних комунікаційних систем та збуту інформації з обмеженим доступом. Зловмисникам загрожує до 15 років позбавлення волі.

CERT-UA ЗАФІКСУВАЛА КІБЕРАТАКИ ЗА ДОПОМОГОЮ ЕЛЕКТРОННИХ ЛИСТІВ З ТЕМАТИКОЮ ВІЙСЬКОВОПОЛОНЕНИХ КУРСЬКОГО НАПРЯМКУ

19 серпня урядова команда CERT-UA зафіксувала кібератаки з використанням електронних листів на тему військовополонених з Курського напрямку. Зловмисники розсилають електронні листи, які містять фотографії з зображеннями нібито військовополонених та посилання для завантаження архіву «spysok_kursk.zip». В архіві знаходиться файл з розширенням CHM та назвою «список вп, що вибувають. курск.»

Відкриття цього файлу призводить до завантаження на комп'ютер компонентів вже відомої шпигунської програми SPECTR, а також нової програми FIRMACHAGENT, призначенням якої є вивантаження викрадених даних на сервер управління.

За атаку відповідальне угруповання UAC-002

CERT-UA ЗАФІКСУВАЛА МАСОВЕ РОЗПОВСЮДЖЕННЯ ЕЛЕКТРОННИХ ЛИСТІВ ЗІ ШПЗ, ЯКІ НАДСИЛАЮТЬСЯ НІБИТО ВІД ІМЕНІ СБУ

12 серпня CERT-UA зафіксувала масове розповсюдження електронних листів зі шкідливим програмним забезпеченням, які надсилаються нібито від імені Служби безпеки України. Листи містять посилання на файл "Документи.zip", завантаження якого запускає шкідливу програму ANONVNC.

Ця програма дозволяє зловмисникам отримати прихований несанкціонований доступ до комп'ютера жертви. CERT-UA виявлено понад 100 уражених комп'ютерів, серед яких державні органи та органи місцевого самоврядування.

8. ПЕРША СВІТОВА КІБЕРВІЙНА

РОСІЯ ЗМІНЮЄ СТРАТЕГІЮ КІБЕРОПЕРАЦІЙ: ВІД АТАК НА ІНФРАСТРУКТУРУ ДО ПІДТРИМКИ НА ПОЛІ БОЮ

Останні повідомлення вказують на те, що росія змінила підхід до кібероперацій в Україні. російські кіберпідрозділи тепер зосереджуються на військових цілях, намагаючись скомпрометувати пристрої, які використовують українські солдати, отримати доступ до систем управління військовими операціями та використовувати загальнодоступні вебкамери для збору розвідувальних даних про розташування українських військових активів. За два роки після початку вторгнення росія відходить від атак на стратегічні цивільні цілі, такі як телекомунікації та енергетика, які були в центрі уваги на початку. Ця зміна стратегії вказує на нові пріоритети москви та демонструє, що потенціал кіберзброї на початкових етапах конфлікту не був повністю реалізованим.

APT41 СКОМПРОМЕТУВАЛА УРЯДОВИЙ ДОСЛІДНИЦЬКИЙ ІНСТИТУТ ТАЙВАНЮ ЗА ДОПОМОГОЮ SHADOWPAD І COBALT STRIKE

15 серпня дослідники Cisco Talos повідомили, що китайська хакерська група APT41 зламала урядовий науково-дослідний інститут Тайваню, який працює над конфіденційними технологіями. Атака почалася в липні 2023 року і використовувала шкідливі програми ShadowPad та Cobalt Strike. За даними звіту, інститут спеціалізується на обчислювальних технологіях, що є стратегічною галуззю для Тайваню, який є світовим лідером у сфері напівпровідників.

Cisco Talos приписує атаку APT41 – хакерській групі, яку Міністерство юстиції США у 2020 році звинуватило у використанні програм-вимагачів та інших інструментів для атак на понад 100 компаній і урядів по всьому світу.

