НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

CYBER DIGEST

Огляд подій в сфері кібербезпеки,
січень 2023

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

Підготовлено за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»
Створення цієї публікації стало можливим завдяки підтримці американського народу, наданій через Агентство США з міжнародного розвитку (USAID). Погляди авторів, висловлені у цій публікації, не обов'язково відображають погляди USAID або Уряду США.

ЗМІСТ

ОСНОВНІ ТЕНДЕНЦІЇ

Загальна тенденція з ransomware у світі покращується. Хоча кількість зловмисників та бізнес-моделей для таких вірусів зростає, але спостерігається зменшення кількостітаких атак, а також тих, хто платить викуп. Водночас для цієї сфери продовжує залишатись актуальним високий рівень латентності злочинів (про них не повідомляють), а атаки стають все більш скерованими та підготовленими. Таке зменшення пов'язано як з кращою координацією різних країн у протидії цій загрозі (в т.ч. у сфері контролю за криптовалютами), так і успішним операціям правоохоронних органів.

ФБР завдяки довготривалій спеціальній операції вдалось знищити потужне ransomware угрупування Hive. Хоча це лише одна з таких груп, але її знищення матиме ширші наслідки, ніж просто запобігання отриманню зловмисниками 130 млн доларів, які вони вимагали у жертв. Це також дає правоохоронним органам ліпше розуміння внутрішніх процедур таких зловмисних угрупувань та дозволить зменшити активність цілої низки менших груп, які користувались ресурсами Hive за принципом RaaS. Водночас вже зараз експерти очікують, що звільнене місце стане предметом протиборства інших хакерських груп.

Все більше занепокоєння у провідних держав світу (США, Великобританії, Франції, Австралії) викликають атаки вірусів-вимагачів на медичні установи. І хоча на сьогодні не існує точної статистики щодо кількості смертей, додатково спричинених такими атаками через неможливість надавати послуги пацієнтам, така тенденція викликає все більше занепокоєння. В США законом про асигнування на 2023 рік було запроваджено вимоги щодо кібербезпеки медичних приладів. І хоча експерти вітають таку ініціативу, вони підкреслюють недостатність таких заходів.

Державні установи залишаються привабливими цілями для зловмисників. В останній половині 2022 року кількість кібератак на уряди зросла на 95%. Атаки проти Королівської пошти Великобританії, Міністерства громадських робіт і транспорту Коста-Рики, державні установи Молдови, кампанія проти військових та державних структур в азійському регіоні – все це вказує на зростання загроз для організацій державного сектору та необхідність вдаватись до належних заходів кібербезпеки.

Державні кібербезпекові органи, розуміючи зростаючі ризики, продовжують коригувати свою політику та посилюють вимоги до законодавства у сфері кібербезпеки. Очікуване посилення обов'язковості вимог кібербезпеки в новій Національній стратегії кібербезпеки США, друга за останні пів року модифікація Cyber Essentials Національним центром кібербезпеки (NCSC) Великобританії, тестування підрядників на вразливість та готовність до впровадження політики zero trust (США), постійні навчання та розвиток співпраці урядових агенцій – все це є логічним наслідком нових загроз.

Кількість виявлених вразливостей у різноманітних ICS/OT системах зростає. Лише протягом січня стало відомо про вразливості в продуктах Siemens, InHand, GE Proficy Historian, які використовуються на багатьох небезпечних виробництвах, для функціонування промислових роботів, нафтових свердловин, ліфтів, медичного обладнання, зарядних станцій для електромобілів. Окремі непідтверджені повідомлення вказують на успішні зовнішні кібератаки на ICS системи. Довгостроковий інтерес зловмисників до промислових систем зростає і їх спроби знайти вразливості в них не припиняються. Експерти вже зауважують, що це може призвести до тяжких наслідків та до кейсів, аналогічних Stuxnet. Навіть без доступу до ICS зловмисникам вдається паралізувати роботу великих судноплавних компаній (Норвегія) чи ускладнити функціонування енергетичних об'єктів (Канада).

Дискусія щодо глобальних правил поведінки в кіберпросторі для всіх країн знову на порядку денному. Оглядачі зауважують, що масштаби поширення кіберзлочинності набувають форми кіберпандемії й країни не мають розв'язання цієї проблеми. В той час як дослідники пропонують найбільшим державам (зокрема США) взяти на себе підвищені односторонні зобов'язання щодо просування норм кібербезпеки на глобальному рівні, інші країни (Україна, зокрема) виходять з ініціативою про створення спільного простору, де держави можуть безпечно обмінюватися інформацією, підтримувати один одного і взаємодіяти.

російські хакери продовжують атакувати партнерів України. Під особливим прицілом Польща, Німеччина, Великобританія, балтійські країни та США. Так Польща була мішенню кібератак з боку хакерського угрупування Ghostwriter. Латвія підтверджує фішингову атаку на Міністерство оборони, пов'язуючи її з російською хакерською групою. Великобританія попереджає своїх громадян про кібератаки з боку російських груп. А проти США російські хакери проводили велику кампанію спрямовану на ядерний сектор – намагались атакувати американських науковців-ядерників. Експерти вказують, що ці тенденції продовжаться і у 2023 році, що буде вимагати від країн Заходу підвищеної готовності.

Світ продовжує оцінювати наслідки першої світової кібервійни та заходи, які дозволили Україні ефективно протистояти ворогу. Крім тез про важливість міжнародної допомоги, яка надавалась протягом останніх 8 років Україні у сфері кібербезпеки, експерти кажуть і про те, що Україна була готовою до кібервійни не лише через надану допомогу, але і завдяки концентрації на забезпеченні стійкості найважливіших функцій. І, звичайно, посилене державно-приватне партнерство стало важливим чинником протидії російській кіберактивності. Про ефективність цієї кібербезпекової політики каже і той факт, що навіть зростання у 20 разів кількості кібератак націлених на Україну в 4 кварталі 2022 року не призвело до тяжких наслідків.

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

НОВА ПОЛІТИКА КІБЕРБЕЗПЕКИ США СТАНЕ БІЛЬШ ЖОРСТКОЮ ТА ВИМОГЛИВОЮ

17 січня журналісти видання Slate оприлюднили аналіз проєкту нової «Національної стратегії кібербезпеки США». Відповідно до оприлюднених ними даних, новий стратегічний підхід буде відходити від добровільності виконання вимог кібербезпеки в різних галузях промисловості на користь обов'язковості (особливо для енергетичного та комунального секторів).

Другий елемент нової стратегії – проактивність держави. Документ має істотно розширити можливості та повноваження безпекових органів (в т.ч. – військових структур) у проведенні наступальних кібероперацій.

CISA ВИЗНАЧИЛО НОВІ ПРІОРИТЕТИ ДІЯЛЬНОСТІ JCDC НА 2023 РІК

26 січня CISA оприлюднила плани щодо оновлення цілей ініціативи Joint Cyber Defense Collaborative (JCDC). JCDC є ініціативою державно-приватного партнерства яка функціонує під егідою CISA. Визнаючи успішність запуску ініціативи JCDC у 2023 році CISA планує зосередитись на таких напрямках:

- безпека для ланцюжків постачання для ОКІ;
- більше кооперації з енергетичним та водним секторами;
- оновлення Національного плану реагування на кіберінциденти;
- захист журналістів та громадянського суспільства від кібератак.

ОФІС НАЦІОНАЛЬНОГО КІБЕРДИРЕКТОРА США СПІВПРАЦЮЄ З ДОСЛІДНИКАМИ КІБЕРБЕЗПЕКИ ПРИ ПІДГОТОВЦІ НОВОЇ НАЦІОНАЛЬНОЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ

19 січня представники Офісу національного кібердиректора США провели зустріч з дослідниками кібербезпеки. Під час зустрічі обговорювалось бачення нової Національної стратегії кібербезпеки та погляди дослідників на такі питання як боротьба з програмами-вимагачами, зміцнення безпеки програмного забезпечення з відкритим вихідним кодом та реалізація Федеральної стратегії нульової довіри.

ENISA ПОШИРИЛА НАБІР ІНСТРУМЕНТІВ ДЛЯ ОРГАНІЗАЦІЇ КОМПАНІЇ ПІДВИЩЕННЯ КІБЕРОБІЗНАНОСТІ

19 січня ENISA оприлюднила AR-in-a-Box – набір настанов, інструкцій та матеріалів (в т.ч. практично орієнтованих ігор) для надання знань державним органам, операторам основних послуг, великим приватним компаніям, а також малим і середнім (МСП) підприємствам про те, як розробляти та впроваджувати заходи з підвищення обізнаності щодо кібербезпеки в їх організаціях.

НАЦІОНАЛЬНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ (NCSC) ВЕЛИКОБРИТАНІЇ ОПУБЛІКУВАВ РЕКОМЕНДАЦІЇ З КІБЕРБЕЗПЕКИ ДЛЯ БЛАГОДІЙНИХ ОРГАНІЗАЦІЙ

20 січня NCSC Великобританії оприлюднив набір рекомендацій для благодійних організацій, в якому описано основні загрози, з якими стикається цей сектор в мережі Інтернет. Зокрема проблеми ransomware та фішингових атак. Звіт з'явився на фоні зростаючої активності зловмисників саме щодо цього сектору. Зокрема атака ransomware на Edinburgh Festival Fringe Society коштувала останньому 95 000 фунтів стерлінгів, а хоспіс у Вест-Мідлендсі внаслідок компрометації електронної пошти втратив 17 000 фунтів стерлінгів.

НАЦІОНАЛЬНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ ВЕЛИКОБРИТАНІЇ ПОПЕРЕДЖАЄ КОРИСТУВАЧІВ ПРО ЦІЛЕСПРЯМОВАНІ ФІШИНГОВІ АТАКИ З БОКУ РОСІЇ ТА ІРАНУ

26 січня NCSC Великобританії випустив попередження про підвищену активність російської групи SEABORGIUM та іранської групи TA453. Протягом 2022 року ці групи проводили шкідливі кампанії з метою збору інформації проти низки організацій й осіб у Великобританії та в інших країнах. Ці атаки були спрямовані на конкретні сектори, включаючи наукові кола, оборону, урядові організації, неурядові організації, аналітичні центри, а також політиків, журналістів та активістів.

КИТАЙ ПЛАНУЄ ЗАПУСТИТИ ВЕЛИКУ ПРОГРАМУ РОЗВИТКУ СЕКТОРУ КІБЕРБЕЗПЕКИ

У січні було опубліковано документ «Настанови шістнадцяти департаментів, включаючи Міністерство промисловості та інформаційних технологій щодо сприяння розвитку індустрії безпеки даних». Документ описує програму розвитку галузі кібербезпеки Китаю. Її мета – забезпечити 30% річне зростання сектору. Короткострокова мета – у 2025 році дохід сектору має сягнути 15 мільярдів єн (22 мільярди доларів США).

Для цього буде побудовано п'ять лабораторій безпеки, від трьох до п'яти національних індустріальних парків (з акцентом на питання безпеки даних), десять передових демонстраційних майданчиків для інноваційних продуктів тощо. План Китаю також передбачає співпрацю з індустрією безпеки даних у країнах, які беруть участь в ініціативі «Один пояс, один шлях».

ВІНСЕНТА СТРУБЕЛЯ ПРИЗНАЧЕНО НОВИМ ОЧІЛЬНИКОМ КІБЕРБЕЗПЕКОВОГО ВІДОМСТВА ФРАНЦІЇ

5 січня було оголошено, що новим головою ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) призначено Вінсента Струбеля, який працював в Агенції протягом 15 років, починаючи з 2005. Останні майже три роки він очолював OSIIC (Оператор секретних міжміністерських інформаційних систем), який є французьким урядовим органом, відповідальним за захист секретного зв'язку. Його попередник пішов з посади у грудні минулого року.

ЗАКОН США ПРО ВИТРАТИ НА 2023 РІК МІСТИТЬ ВИМОГИ ЩОДО КІБЕРБЕЗПЕКИ МЕДИЧНОГО ОБЛАДНАННЯ

В США було вперше запроваджено законодавство, яке вимагає від виробників медичних пристроїв піклуватися про їх кібербезпеку. Консолідований закон про асигнування 2023 року, який був підписаний наприкінці грудня, містить положення, які вимагають від виробників медичних пристроїв документувати, що їхні продукти можна оновлювати та виправляти, а також надавати специфіку програмного забезпечення для пристроїв.

На думку експерта SANS Джона Прескатора новації стосуються лише нових пристроїв, а FDA отримала лише 5 мільйонів доларів США на фінансування розробки політики, процедур і заходів із забезпечення дотримання нових правил. Разом з тим, лише в США налічується майже 1000 виробників медичних приладів. 5 мільйонів доларів США – це менше ніж тижневі витрати на маркетинг у секторі медичного обладнання та обладнання в США.

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

ПЕРЕБУВАЮЧИ НА ЧОЛІ ЄС, ШВЕЦІЯ ОБІЦЯЄ ПРОСУВАТИ ОБОРОННУ СПІВПРАЦЮ ТА КІБЕРЗАХИСТ

Піврічне головування Швеції в Європейському Союзі розпочалося 1 січня. Серед іншого, досягнення більш значущого рівня співпраці між країнами-членами ЄС у сфері кібербезпеки стало однією з найважливіших цілей Швеції. Ця мета набула додаткової ваги 3 січня, коли Європейська комісія представила Європейському парламенту Спільну комунікацію щодо спільної політики ЄС у сфері кіберзахисту. Joint Communication (JC) for an EU common cyber defense policy). Політика ЄС щодо кіберзахисту у питаннях та відповідях.

ЯПОНІЯ ТА США ПІДПИСАЛИ МЕМОРАНДУМ ПРО СПІВПРАЦЮ У СФЕРІ КІБЕРЗАХИСТУ

Під час візиту японської делегації до США 6 січня Міністр економіки, торгівлі та промисловості Японії Ясутосі Нісімура та Міністр внутрішньої безпеки США Алехандро Майоркас підписали меморандум про зміцнення співпраці між двома країнами у сфері кібербезпеки.

Обидві країни запровадять однакові стандарти безпеки для програмного забезпечення, закупленого урядом, щоб знизити ризик шкоди від дедалі складніших кібератак.

Згідно з меморандумом, Японія та Сполучені Штати створять систему, яка буде отримувати інформацію про безпеку від постачальників програмного забезпечення. Вони також сприятимуть зміцненню потенціалу кібербезпеки своїх індо-тихоокеанських партнерів у надії протистояти Китаю.

США ПЛАНУЄ ПОШИРИТИ ПОЛІТИКУ ZERO TRUST НА ВІДНОСИНИ В МЕЖАХ АЛЬЯНСУ FIVE EYES

На початку січня в США відбувся триденний форум представників міністерств оборони країн, що входять до альянсу Five Eyes. Сторони обговорили бачення країн щодо впровадження політики zero trust на фоні зростаючих кіберзагроз з боку Китаю та росії. США, Австралія та Великобританії поділились своїми поглядами на впровадження такої політики на національному рівні.

ENISA СПІЛЬНО З ЄВРОПЕЙСЬКОЮ КОМІСІЄЮ ПРОВЕЛИ КОНФЕРЕНЦІЮ З ПОЛІТИКИ КІБЕРБЕЗПЕКИ

26 січня ENISA спільно з Європейською комісією провели першу велику європейську конференцію високого рівня з політики кібербезпеки (за участі керівників європейських агенцій кібербезпеки або старших керівників цих структур). Основні теми для обговорення: розвиток кіберполітики ЄС, майбутнє Директиви NIS2 та Акту про кіберстійкість (Cyber-resilience Act), програми відповідального розкриття вразливостей та нові виміри політики кібербезпеки.

ПІВНІЧНОЄВРОПЕЙСЬКІ КРАЇНИ ПЛАНУЮТЬ СТВОРИТИ СПІЛЬНУ СТРАТЕГІЮ КІБЕРБЕЗПЕКИ ДЛЯ ЦЬОГО РЕГІОНУ

17 січня стало відомо, що 8 країн-членів Північної ради (Данія, Фінляндія, Ісландія, Норвегія, Швеція, Фарерські острови, Гренландія та Аландські острови) уклали угоду щодо розробки спільної стратегії кібербезпеки. Ці зусилля будуть частиною ініціативи NORDEFCO Vision 2025. Основна ідея стратегії – посилення обміну розвідувальними даними між країнами, надаючи скандинавським країнам здатність захищатися від загроз, що виходять із кіберсфери. Ключову роль у розробці документа буде відігравати Норвегія, а його текст буде напрацьовано групою Nordic Defense Cooperation, яка складається з Данії, Фінляндії, Ісландії, Норвегії та Швеції.

ФБР ТА МІНІСТЕРСТВО ЮСТИЦІЇ США ВДАЛОСЬ ЗНИЩИЛИ ІНФРАСТРУКТУРУ ГРУПИ RANSOMWARE HIVE

26 січня, ФБР та Міністерство юстиції США заявили, що завдяки співпраці з Європолом, а також правоохоронними органами Німеччини, Нідерландів, Канади, Франції, Ірландії, Литви, Норвегії, Португалії, Румунії, Іспанії, Швеції та Великобританії, їм вдалось знищити угрупування Hive. Співробітники ФБР змогли проникнути в мережу зловмисників ще у липні 2022 року, документувати дії злочинців та допомагати жертвам отримувати ключі для дешифрування.

Цікавим результатом розслідування стало те, що лише близько 20% жертв повідомили про свої інциденти з програмами-вимагачами в правоохоронні органи. Це підкреслює проблему, коли жертви просто не звертаються до правоохоронців, а натомість платять викуп.

СИЛИ КІБЕРОБОРОНИ ФРАНЦІЇ ДИСКУТУЮТЬ ЩОДО РОЛІ ОКРЕМИХ КІБЕРБЕЗПЕКОВИХ ПРОЄКТІВ США В ЄВРОПІ

10 січня голова Кіберкомандування Франції (COMCYBER) генерал Еймерік Боннемізон, заявив, що операції технічної підтримки hunt forward, які проводять американські військові в мережах європейських країн з метою відстеження можливих російських вторгнень, зокрема з початку війни в Україні, «викликають запитання».

Він висловив побоювання, що такі операції, які все більше стають основним елементом стратегії випереджувального захисту Пентагону (defend forward), – є першим етапом шпигунських операцій. І хоча він не навів доказів на підтвердження своїх слів, його заяви можуть підірвати довіру до такої стратегії США.

Американські посадовці відкинули такі звинувачення, але слова Боннемізона процитувало вже принаймні одне російське пропагандистське видання.

МІЖНАРОДНА РОБОЧА ГРУПА З БОРОТЬБИ З ПРОГРАМАМИ-ВИМАГАЧАМИ РОЗПОЧАЛА РОБОТУ

23 січня офіційно розпочала роботу Міжнародна цільова група з боротьби з програмами-вимагачами, про створення якої було оголошено на заході в Білому домі в листопаді минулого року. Про це повідомив уряд Австралії, яка головує у цій групі.

Діяльність Міжнародної цільової групи з боротьби з програмами-вимагачами (ICRTF) спрямована на стимулювання співпраці в рамках коаліції з 36 держав-членів (в т.ч. Україна) та Європейського Союзу для протидії поширенню та впливу програм-вимагачів, які, попри те, що зазвичай є кримінальною, а не державною діяльністю, в останні роки перетворилися на значну загрозу національній безпеці.

Група має на меті допомогти державам-членам обмінюватися інформацією та розвідувальними даними про загрози, з якими вони стикаються, а також обмінюватися інформацією щодо державної політики та правовими рамками повноважень і заохочувати правоохоронні та кіберорган члени до співпраці.

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

КОРОЛІВСЬКА ПОШТА ВЕЛИКОБРИТАНІЇ СТАЛА ЖЕРТВОЮ RANSOMWARE

11 січня Королівська пошта Великобританії була атакована ransomware LockBit (попередньо), що призвело до серйозного збою в обслуговуванні та тимчасово зупинилось відправлення товарів у закордонні пункти призначення. Станом на 26 січня компанія все ще продовжувала відновлення своєї діяльності, а частина її послуг не працювала.