КУРСЬКА ОБЛАСТЬ РОСІЇ ЗАЗНАЛА «МАСОВАНОЇ» DDOS-АТАКИ НА ТЛІ УКРАЇНСЬКОГО НАСТУПУ

8 серпня курська область росії зазнала масштабної DDoS-атаки під час активного наступу українських військ. Хакери атакували урядові та бізнес-сайти, а також об'єкти критичної інфраструктури, що спричинило тимчасові збої в їхній роботі. Атака включала понад 100 000 запитів на секунду, причому більшість IP-адрес було відстежено до Німеччини та Великобританії. Незважаючи на значний масштаб, інцидент не призвів до компрометації інфраструктури електронного уряду чи витоку даних користувачів. Це вважається однією з найбільших кібератак, спрямованих на регіон з початку війни, хоча відповідальність за неї поки ніхто не взяв.

APT28 НАЦІЛЮЄТЬСЯ НА ДИПЛОМАТІВ ЗА ДОПОМОГОЮ ЗЛОВМИСНОГО ПЗ HEADLACE ЧЕРЕЗ ФІШИНГ-ПРИМАНКУ ПРО ПРОДАЖ АВТОМОБІЛІВ

Нову кампанію, в якій використано оголошення про продаж автомобілів як фішинг-приманку для доставки модульного бекдору Windows під назвою HeadLace, приписують російській хакерській групі APT28.

Згідно зі звітом Palo Alto Networks Unit 42, опублікованим 2 серпня, кампанія, ймовірно, націлена на дипломатів і триває з березня 2024 року. З високим рівнем впевненості кампанію приписують групі APT28, також відомій під іншими назвами, такими як Fancy Bear, BlueDelta, Sofacy, і TA422.

ДОСЛІДНИКИ ВВАЖАЮТЬ, ЩО КІБЕРАТАКИ НА РОСІЙСЬКІ ДЕРЖАВНІ ОРГАНИ МОЖУТЬ БУТИ ПОВ'ЯЗАНІ З КИТАЙСЬКИМИ ХАКЕРАМИ

13 серпня видання The Record повідомило, що хакери, ймовірно пов'язані з китайськими групами APT31 і APT27, атакували російські державні установи та технологічні компанії в рамках кампанії кібератак під назвою EastWind. Атака, виявлена дослідниками з Kaspersky, була здійснена за допомогою трояна віддаленого доступу GrewApacha (RAT), бекдора PlugY та оновленої версії зловмисного ПЗ CloudSorcerer. Для розгортання цих інструментів зловмисники використовували фішингові електронні листи, що мають зв'язок з відомими китайськими кібершпигунськими групами. Хоча Kaspersky не приписує атаки безпосередньо APT31 чи APT27, використовувані інструменти вказують на можливу причетність цих угруповань.

EARTH BAKU, ПІДТРИМУВАНА КИТАЄМ, РОЗШИРЮЄ ГЕОГРАФІЮ КІБЕРАТАК НА ЄВРОПУ, БЛИЗЬКИЙ СХІД І АФРИКУ

14 серпня видання The Hacker News повідомило, що китайська хакерська група Earth Baku з кінця 2022 року розширила свою діяльність, включивши до кола своїх цілей країни Європи, Близького Сходу та Африки. Серед нових мішеней – Італія, Німеччина, ОАЕ, Катар, а також імовірні атаки в Грузії та Румунії. Уряди, засоби масової інформації, телекомунікації, технологічні компанії, охорона здоров'я та освіта – це деякі з секторів, які зазнали кібервторгнень з боку Earth Baku.

МАСШТАБНА КІБЕРАТАКА ПОРУШИЛА РОБОТУ ЦЕНТРАЛЬНОГО БАНКУ ІРАНУ

14 серпня видання Jerusalem Post повідомило про масштабну кібератаку, яка порушила роботу Центрального банку Ірану та інших великих банків країни. За поточними оцінками, цей інцидент вважається однією з найбільших атак на іранську інфраструктуру. Наразі невідомо, хто несе відповідальність за цю атаку, існують припущення, що за нею можуть стояти Сполучені Штати та/або Ізраїль.

НОВА ФІШИНГОВА КАМПАНІЯ НАЦІЛЕНА НА РОСІЙСЬКИХ ДИСИДЕНТІВ ПО ВСЬОМУ СВІТУ

Згідно з дослідженням Citizen Lab і Access Now, хакери, пов'язані з російською розвідкою, зокрема групи Cold River і нової групи Coldwastrel, запустили фішингову кампанію, спрямовану проти російських опозиціонерів і критиків кремля по всьому світу. Кампанія, яка розпочалася у 2022 році, атакувала російських опозиціонерів у вигнанні, співробітників некомерційних організацій у США та ЄС, а також медіа-організації. Зловмисники використовували техніку видавання себе за довірених осіб, щоб змусити жертв розкрити свої облікові дані. Серед жертв опинилися й високопосадовці, зокрема колишній посол США в Україні.