ХАКЕРИ ПРОДОВЖУЮТЬ ЕФЕКТИВНО ВИКОРИСТОВУВАТИ СТАРІ ВІДОМІ ВРАЗЛИВОСТІ

10 січня дослідники з CrowdStrike оприлюднили аналіз діяльності угрупування SCATTERED SPIDER, яка використовує вразливість 2015 року (CVE-2015-2291) у діагностичному драйвері Intel Ethernet. Попри те, що ця вразливість добре відома і для неї оприлюднено відповідні патчі, однак багато компаній все ще ігнорують оновлення безпеки, що дає зловмисникам можливість проникати в їх системи.

SCATTERED SPIDER – це фінансово мотивована кіберзлочинна група, яка націлена на компанії телекомунікаційного сектору та аутсорсингового бізнесу.

МІНІСТЕРСТВО ГРОМАДСЬКИХ РОБІТ І ТРАНСПОРТУ КОСТА-РИКИ ПОСТРАЖДАЛО ВІД RANSOMWARE

17 січня 12 серверів міністерства були зашифровані невідомим ransomware. Це призвело до того, що послуги з організації дорожнього руху та громадських робіт, навігації та безпеки на морі, які пропонувалися у цифровому вигляді, довелось надаватися особисто. З метою недопущення поширення вірусу більшість урядових агентств Коста-Рики розірвали з'єднання з атакованим міністерством. Навесні 2022 року урядовий сектор Коста-Рики вже ставав жертвою масштабної кібератаки з боку угрупування Conti.

УГРУПУВАННЯ DARK PINK АТАКУЄ УРЯДОВІ ТА ВІЙСЬКОВІ ОРГАНІЗАЦІЇ В АЗІЇ ТА ЄВРОПІ

Виявлено нову хакерську групу Dark Pink. Основний фокус її уваги – урядові, військові, релігійні та некомерційні організації в Азії та Європі. Основна мета – корпоративне шпигунство (хакери викрадають файли, аудіо з мікрофона та дані месенджерів із заражених пристроїв).

PROOFPOINT ОПРИЛЮДНИЛИ ДЕТАЛЬНИЙ АНАЛІЗ МЕТОДІВ ТА ТАКТИК APT ГРУПИ TA444

25 січня спеціалісти кібербезпекової компанії Proofpoint опублікували детальний аналіз APT TA444 – спонсорованої Північною Кореєю групою, що сфокусована на фінансових злочинах в інтересах керівництва Північної Кореї. Основні цілі її атак: банки, фінансові установи, а також обіг криптовалют.

ГРУПА ОПЕРАТОРІВ ПРОГРАМ-ВИМАГАЧІВ ВИБАЧИЛАСЯ ТА ПОДАРУВАЛА ЛІКАРНІ SICKKIDS БЕЗКОШТОВНИЙ ДЕШИФРАТОР

31 грудня група вимагачів LockBit випустила безплатний дешифратор для лікарні для хворих дітей (SickKids), заявивши, що один із її членів порушив правила, атакувавши медичну установу. «Партнер, який атакував цю лікарню, порушив наші правила, [він] заблокований і більше не входить до нашої партнерської мережі», – заявили у банді вимагачів.

LockBit працює як програма-вимагач за винаймом, де оператори підтримують шифрувальники та вебсайти, а афілійовані особи або учасники операції зламують мережі жертв, викрадають дані та шифрують пристрої.

ВІРУС RASPBERRY ROBIN АДАПТУЄТЬСЯ ДЛЯ АТАК НА ФІНАНСОВИЙ І СТРАХОВИЙ СЕКТОРИ В ЄВРОПІ

Згідно зі звітом, опублікованим Security Joe's 2 січня, деякі атаки, задокументовані в попередні місяці, схоже, були організовані хакерськими групами за допомогою фреймворку під назвою Raspberry Robin. Цей автоматизований фреймворк дозволяє зловмисникам уникати виявлення після зараження, переміщатися латерально і використовувати надійні хмарні інфраструктури відомих постачальників даних, таких як Discord, Azure і Github, серед інших.

«Унікальність зловмисного програмного забезпечення полягає в тому, що воно сильно заплутане та дуже складне для статичного аналізу», – йдеться у звіті.

ДЕРЖАВНІ УСТАНОВИ МОЛДОВИ ЗАЗНАЛИ КІБЕРАТАКИ

5 січня Служба інформаційних технологій і кібербезпеки Молдови (STISC) заявила про фішингову атаку на державні установи країни. Хакери розіслали понад 1330 електронних листів на облікові записи, що належать державним службам країни.

Під час однієї кампанії електронні листи містили повідомлення про нібито закінчення терміну дії державного домену .md і відправляли користувачів за зловмисним посиланням, яке веде на підроблену платіжну сторінку, щоб поновити його. Про те, скільки державних установ постраждали в результаті атаки, STISC не повідомляє.

BITDEFENDER ВИПУСТИВ ДЕШИФРАТОР ДЛЯ ПРОГРАМ-ВИМАГАЧІВ MEGACORTEX

5 січня компанія з кібербезпеки Bitdefender випустила дешифратор для програми-вимагача MegaCortex, яка використовувалася для атак по всьому світу, перш ніж поліція завадила її роботі.

Дешифратор був розроблений у співпраці зі швейцарською поліцією та європейськими правоохоронними органами, які у жовтні 2021 року провели рейди проти ймовірних кіберзлочинців, які стоять за штамами програм-вимагачів Dharma, MegaCortex і LockerGoga.

Bitdefender використала головні ключі дешифрування, знайдені під час рейдів, для створення універсальних дешифраторів. «Оскільки MegaCortex більше не активний, дешифратор допоможе лише жертвам, які зберегли своє зашифроване обладнання», – сказав експерт із програм-вимагачів Recorded Future Аллан Ліска.

КІБЕРАТАКА НА ПОСТАЧАЛЬНИКА ПОСЛУГ З ОБРОБКИ ДЕРЖАВНИХ ЕЛЕКТРОННИХ ДАНИХ ТОРКНУЛАСЯ БАГАТЬОХ ОКРУГІВ США

4 січня хмарна компанія з управління цифровими даними Cott Systems повідомила клієнтів, що наприкінці грудня зазнала «організованої кібератаки». Cott Systems допомагає керувати державними даними, включаючи демографічні дані, земельні дані та судові справи.

Згідно з вебсайтом, компанія обслуговує понад 400 органів місцевого самоврядування у 21 штаті та має давні зв'язки з кількома національними та міжнародними органами. Cott відключила свої сервери, щоб ізолювати інфекцію. Як результат, багато місцевих органів влади в США були змушені вручну обробляти свідоцтва про народження, свідоцтва про шлюб та операції з нерухомістю.

Дослідники компанії наголосили, що у 14,6% випадків викрадення даних стало можливим через повну відсутність заходів кібербезпеки проти ризиків, які можна було легко пом'якшити.

ХМАРНІ СЛУЖБИ ЕЛЕКТРОННОЇ ПОШТИ ЗМІЦНЮЮТЬ ШИФРУВАННЯ ВІД ХАКЕРІВ

Google, Microsoft і Proton запустили нові продукти наскрізного шифрування, щоб протистояти 50% зростанню кількості атак вірусів-вимагачів, фішингу та інших атак з використанням електронної пошти, яке спостерігається з першої половини 2022 року. Наскрізне шифрування електронної пошти та інших хмарних сервісів стає все популярнішим. З огляду на те, що електронна пошта є одним із двох найбільших векторів кібератак, це не дивно, пише The Tech Republic, описуючи нові послуги, які пропонують компанії.

ПРОМИСЛОВЕ ШПИГУНСТВО: ЯК КИТАЙ ВИКРАДАЄ ТЕХНОЛОГІЧНІ СЕКРЕТИ США

У статті для BBC Ніколас Йонг описує деякі прийоми, до яких вдаються китайські шпигуни для викрадення передових технологічних рішень, розроблених американським бізнесом. Автор наголошує, що такі дії є частиною більшої конкуренції між Китаєм та США, в якій Китай намагається порушити глобальний порядок, швидкими темпами наздогнавши США.

СЕРЙОЗНИЙ НЕДОЛІК МОБІЛЬНОГО ЗАСТОСУНКУ РОЗКРИВ ДАНІ МІЛЬЙОНІВ ІНДІЙСЬКИХ СТУДЕНТІВ

23 січня видання Wired повідомило, що витік даних, який містив ідентифікаційну інформацію про мільйони студентів і викладачів в Індії, стався через збій безпеки в обов'язковому застосунку, яким керує Міністерство освіти країни.

Дані користувачів зберігалися у застосунку Digital Infrastructure for Knowledge Sharing, відомому як Diksha, який студенти широко використовували у розпал пандемії, щоб отримати доступ до навчальних завдань з дому. Але хмарний сервер залишився незахищеним, через що дані стали доступними для хакерів та шахраїв.
Ці файли містять повні імена, номери телефонів та адреси електронної пошти понад мільйона вчителів із сотень тисяч шкіл у кожному штаті Індії. Інший файл містив інформацію про понад 600 000 учнів, включаючи повні імена та інформацію про те, де вони навчалися.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

NIST ЗАВЕРШИВ РОБОТУ НАД ІНСТРУКЦІЯМИ З КІБЕРБЕЗПЕКИ ДЛЯ НАЗЕМНОГО СЕГМЕНТА КОСМІЧНИХ ОПЕРАЦІЙ

Національний інститут стандартів і технологій (NIST) опублікував остаточну версію інструкцій із застосування фреймворку кібербезпеки до наземного сегмента космічних операцій, зокрема супутникового командування та управління. Вони містяться у Міжвідомчому звіті NIST (IR) 8401. Рекомендації NIST розроблено у відповідь на те, що уряд США розглядає космос як дедалі важливіший елемент критичної інфраструктури.

ЧОГО ЧЕКАТИ ВІД ШІ У 2023 РОЦІ

Опитані експерти вважають, що у 2023 році спостерігатимуться такі тенденції:

- ми будемо продовжувати спостерігати «рух від людей, які використовують програмне забезпечення ШІ та машинного навчання для покращення своєї роботи, до людей, які покладаються на програмне забезпечення, яке автономно виконує роботу за них». Очікувана рецесія може посилити цей тренд, адже бізнесу необхідно буде скорочувати розходи.
- глобальні зміни споживчого досвіду покупців у 2023 році завдяки «інноваційним рішенням «нульової сторони», які використовують передові методи машинного навчання та розроблені для прямої та прозорої взаємодії зі споживачами». Тобто, споживач не очікуватиме на відповідь оператора, а спілкуватиметься з ШІ.
- більше уваги буде приділятися різноманіттю при розробці застосунків для здоров'я та фітнесу, адже сьогодні вони працюють добре переважно «якщо ви людина середньої статури та маєте останню модель iPhone із великим екраном».

НАЦІОНАЛЬНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ (NCSC) ВЕЛИКОБРИТАНІЇ ПЛАНУЄ ОНОВИТИ ТЕХНІЧНІ ВИМОГИ CYBER ESSENTIALS

23 січня NCSC Великобританії повідомив, що у квітні 2023 року планується оновлення низки технічних вимог Cyber Essentials – розроблений урядом набір контролів, які британські організації мають запровадити для досягнення базового рівня кібербезпеки. Планується внести 9 змін, в т.ч. вимоги до пристроїв користувачів, захисту від шкідливих програм, архітектури нульової довіри тощо. Зміни ґрунтуються на відгуках оцінювачів і заявників та внесені після консультації з технічними експертами з NCSC.

МІНІСТЕРСТВО ОБОРОНИ США ПРОТЕСТУЄ БЕЗПЕКУ ХМАРНИХ СЕРВІСІВ AMAZON, GOOGLE, MICROSOFT І ORACLE

20 січня Міністерство оборони США повідомило, що за домовленістю з Amazon, Google, Microsoft і Oracle «червоні команди» NSA перевірять готовність інфраструктури цих комерційних компаній до складних кібератак та стану впровадження політики zero trust. Ця діяльність відбувається в межах підготовки запуску програми Joint Warfighting Cloud Capability вартістю 9 мільярдів доларів США. Вказані приватні компанії обрані як основні підрядники цієї програми.

У НІДЕРЛАНДАХ КІЛЬКІСТЬ КІБЕРЗЛОЧИНІВ ЗРОСЛА У ТРИ РАЗИ У ПОРІВНЯННІ З 2018 РОКОМ

19 січня правоохоронні органи Нідерландів поширили статистку кіберзлочинів за 2022 рік. За їх даними кількість злочинів склала 13 949, що в три рази більше ніж у 2018 році. Це відбувається на фоні зниження кількість крадіжок зі зломом та пограбувань. На думку експертів серед причин такого зростання – пандемія COVID-19, яка зробила складнішими здійснення традиційних злочинів, що стимулювало розвиток кібершахрайства.

УСТАНОВИ ОХОРОНИ ЗДОРОВ'Я АВСТРАЛІЇ ЗНАХОДЯТЬСЯ ПІД ПОСТІЙНОЮ УВАГОЮ КІБЕРЗЛОЧИНЦІВ – TREND MICRO

9 січня аналітики компанії Trend Micro оприлюднили результати свого дослідження щодо зловмисного інструменту Gootkit (він же Gootloader). За їх даними цей інструмент спрямований саме на медичні заклади і використовує для проникнення вразливості VLC Media Player. Проаналізовані зразки вказували на ключові слова «лікарня», «здоров'я», «медичний» в поєднанні з назвами конкретних австралійських міст. Також ціллю були назви конкретних постачальників медичних послуг по всій Австралії.

ПОСЛАБЛЕННЯ ГЛОБАЛІЗАЦІЙНИХ ПРОЦЕСІВ ВЕДЕ ДО ЗРОСТАННЯ ДЕСТРУКТИВНОЇ КІБЕРАКТИВНОСТІ – CISCO TALOS

24 січня аналітик компанії Cisco Talos Нік Біасіні спробував описати глобальний кібербезпековий тренд, пов'язаний зі зростаючим послабленням глобальних економічних зв'язків. На його думку, такі події як COVID-19, російсько-українська війна та низка інших подій ускладнюють глобалізаційні процеси. Це веде до того, що спонсоровані державою хакери будуть активніше використовувати віруси-wiper'и, а також вдаватись до крадіжок інтелектуальної власності. Також будуть зростати кіберзагрози для різних секторів критичної інфраструктури.

НОВИЙ КИТАЙСЬКИЙ КВАНТОВИЙ АЛГОРИТМ ЗЛОМУ ВИКЛИКАЄ ЗАНЕПОКОЄННЯ В США

На початку січня китайські дослідники опублікували статтю, у якій стверджують, що розробили новий алгоритм злому коду, який у разі успіху може зробити основне шифрування безсилим протягом декількох років, а не десятиліть, як очікувалося раніше.

Команда на чолі з професором Лонгом Гуйлу з Університету Цінхуа заявила, що квантовий комп'ютер, створений за наявними на цей час технологіями, здатний запустити їхній алгоритм. У разі успіху, під загрозою опиняється один із найсуворіших галузевих стандартів, який використовується багатьма урядами, фінансовими установами та технологічними компаніями для захисту інформації.
Разом з тим, дослідники з інших країн, зокрема з США, висловлюють сумніви, що підхід, запропонований Логом, буде успішним.

Дискусія на цю тему триває в безпекових колах. США та Китай конкурують в галузі квантових технологій, як і в низці інших технологічних сфер.

5. КРИТИЧНА ІНФРАСТРУКТУРА

ЕКСПЕРТИ З КІБЕРБЕЗПЕКИ СТАВЛЯТЬ ПІД СУМНІВ ЗАЯВИ ХАКЕРІВ З GHOSTSEC ПРО ВДАЛИЙ ВИПАДОК ЗАПУСКУ RANSOMWARE ПРОТИ ICS

У січні хактивістська група GhostSec, чиї останні операції були зосереджені проти росії через її вторгнення в Україну, стверджує, що провела першу в історії атаку ransomware на віддалений термінал (RTU) – пристрій ICS, який використовується для зв'язку між польовими пристроями та системами диспетчерського керування та збору даних (SCADA).

За словами хактивістів пристрій знаходиться на одному з білоруських підприємств. Водночас експерти (на основі відкритих хактивістами даних про інцидент) сумніваються у правдивості кейса. Водночас вони попереджають, що такі спроби будуть все частішими і є вірогідність того, що вони колись будуть дійсно вдалими.

НАТО ПЕРЕВІРЯЄ ЗДАТНІСТЬ ШІ ЗАХИЩАТИ КРИТИЧНУ ІНФРАСТРУКТУРУ ВІД КІБЕРАТАК

Штучний інтелект може допомогти визначити шаблони кібератак на критичну інфраструктуру та мережеву активність, а також виявляти зловмисне програмне забезпечення, таким чином покращуючи прийняття рішень щодо захисних заходів. Таких попередніх висновків дійшли учасники міжнародного експерименту щодо здатності ШІ убезпечувати та захищати системи, електромережі та інші критичні активи, проведеного кіберекспертами під час заходу Кіберкоаліції НАТО наприкінці минулого року.

В експерименті взяли участь шість команд з країн-членів НАТО, які мали підтримувати роботу уявної комп'ютерної системи та мережі на уявній військовій базі під час кібератаки.

Метою експерименту було перевірити та виміряти ефективність ШІ у зборі даних і допомозі командам реагувати на кібератаки проти критично важливих систем і сервісів, а також підкреслити потребу в інструментах, які покращують співпрацю між людьми та машинами для зниження кіберризику.

ВРАЗЛИВОСТІ В ПРОМИСЛОВИХ МАРШРУТИЗАТОРАХ INHAND СТАВЛЯТЬ ПІД ЗАГРОЗУ ОТ МЕРЕЖІ

13 січня CISA опублікувала повідомлення про виявлені дослідниками з компанії Otorio вразливості у промислових маршрутизаторах InHand Networks. Вразливість стосується щонайменше двох приладів – InRouter302 та InRouter615. Одна з вразливостей позначена як «критична», дві – «високої серйозності», а ще дві – «середньої серйозності».

Уражені пристрої використовуються для функціонування промислових роботів, нафтових свердловин, ліфтів, медичного обладнання, зарядних станцій для електромобілів і розумних лічильників.

ЗЛОВМИСНИКИ НАМАГАЛИСЬ АТАКУВАТИ ПОСТАЧАЛЬНИКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЕЛЕКТРОННИХ МЕДИЧНИХ ЗАПИСІВ (EHR) NEXTGEN HEALTHCARE

17 січня невизначена ransomware група атакувала системи NextGen Healthcare вірусом AlphV/BlackCat. Наразі невідомо, чи ця атака досягла результату. Представники компанії кажуть, що системи не були уражені та дані клієнтів не постраждали. Підозрюють, що за атакою стоїть те саме угрупування, яке атакувало Colonial Pipeline у 2021 році (можливо угрупування FIN7).

БЛИЗЬКО 1000 МОРСЬКИХ СУДЕН ПОСТРАЖДАЛИ В РЕЗУЛЬТАТІ АТАКИ RANSOMWARE НА КОМПАНІЮ DNV

7 січня системи однієї з найбільших у світі морських організацій DNV (Осло) були атаковані ransomware. Це змусило компанію вимкнути IT-сервери, підключені до їхньої системи Ship-Manager. Постраждало 70 клієнтів, які керують тисячею суден. Загалом DNV обслуговує понад 13 175 суден.

ХАКЕРИ АТАКУВАЛИ ЕНЕРГЕТИЧНУ КОМПАНІЮ У КАНАДІ

15 січня стало відомо, що невстановлені хакери атакували енергетичну компанію Qulliq Energy Corporation (QEC) на території Нунавут (Канада). Системи розподілення чи генерації не були уражені (лише адміністративні системи) компанія не приймає оплату рахунків за допомогою кредитних карток, але клієнти можуть платити готівкою або банківським переказом. Дані про тип вірусу чи групу, яка стоїть за атакою, наразі відсутні.