ЧОМУ ЗАГОВОРИЛИ ПРО ВТРУЧАННЯ ІРАНУ У ВИБОРИ США

21 серпня Foreign Policy повідомило, що з наближенням президентських виборів у США Іран посилив свої зусилля щодо втручання у виборчий процес через дезінформацію, операції впливу та кібератаки. Іранські хакери націлені на кампанії Дональда Трампа та Камали Гарріс. Агентства США, зокрема ФБР і CISA, попередили про ці загрози, наголосивши, що Іран вважає вибори важливими для своєї національної безпеки. Це частина ширшої стратегії, яка також включає атаки на офіційних осіб США, можливо, в помсту за вбивство іранського генерала Касема Сулеймані у 2020 році.

У цьому виборчому циклі діяльність Ірану є більш агресивною, ймовірно через триваючі конфлікти на Близькому Сході. Хоча росія і Китай залишаються основними загрозами, дії Ірану показують його готовність скористатися вразливими місцями виборчої безпеки США. Водночас офіційні особи США запевняють, що вони краще підготовлені до таких загроз, ніж на попередніх виборах, і закликають до обережної реакції, щоб не підірвати довіру до виборчого процесу.

АРЕШТ CEO TELEGRAM СПРОВОКУВАВ КІБЕРАТАКИ НА ФРАНЦУЗЬКІ САЙТИ

25 серпня арешт генерального директора Telegram Павла Дурова у Франції викликав хвилю кібератак з боку хакерів, які виступали проти його затримання. Французька влада заарештувала Дурова через звинувачення у відсутності модерації та співпраці з правоохоронними органами, що сприяло злочинам, таким як торгівля наркотиками та шахрайство. У відповідь хактивісти, включаючи проросійські групи, такі як російська кіберармія та UserSec, розпочали DDoS-атаки на французькі сайти уряду, ЗМІ та агентств охорони здоров'я під гаслом opDurov. Хоча багато сайтів зазнали збоїв, їх роботу було відновлено наступного понеділка.

РОСІЙСЬКІ ЗЛОВМИСНИКИ ТА КОМЕРЦІЙНІ ПОСТАЧАЛЬНИКИ СИСТЕМ СПОСТЕРЕЖЕННЯ ВИКОРИСТОВУЮТЬ ОДНАКОВІ ЕКСПЛОЙТИ – ЗВІТ GOOGLE

У своєму блозі Google Threat Analysis Group розкрила, що російська державна хакерська група APT29 (Cozy Bear) та комерційні постачальники систем спостереження, такі як Intellexa і NSO Group, неодноразово використовують ті самі експлойти. Дослідники виявили шпигунську кампанію, спрямовану проти вебсайтів, які контролюються урядом Монголії. Особливістю цієї кампанії стало те, що вперше було зафіксовано використання членами російської APT29 тих самих експлойтів, які продаються комерційними постачальниками систем спостереження.

США ЗВІЛЬНИЛИ ВІДОМИХ РОСІЙСЬКИХ ХАКЕРІВ У РАМКАХ ДИПЛОМАТИЧНОГО ОБМІНУ ПОЛОНЕНИМИ

2 серпня видання The Hacker News повідомило про звільнення двох відомих російських хакерів, Романа Селезньова та Владислава Клюшина, у рамках міжнародного обміну полоненими між Білоруссю, Німеччиною, Норвегією, росією, Словенією та США.

Селезньов, також відомий під псевдонімами Track2, Bulba та nCux, був засуджений у 2017 році до 27 років ув'язнення за шахрайство з платіжними картками, що завдало збитків на суму майже 170 мільйонів доларів малому бізнесу та фінансовим установам у США. Згодом він отримав додаткові 14 років за участь у кібершахрайстві на суму 50 мільйонів доларів. Другий звільнений хакер, Владислав Клюшин, власник фірми M-13, був засуджений у вересні 2022 року за викрадення конфіденційної фінансової інформації американських компаній, що призвело до інсайдерської торгівлі на суму 93 мільйони доларів. Обидва хакери повернулися до росії.