VICE SOCIETY RANSOMWARE GROUP НАЦІЛИЛАСЬ НА КОМПАНІЇ ПРОМИСЛОВОГО СЕКТОРУ

24 січня Trend Micro оприлюднила результати свого дослідження діяльності Vice Society Ransomware Group. За даними дослідників, ця група націлилась на промисловий сектор (раніше активність групи була зосереджена на освітньому та медичному). Швидше за все таке проникнення буде проводитись через придбання скомпрометованих облікових даних. Вже виявлено присутність Vice Society в Бразилії (головним чином атакує підприємства обробного комплексу країни), Аргентині, Швейцарії та Ізраїлі.

NSA, CISA ТА MS-ISAC ВИПУСТИЛИ СПІЛЬНІ НАСТАНОВИ ЩОДО БЕЗПЕЧНОГО ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ВІДДАЛЕНОГО МОНІТОРИНГУ ТА КЕРУВАННЯ

25 січня NSA та CISA одночасно оприлюднили настанови «Захист від зловмисного використання програмного забезпечення для віддаленого моніторингу та керування». Вони мають допомогти компаніям, які використовують законне програмне забезпечення віддаленого моніторингу та керування (RMM) не допустити його зловмисного використання.

Програмне забезпечення RMM зазвичай використовується постачальниками керованих послуг (MSP) і довідковими службами для забезпечення безпеки та/або технічної підтримки.

SIEMENS ЗАЯВИЛА ПРО ВИЯВЛЕННЯ ВРАЗЛИВОСТІ У СВОЇХ КОНТРОЛЕРАХ СЕРІЇ S7-1500

10 січня компанія Siemens оголосила, що зловмисники можуть використати вразливість у контролерах серії S7-1500 (близько 122 моделей серії), щоб непомітно встановити шкідливе програмне забезпечення на пристрої та отримати повний контроль над ними.

Компанія не планує вдаватись до заходів виправлення, адже експлуатація вразливість потребує фізичного доступу до контролера. Відтак вона рекомендує компаніям впровадити заходи, щоб переконатися, що лиш довірений персонал має доступ до фізичного обладнання.

Вразливість виявили дослідники Red Balloon Security і вони висловлюють занепокоєння, що відсутність виправлень у цій серії контролерів (які використовуються на багатьох небезпечних виробництвах) може призвести до ситуацій, схожих з вірусом Stuxnet.

В ПРОДУКТІ GE PROFICY HISTORIAN ВИЯВЛЕНО ВРАЗЛИВОСТІ

У січні спеціалісти кібербезпекової компанії Claroty, яка спеціалізується на промисловій безпеці, оприлюднили дані про вразливість в продукті GE Proficy Historian. Сервери Historian призначені для збору даних із промислових систем керування (ICS), щоб допомогти організаціям контролювати та вдосконалювати свої процеси. Часто вони розташовуються між мережами IT і OT, що робить їх привабливою ціллю для зловмисників.

Дослідники Claroty виявили загалом п'ять вразливостей критичного та серйозного рівня. До недоліків належать обхід автентифікації, довільне завантаження файлів, розкриття інформації та проблеми з видаленням файлів.

6. АНАЛІТИЧНІ ОЦІНКИ

СТАН RANSOMWARE У США: ЗВІТ І СТАТИСТИКА ЗА 2022 РІК

Як стверджують дослідники компанії Emsisoft, у звіті, опублікованому 2 січня, попри те, що протягом 2022 року уряд США приділяв значну увагу рансомвер, кількість атак на установи і організації у сфері освіти, охорони здоров'я та в урядовому секторі більш-менш залишаються незмінними з 2019 року. У своєму аналізі експерти компанії зосередилися саме на цих сферах, адже там існують суворіші вимоги до звітності, що забезпечує більшу впевненість у точності даних.

Дослідники наголошують, що інформація про атаки на приватні компанії дуже часто є недоступною, і тому важко точно визначити суму збитків, які наносять атаки вимагачів.

ДОХІД ВІД RANSOMWARE У 2022 РОЦІ СКОРОТИВСЯ – CHAINALYSIS

19 січня було оприлюднено дані дослідження компанії Chainalysis щодо ситуації із ринком зловмисних програм ransomware. Згідно зі звітом, доходи, отримані від атак ransomware, впали з $765,6 млн у 2021 році до $456,8 млн у 2022 році. Одним з факторів є відмови жертв платити викуп.

А загалом з 2019 року відсоток виплат потерпілими знизився з 76% до 41% – значною мірою через те, що виплата викупу несе додатковий ризик порушення санкцій США. Також істотний вплив на ситуацію здійснили дії правоохоронних органів та посилення заходів кібербезпеки, до яких вдаються організації.

Ці дані підтверджуються іншими схожими дослідженнями. Так Delinea вказує у своєму звіті на те, що кількість атак програм-вимагачів зменшилася на 61% у 2022 році, а виплати викупу впали з 82% до 68%.

РЕЙТИНГ ЛІДЕРІВ ПРОГРАМ-ВИМАГАЧІВ 2022 РОКУ

5 січня Trustwave SpiderLabs опублікувала підсумковий звіт найактивніших за їх оцінками груп загроз серед програм-вимагачів минулого року. До них відносяться: LockBit (який працює як бізнес), Black Basta (новіший і з очевидними зв'язками з Conti, REvil і Fin7), Hive (програма-вимагач як послуга) і BlackCat (також відомий як ALPHV, який, можливо, пов'язаний з бандами Darkside і BlackMatter).

ENISA ОПУБЛІКУВАЛА ДОСЛІДЖЕННЯ ЩОДО ОБМІНУ ПЕРСОНАЛЬНИМИ ДАНИМИ

27 січня ENISA, до Дня захисту персональних даних, опублікувала результати свого дослідження «Інженерія обміну персональними даними» (Engineering Personal Data Sharing). Основний фокус дослідження – краще зрозуміти технічні та правові проблеми обміну персональними даними у різних випадках та сферах, як саме такі дані стають відомі третім сторонам і як зробити таке розкриття безпечнішим.

CYBERCOM ПІДВІВ ПІДСУМКИ СВОЄЇ ДІЯЛЬНОСТІ У 2022 РОЦІ

Наприкінці 2022 року Кіберкомандування США (CYBERCOM) підбили підсумки своєї діяльності та основні напрямки своїх зусиль у 2022 році. До цих напрямків належать:

- зміцнення відносин із партнерами та союзниками;
- проведення двох ітерацій щорічних навчань CYBERCOM CYBER FLAG - CF22 та CF23-1;
- забезпечення безпеки проміжних виборів в США;
- розвиток інновацій та розвитку Місія національних кіберсил (CNMF).

Окремо підкреслено важливість операції Hunt Forward – розгортання в Україні найбільшої в історії CYBERCOM групи розслідування, що складалась з операторів ВМС США та Корпусу морської піхоти США. Група займалась полюванням на зловмисну кіберактивність в українських мережах. Група працювала спільно з українськими колегами та усунути потенційні загрози напередодні російської агресії.

CISA ОПРИЛЮДНИЛА ЗВІТ ПРО СВОЮ ДІЯЛЬНІСТЬ У 2022 РОЦІ

12 січня CISA випустила підсумковий звіт про свою діяльність у 2022 році. Серед ключових здобутків:

- оприлюднення базових вимог кібербезпеки (performance goals) для всіх секторів критичної інфраструктури;
- впровадження нових технологій кіберзахисту федеральних мереж;
- координація процесом розкриття вразливостей через платформу Vulnerability Information and Coordination Environment;
- запуск ініціативи державно-приватного партнерства JCDC;
- проведення восьмої вправи з кібербезпеки Cyber Storm для 2000 учасників та інші.

ANSSI ОПРИЛЮДНИЛА ЗВІТ ПРО ОСНОВНІ КІБЕРЗАГРОЗИ У 2022 РОЦІ

24 січня французька ANSSI оприлюднила підсумки своєї діяльності у 2022 році та визначали ключові загрози, з якими вона стикалась за цей період. На їх думку російсько-українська кібервійна прямо не вплинула на характер основних кіберзагроз, хоча і створила для багатьох традиційних сприятливіше середовище.

Кібершпигунство залишається основною проблемою – більша частина операцій з кіберзахисту, до яких вдалась ANSSI, стосувались діяльності китайських хакерів. При цьому зловмисники як і раніше не шукають весь час нові вразливості, а експлуатують наявні чи шукають менш захищені цілі (де не дотримуються вимог кібербезпеки). І жертви просто не звертаються, а замість цього платять викуп.

У 2022 РОЦІ НАЙБІЛЬШЕ КІБЕРАТАК БУЛО СПРЯМОВАНО ПРОТИ АКАДЕМІЧНОГО СЕКТОРУ – ДОСЛІДЖЕННЯ CHECK POINT RESEARCH

20 січня Check Point Research оприлюднило результати свого дослідження за 2022 рік щодо кількості та спрямованості кібератак. За результатами отриманих даних, загальна кількість атак зросла на 38%, а найбільше і найчастіше атакують освітній та науковий сектори – у середньому 2314 атак на організацію щотижня. Водночас найбільшу динаміку приросту атак показує галузь охорони здоров'я – в середньому 1463 атаки на організацію щотижня (зростання становить 74% порівняно з попереднім роком).

ДОСЛІДНИКИ ПРОПОНУЮТЬ США ВЗЯТИ НА СЕБЕ ОДНОСТОРОННІ ЗОБОВ'ЯЗАННЯ ЩОДО ПРОСУВАННЯ НОРМ КІБЕРБЕЗПЕКИ НА ГЛОБАЛЬНОМУ РІВНІ

У січні два дослідники з Belfer Center for Science and International Affairs, Harvard Kennedy School Б. Саундерс та А.Купер оприлюднили результати свого дослідження, в якому вказують на важливість впровадження міжнародних норм/правил кібербезпеки задля більшої безпеки людства.

Вони пропонують США взяти на себе односторонні зобов'язання в цьому питанні та змінити свою кібербезпекову політику, що впливатиме і на інших міжнародних суб'єктів. Ці заходи включають посилення обов'язковості дотримання вимог кібербезпеки в середині США, більшу увагу до безпеки ланцюжків постачання, недопущення поширення кіберзброї (cyberweapon proliferation) та інші – всього 9 основних пунктів.

КІБЕРПАНДЕМІЯ СТАЄ ВСЕ МАСШТАБНІШОЮ

18 січня Д. Фрідман, автор видання Newsweek, аналізуючи ситуацію з розвитком кіберзлочинності, вказує на те, що складно знайти хоча б якісь прийнятні стратегічні рішення для таких зменшення загроз. Цьому сприяє як величезний зиск від кіберзлочинної діяльності (не лише фінансовий, але і розвідувальний), але і не бажання громадян свідомо ставитись до власної кібербезпеки (оскільки це створює їм незручності). Серед можливих рішень він називає зменшення доступності своїх цифрових даних в Мережі (в т.ч. номерів мобільних телефонів, імейлів та дат народження).

ШВЕЙЦАРСЬКІ НАУКОВЦІ ВИЯВИЛИ ЩОНАЙМЕНШЕ 7 ВРАЗЛИВОСТЕЙ У ЗАХИЩЕНОМУ МЕСЕНДЖЕРІ THREEMA

У першу декаду січня університетська група прикладної криптографії ETH Zurich опублікувала дослідження із детальним описом семи вразливостей у домашніх криптографічних протоколах Threema. Вразливості могли дозволити зловмиснику клонувати облікові записи та читати їхні повідомлення, а також викрадати приватні ключі та контакти, або навіть виготовляти компрометуючий матеріал для цілей шантажу.
Розробники Threema заперечують вплив вразливостей на функціональність месенджера, вказуючи, що вони стосуються протоколу, який Threema більше не використовує.

ПІДСУМКОВИЙ ЗВІТ CISCO TALOS ПРО ЛАНДШАФТ ЗАГРОЗ У 2022 РОЦІ

24 січня кібербезпекова компанія Cisco Talos оприлюднила свій підсумковий звіт про кібербезпекову ситуацію у 2022 році. Крім виразного впливу російсько-українського кіберпротистояння, спеціалісти компанії відзначають ще декілька важливих тенденцій:

- кібербезпекові інструменти подвійного призначення залишають зловмисним суб'єктам можливості непомітно залишатись в ураженому середовищі;
- злочинці активно використовують у своїх цілях легітимні утиліти/системи (на кшталт PowerShell);
- розширення масштабів використання традиційної форми поширення вірусів через USB.

ЗРОСТАЄ КІЛЬКІСТЬ ЛЮДСЬКИХ ЖЕРТВ ВНАСЛІДОК КІБЕРАТАК НА ЛІКАРНІ

Збільшення кількості ransomware атак на лікарні та відповідне збільшення кількості смертей викликають занепокоєння адміністрації США. І хоча статистику знайти важко, адже смерть не завжди настає одразу після того, як пацієнту не надали необхідної допомоги, очевидно, що кібератаки завдають значної шкоди здатності лікарень надавати послуги пацієнтам.

За словами національного радника з кібербезпеки та ризиків Американської асоціації лікарень Джона Ріггі, настав час розглядати атаки програм-вимагачів на лікарні, як злочини, що загрожують життю, а не як фінансові злочини.

Питання також виникає і через можливість ворожої країни атакувати лікарню в країні НАТО, і чи призведе така атака до активації статті 5, якщо вона буде навмисною і матиме наслідком смерть значної кількості людей.

У своєму підсумковому звіті за 2022 рік фірма Krol дійшла висновку, що найбільш значні витоки даних відбувалися в секторі охороні здоров'я та фінансах.

КІЛЬКІСТЬ КІБЕРАТАК НА УРЯДИ ЗРОСЛА НА 95% В ОСТАННЬОМУ ПІВРІЧЧІ 2022 РОКУ

Згідно з новим звітом компанії з кібербезпеки CloudSek, опублікованому 30 грудня, кількість атак, спрямованих на урядовий сектор, у другій половині 2022 року у всьому світі зросла на 95% порівняно з тим самим періодом 2021 року.

Згідно зі звітом, збільшення кількості атак можна пояснити стрімкою цифровізацією та переходом до віддаленої роботи під час пандемії, що розширило зону атаки державних установ і проклало шлях до інтенсифікації кібервійни, яку ведуть національні держави.

ПРОГНОЗ ЩОДО БЕЗПЕКИ У 2023: КІБЕРВІЙНА РОЗШИРЮЄ КОЛО ЗАГРОЗ

Як зазначає eSecurity Planet, 2023 рік не буде простішим за 2022 з точки зору атак рансомвер та збереження даних користувачів. Публікація містить загрози, цілі та вектори атак, які, ймовірно, будуть популярні серед кіберзлочинців наступного року. До них належать:

- вайпери, загрози критичній інфраструктурі перекинулися й на інші країни через війну в Україні. У 2023 році така тенденція продовжиться;
- рансомвер як послуга і кіберзлочини як послуга продовжать розвиватися. Серед іншого, розвиватимуться послуги «детективів» у дарк вебі, які збиратимуть інформацію про потенційних жертв перед атакою;
- атаки на ланцюги постачання, залежність залишатимуться проблемою, хоча почнуть з'являтися рішення;
- підвищиться увага до ефективності продуктів, для створення безпеки, зокрема з боку користувачів, які зазвичай мають недостатньо інформації про це;
- кінцеві користувачі залишаються вразливістю. Вектор атаки, швидше за все, буде незмінним, а розвиток технологій на кшталт діп фейків вимагатиме від користувачів бути постійно напоготові;
- автоматизація та послуги з кібербезпеки набуватимуть важливості з огляду не зростаючу кількість та складність атак. Особливо актуальними вони будуть для малого та середнього бізнесу;
- більше компаній відмовляються від куків, наслідуючи ініціативу Google. Для користувачів це означатиме більше приватності, а для сфери реклами – звуження можливостей;
- розвиток Metaverse призведе до збільшення кількості хакерських атак;
- велика кількість атак та викрадених даних, швидше за все, призведе до більш активного регуляторного втручання держави;
- залучення більшої кількості громадян у процеси регулювання та адаптації до нової кіберреальності завдяки усвідомленню ними ризиків, з якими вони стикаються у кіберпросторі.

НАЙЧАСТІШЕ ХАКЕРИ ШУКАЛИ ОСОБИСТУ ІНФОРМАЦІЮ

Нещодавно опубліковане дослідження компанії Imperva, у якому було проаналізовано 100 найбільших зломів з липня 2021 року по липень 2022 року, показало, що хакери полювали за особистою інформацією в 42,7% випадків.

З усіх типів даних, доступних для викрадення (інформація кредитної картки, паролі, вихідний код тощо), автори дослідження вважають, що персональні дані є найціннішими, оскільки злочинці можуть отримати додаткові персональні дані з дарк веб і тоді вдаватися до заходів, які ускладнюють запобігання шахрайству чи повній крадіжці цифрової особистості користувача.

УГРУПОВАННЯ LOCKBIT ЗСЕРЕДИНИ – ЗВІТ ANALYST1

Дослідник фірми Analyst1 Джон ДіМаджіо опублікував звіт «Щоденники програм-вимагачів: том 1», у якому описав результати власного дослідження внутрішнього функціонування угрупування, отримані шляхом інфільтрації в його середовище.

«Я хотів краще дослідити людську сторону операції, щоб дізнатися про ідеї, мотивацію та поведінку людей по той бік клавіатури», – пише ДіМаджіо.

У своєму дослідженні ДіМаджіо описує весь життєвий цикл діяльності LockBit від вересня 2019 до січня 2022. Серед іншого, він виявив, що той самий інженер-програміст зіграв важливу роль у створенні шкідливого програмного забезпечення, яке керує п'ятьма елітними кіберзлочинними групами: BlackCat, DarkSide, BlackMatter, LockBit Black і Fin7. Цей розробник може неабияк зацікавити американські і міжнародні правоохоронні органи, вважає дослідник. Він також стверджує, що спільнота угруповань, що вдаються до вимагання за допомогою вірусів, набагато менша, ніж про неї думають. А, також, що багато хто з її учасників знайомі між собою.

ВИВЧЕННЯ СОЦІАЛЬНИХ КІЛ KILLNET

Як стверджує Radware у статті, опублікованій 27 січня, аналітикам не часто вдається дослідити соціальні кола кримінальних організацій, але саме проросійське хакерське угруповання Killnet, яке здійснює переважно DDoS атаки на противників російської агресії в Україні, виявилося більш прозорим за багатьох інших.

Його очільник Killmilk є набагато публічнішим, ніж лідери інших кримінальних угруповань, що дозволяє організації привертати більше уваги, встановлювати нові зв'язки та збирати гроші на свою діяльність.

У статті на Radware Blog розглянуто три соціальні кола, пов'язані зі злочинною організацією Killnet, і досліджено, як діяльність групи отримала соціальну та фінансову підтримку з боку росіян, які підтримують окупацію України.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

УКРАЇНА ПІДПИСАЛА УГОДУ ПРО ПРИЄДНАННЯ ДО ОБ'ЄДНАНОГО ЦЕНТРУ ПЕРЕДОВИХ ТЕХНОЛОГІЙ З КІБЕРОБОРОНИ НАТО

Секретар РНБО України Олексій Данілов 19 січня підписав Технічну угоду про приєднання України до Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE). Заявку Національного координаційного центру кібербезпеки при РНБО України щодо членства України в Центрі було одностайно підтримано рішенням Керівного комітету Центру 4 березня 2022 року.

Після підписання угоди Секретарем РНБО (керівник НКЦК) її буде передано на підпис всім країнам-членам Центру. Присутність України в Центрі посилить обмін кібердосвідом між Україною та країнами-членами CCDCOE. Крім того, це важливий крок на шляху вступу України до НАТО.

О. Данілов зазначив, що Україна, яка вже понад вісім років бореться з країною-терористом на усіх фронтах, показала високий рівень стійкості й у кіберпросторі. «Ми не просто вистояли, а й стали прикладом для всього світу. Це підтверджують і наші партнери з НАТО», – наголосив він.

Секретар РНБО назвав російських хакерів загрозою для всього світу, нагадавши, що протягом минулого року вони неодноразово атакували наших партнерів – держави, які надають всебічну підтримку Україні для перемоги у цій війні. За словами О. Данілова, йдеться «про першу світову кібервійну, і для протидії цій війні ми формуємо дієву міжнародну кіберкоаліцію, маємо об'єднатися для протистояння спільному ворогу».

НАТАЛІЯ ТКАЧУК: ОБМІН ДОСВІДОМ З ВЕЛИКОЮ БРИТАНІЄЮ ЩОДО ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ТА КІБЕРАТАКАМ Є ВАЖЛИВИМ І АКТУАЛЬНИМ ДЛЯ УКРАЇНИ

Обмін досвідом з Великою Британією щодо протидії дезінформації та кібератакам є важливим і актуальним для України. На цьому наголосила керівник служби з питань інформаційної безпеки та кібербезпеки Апарату Ради національної безпеки і оборони України, секретар НКЦК Наталія Ткачук під час зустрічі 23 січня з представниками Лондонської торгово-промислової палати та муніципалітету Лондонського Сіті, організованою Торгово-промисловою палатою України.

Н. Ткачук зазначила, що Велика Британія є одним із ключових та найважливіших партнерів України, зокрема у питаннях кіберзахисту та боротьби з дезінформацією. «Минулого року Велика Британія оновила законодавство у сфері національної безпеки, зокрема щодо протидії дезінформації та кібератакам. Країна посилила співпрацю з інтернет-провайдерами, компаніями Meta та Google задля виявлення та викорінювання дезінформації із соціальних мереж, а також посилила державний контроль у цій сфері. Цей досвід є надзвичайно важливим та актуальним для України, адже триває війна, і ми боремося з рф й в інформаційному та кіберпросторі», – сказала Н.Ткачук.

Керівник служби також зауважила, що Велика Британія підтримувала Україну із самого початку кібервійни, зазначивши, що нині вже весь світ усвідомив, що рф є країною–терористом.

У заході також взяли участь представники Верховної Ради України, Кабінету Міністрів України, бізнес-асоціацій та приватного сектору.

СБУ НЕЙТРАЛІЗУВАЛА СПРОБУ РОСІЙСЬКИХ ХАКЕРІВ ПРОНИКНУТИ У КОМП'ЮТЕРНІ МЕРЕЖІ БАГАТОКВАРТИРНИХ БУДИНКІВ

Кіберфахівці СБУ нейтралізували російську хакерську атаку на електронні системи житлової інфраструктури у одному із прикордонних регіонів України. Через Wi-Fi мережу багатоквартирних будинків хакери хотіли дистанційно підключитись до системи відеоспостереження за територією житлових комплексів, прилеглими автомобільними дорогами тощо. Таким чином вони планували мати прихований канал для збору інформації про ситуацію в місті.

Також агресора цікавили відомості щодо адрес проживання українських правоохоронців та можливого переміщення військової техніки. Однак, співробітники СБУ спрацювали на випередження і своєчасно викрили спробу окупантів проводити розвідувально-підривну діяльність у прикордонному регіоні.

За оперативними даними, до кібератаки причетне підконтрольне спецслужбам рф хакерське угруповання з росії, яке спеціалізується на зламах електронних систем інфраструктурних об'єктів.

НАТАЛІЯ ТКАЧУК: НЕОБХІДНО РОЗГЛЯНУТИ МОЖЛИВІСТЬ СТВОРЕННЯ ЄВРОПЕЙСЬКОЇ КІБЕРКОАЛІЦІЇ ДЛЯ СПІЛЬНОГО РЕАГУВАННЯ У ВИПАДКУ МАСШТАБНИХ КІБЕРАТАК

Наталія Ткачук взяла участь у зустрічі з політичним керівництвом, що представляє 290 муніципалітетів та 21 регіон Швеції, Шведської асоціації місцевих органів влади та регіонів, у режимі онлайн. Вона поділилася досвідом України щодо протидії ворогові у кіберпросторі під час першої у світі кібервійни, що триває нині, та наголосила на необхідності створення європейської кіберкоаліції.

«Завдяки спільній злагодженій роботі всіх суб'єктів кібербезпеки Україна показала високу стійкість національної системи кібербезпеки. Зараз необхідно розглянути можливість створення європейської кіберкоаліції, яка б не тільки забезпечувала обмін інформацією, розвідувальними даними та єдині стандарти кібербезпеки, але й передбачала створення спільних механізмів реагування у випадку масштабних кібератак та протоколів спільних дій як на національному, так і на міжнародному рівні. І Україна готова ділитися власним досвідом», – сказала вона.

Н. Ткачук також акцентувала на необхідності обговорення на світовому рівні питання щодо ухвалення норм міжнародного права, які б чітко визначали зміст кібервійни, правила її ведення, кібератак та відповідальності за ці дії: «Вже зараз потрібно сформувати чітке бачення, які види кібератак слід вважати воєнними злочинами. Визначити правовий статус кіберкомбатантів і механізм захисту наших кіберволонтерів за міжнародним правом».

Секретар НКЦК подякувала міжнародним партнерам за допомогу. «У цій кібервійні на боці України сьогодні весь демократичний світ – кіберволонтери, урядові структури, IT-бізнес. Ми високо цінуємо їхню підтримку. Але для перемоги нам дуже потрібна зброя, зокрема кіберзброя», – зазначила вона.

ПРЕДСТАВНИКА МІНОБОРОНИ УКРАЇНИ ВКЛЮЧИЛИ ДО РАДИ ДИРЕКТОРІВ РЕГІОНАЛЬНОГО ЦЕНТРУ З КІБЕРЗАХИСТУ В КАУНАСІ

Згідно з Меморандумом щодо взаєморозуміння між Міністерством оборони України та Міністерством національної оборони Литовської Республіки, українські військові беруть активну участь у роботі Регіонального центру з кіберзахисту (RCDC) у місті Каунас.

Серед завдань RCDC — проведення аналізу кіберзагроз, організація навчання спеціалістів із кібербезпеки, проведення наукових досліджень у сфері кібербезпеки, а також розвиток співпраці зі стратегічними партнерами.

Спільні заходи військових фахівців з кібербезпеки проводяться з метою поглиблення взаємовигідної співпраці у сфері розвідки та аналізу кіберзагроз. Крім того, це обмін досвідом фахівців на реагування, обробку і захист від кіберзагроз. Наші фахівці вивчать можливості RCDC щодо забезпечення засобами кіберзахисту (апаратне та програмне забезпечення) в інтересах розвитку систем кіберзахисту Міністерства оборони України та Збройних Сил України, а також розширення технічних можливостей RCDC. Практичні навчання у складі кіберпідрозділів RCDC та на базі навчального центру RCDC додають українським фахівцям практичного досвіду реагування на кіберзагрози.

СБУ ЗАПОБІГЛА СПРОБАМ ЗЛАМУ ДЕРЖАВНОЇ ЕЛЕКТРОННОЇ СИСТЕМИ У ГАЛУЗІ БУДІВНИЦТВА

Кіберфахівці СБУ викрили та зупинили зловмисників, які намагалися легалізувати незаконні забудови через злам Єдиної державної електронної системи у сфері будівництва, а також видавали підроблені сертифікати атестації архітекторів.

«Ми вчасно викрили незаконні схеми і не дозволили зловмисникам зламати державну електронну систему. Мова йде не про звичайний кіберзлам, а про злочини, які могли б призвести до дуже серйозних наслідків у майбутньому. Якби не реакція СБУ, в Україні змогли б узаконити сотні «проблемних» забудов, які були зведені з порушенням чинних вимог і стандартів. А це – ризик техногенних аварій та інших надзвичайних ситуацій. А значить – і ризик для тисяч українців», – підкреслив Ілля Вітюк.

Також, з його слів, не допущено запуск нової масштабної корупційної схеми в будівельній сфері.

«Будівельна сфера стала першою, де команді Мінцифри вдалося реалізувати справжню цифрову трансформацію. Цифровізація дає прозорі інструменти для фіксування кожної дії. Завдяки створенню Єдиної державної електронної системи у сфері будівництва держава заощаджує мільярди гривень щорічно. Окрім цього, стало можливим запобігти і виявити протиправні схеми в будівельній сфері. Адже система побудована таким чином, що цифровий слід кожного користувача залишається назавжди і його легко відстежити», – зазначив віцепрем'єр-міністр – міністр цифрової трансформації Михайло Федоров.

За даними спецслужби, до організації оборудок причетні високопосадовці Національної спілки архітекторів України, відомі «тіньові» посередники. Перевіряється також причетність посадовців органів державної влади та місцевого самоврядування. Зловмисники намагались незаконно отримати гроші через підробку та продаж дозвільних документів представникам будівельного бізнесу.

Серед викритих махінацій – незаконні реєстрації об'єктів, які мають порушення державних будівельних норм, а також - схема видачі підроблених сертифікатів професійної атестації архітекторів. При цьому «архітектором» можна було зробити будь-кого.

УКРАЇНСЬКИЙ ДОСВІД ПРОТИСТОЯННЯ РОСІЙСЬКИМ КІБЕРАТАКАМ ОБГОВОРИЛИ У ВЕЛИКІЙ БРИТАНІЇ

Заступник голови Держспецзв'язку Віктор Жора та представник урядової Команди реагування на комп'ютерні надзвичайні події (CERT-UA), відвідали Національний центр кібербезпеки (National Cyber Security Centre – NCSC) Сполученого Королівства Великої Британії та Північної Ірландії. Ключовою темою діалогу з британськими колегами стало подальше посилення співпраці та об'єднання зусиль для протидії російській агресії у кіберпросторі та необхідність інтенсифікації обміну інформацією про кіберінциденти.

Віктор Жора зазначив, що світ здебільшого спостерігає за російським вторгненням на землі, натомість агресія у кіберпросторі є менш помітною. Однак кількість кібератак проти України минулого року потроїлася, і значна частина з них координувалися з іншими напрямами воєнних дій, наприклад, ракетними ударами.

Під час поїздки українські представники взяли участь у конференції CyberThreat 2022, яка пройшла в Лондоні. Заступник начальника CERT-UA Євген Бриксін розповів учасникам заходу про опрацьовані командою кіберінциденти. Також він презентував аналітичну та технічну інформацію щодо тактик, технік та інструментів, які використовують хакерські групи, пов'язані з урядом рф, під час здійснення кібератак на українські організації та установи.

НКЦК ПРАЦЮЄ НАД УДОСКОНАЛЕННЯМ ПРОЦЕДУРИ ПУБЛІЧНИХ КОМУНІКАЦІЙ ПІД ЧАС РЕАГУВАННЯ НА МАСШТАБНІ КІБЕРАТАКИ

НКЦК за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури» 26 січня провів засідання круглого столу на тему «Національний план реагування на надзвичайні (кризові) ситуації в кіберпросторі: практичні аспекти ефективної публічної комунікації про кіберінциденти».

У засіданні взяли участь комунікаційні менеджери та фахівці з кібербезпеки всіх основних суб'єктів забезпечення кібербезпеки, Центру протидії дезінформації, Міністерства охорони здоров'я, Національної служби здоров'я України, Міністерства культури та інформаційної політики та Державної служби України з надзвичайних ситуацій, підприємств критичної інфраструктури.

Метою заходу було формування спільного розуміння всіма сторонами важливості координації дій і взаємоузгодження повідомлень для суспільства про виявлені інциденти та кризові явища в кіберпросторі. Учасники круглого столу обговорили питання щодо поточного стану інформування суспільства про кризові явища в кіберпросторі та про окремі кіберінциденти. За результатами обговорення внесено пропозиції щодо вдосконалення процесів інформування суспільства про кіберінциденти та наповнення Плану реагування.

КОМАНДИ-ПЕРЕМОЖЦІ МИНУЛОРІЧНОГО НАЦІОНАЛЬНОГО ОБОРОННОГО ХАКАТОНУ ВІЗЬМУТЬ УЧАСТЬ У ХАКАТОНІ НАТО У ВАРШАВІ

Команда кіберполіції «С.О.Р.», яка за результатами змагань National Defence Hackathon 2022 зайняла перше місце за технічним напрямком серед команд державного сектору України, представлятиме державні органи України на щорічному змаганні з програмування НАТО TIDE Hackathon 2023. Відповідний сертифікат від партнерів НАТО команда «С.О.Р.» отримала в рамках проєкту з обміну знаннями Трастового фонду НАТО — Україна С4 (командування, управління, зв'язок, ком'ютеризація).

NATO TIDE Hackathon 2023 відбудеться наприкінці лютого в Польщі. Серед головних завдань змагань, зокрема, розробка нових програмно-апаратних рішень, розробка інноваційних архітектурних моделей, методів для представлення і розуміння інформації посадовими особами органів управління. А також забезпечення інформаційної взаємодії підрозділів шляхом обміну знаннями під час спільного вирішення проблем.

У NATO TIDE Hackathon 2023 також братимуть участь й інші переможці National Defence Hackathon 2022: команда «Валькірія», що зайняла перше місце за технічним напрямком у змаганнях з-поміж учасників з приватного сектору та команда «ДДК ДССЗЗІ», яка за результатами Національного оборонного хакатону 2022 року була другою серед команд державного сектору.

РЕКТОРА, ВИКЛАДАЧІВ ТА КУРСАНТІВ НАЦІОНАЛЬНОЇ АКАДЕМІЇ СБУ НАГОРОДЖЕНО ВІДЗНАКАМИ РНБО УКРАЇНИ

У річницю створення Національної академії Служби безпеки України заступник Секретаря РНБО України Сергій Демедюк вручив нагороди її співробітникам та курсантам.

«Насамперед хочу подякувати курсантам, хлопцям та дівчатам, які нині, під час війни, допомагають державі боротися з ворогом та в майбутньому покарати винних. Адже ваш неоціненний досвід та ідеї сприятимуть розбудові системи національної безпеки і оборони держави. Також хочу відзначити волонтерську діяльність Академії та подякувати її керівництву, кожному викладачу, працівнику, які в такий важкий для країни час продовжує навчати майбутніх фахівців», – сказав заступник Секретаря РНБО.

За ефективну співпрацю з НКЦК в інтересах національної безпеки і оборони України, значний вклад у підготовку висококваліфікованих спеціалістів у сфері кібербезпеки, високий професіоналізм, ініціативу і наполегливість ректора Академії Андрія Черняка та викладачів закладу нагороджено відзнаками РНБО України. Також з нагоди свята С. Демедюк вручив подяки найактивнішим у співпраці з НКЦК курсантам Академії за старанність і наполегливість у навчанні, ініціативність та сприяння діяльності НКЦК під час дії правового режиму воєнного стану.

УКРАЇНА ТА ФІНЛЯНДІЯ СПІВПРАЦЮВАТИМУТЬ У СФЕРІ ЦИФРОВІЗАЦІЇ ТА ЦИФРОВОЇ СТІЙКОСТІ – ПІДПИСАНО МЕМОРАНДУМ

Мінцифра та Міністерство транспорту та зв'язку Фінляндії підписали меморандум у сфері цифрової трансформації. Під час зустрічі сторони обговорили подальший обмін досвідом та співпрацю країн у відбудові цифрової інфраструктури та посиленні кіберзахисту.

«Ми вдячні Фінляндії за підтримку цифровізації в Україні у такий складний час. Підписаний меморандум допоможе підсилити цифрову трансформацію та модернізацію телеком-інфраструктури в Україні. Також будемо переймати найкращі практики для запобігання кіберзагрозам та гібридним загрозам і розвивати цифрову стійкість держави», – зазначив Михайло Федоров.

«Я дуже вражений роботою, яку зробила Україна для просування цифровізації. Цією угодою ми вже заглядаємо в період відновлення України. Я вірю, що ми можемо багато чого навчитися один у одного», – додав Тімо Гаракка.

Підписаний меморандум дасть змогу країнам обмінюватися досвідом у сферах цифровізації, інформаційних технологій та кібербезпеки. Україна і Фінляндія співпрацюватимуть у галузі цифрової стійкості, а також у сфері відбудови та модернізації цифрової інфраструктури.

ЗА ПІДТРИМКИ НКЦК ВІДБУВСЯ ЧЕТВЕРТИЙ НАВЧАЛЬНИЙ МОДУЛЬ ПРОГРАМИ СТРАТЕГІЧНОГО ЛІДЕРСТВА ДЛЯ УПРАВЛІНЦІВ У СФЕРІ КІБЕРБЕЗПЕКИ «SJC-2022»

Четвертий навчальний модуль програми стратегічного лідерства для управлінців у сфері кібербезпеки «SJC-2022» був присвячений «(не)очевидним, але вирішальним партнерствам 2.0». У навчаннях взяли участь дві команди – «Академія Цивільного Офіцерства» та «Sophos Joint Cyber». Майже 70 учасників – держслужбовці, військові, правоохоронці, управлінці, волонтери, підприємці, представники міжнародних партнерів, розробляли стратегії взаємозв'язків та екосистеми майбутнього в кіберпросторі.

«Ключовим завданням НКЦК є побудова ефективної національної системи кібербезпеки, і головна складова цієї системи – кадровий потенціал. Тому один з пріоритетів – збільшення якісного кадрового потенціалу держави у сфері кібербезпеки як у державному, так і в приватному секторі», – зазначила керівник служби з питань інформаційної та кібербезпеки Апарату РНБО України, секретар НКЦК Наталія Ткачук.

КІБЕРАТАКА НЕ ЗМОГЛА ЗУПИНИТИ РОБОТУ ІНФОРМАЦІЙНОГО АГЕНТСТВА «УКРІНФОРМ»

Завдяки оперативним діям Урядової команди реагування на комп'ютерні надзвичайні події (CERT-UA) атака російських хакерів 17 січня на Українське національне інформаційне агентство «Укрінформ» не зупинила його роботи – українці та весь світ і надалі можуть отримувати оперативну та об'єктивну інформацію про ситуацію в країні.

«Росіяни від перших днів повномасштабного вторгнення роблять спроби позбавити українців інформації про стан справ у країні та хід війни. Вони відключали українське телебачення, інтернет та мобільний зв'язок на тимчасово окупованих територіях, завдавали ракетних ударів по теле- та радіовежах у багатьох українських містах. Здійснювали кібератаки на українські ЗМІ. Атака на Укрінформ – це чергова спроба знищити правду», – зазначив голова Держспецзв'язку Юрій Щиголь.

КІБЕРПОЛІЦЕЙСЬКІ КИЄВА ВИКРИЛИ СПІВМЕШКАНЦІВ У ШАХРАЙСТВІ З ВИКОРИСТАННЯМ ФІШИНГУ

Зловмисники отримували доступ до банківських карт громадян і використовували гроші потерпілих для розрахунків у інтернет-магазинах. Організатору схеми оголосили підозру.
21-річний уродженець Миколаївщини спільно зі своєю співмешканкою використовували фішингові посилання та Telegram-боти для отримання банківських даних громадян. Фішинг маскували під надання соціальної допомоги від держави. Також правопорушники купували в Даркнеті скомпрометовані дані банківських карт громадян.

Використовуючи ці відомості, вони розраховувалися в інтернет-магазинах грошима з рахунків потерпілих. Більшість товарів купували для власного користування, а частину з них – перепродавали на платформах оголошень.

Працівники поліції наразі встановлюють потерпілих. За місцем мешкання фігурантів правоохоронці провели обшуки. Вилучено мобільні телефони, ноутбуки, техніку, товарні чеки та банківські картки. До проведення слідчих дій також залучили працівників полку поліції особливого призначення.

З ЛЮТОГО 2022 РОКУ КІЛЬКІСТЬ АТАК НА ЕНЕРГЕТИЧНИЙ СЕКТОР УКРАЇНИ ЗРОСЛА НА 20-25%

В опублікованій 11 січня статті видання The Record представники енергетичного сектору України оприлюднили деталі російських кібератак проти українського енергетичного сектору. Зокрема зазначено, що з лютого 2022 року кількість атак на енергетичний сектор України зросла на 20-25%. Найпоширенішими атаками були DDoS, фішинг і спроби виконання зловмисного коду. За даними Укренерго, кібератаки були найбільш інтенсивними у березні 2022 року, коли Україна підключалася до енергосистеми ЄС.

РОСІЙСЬКІ КІБЕРАТАКИ МОЖУТЬ КВАЛІФІКУВАТИСЯ ЯК ВІЙСЬКОВІ ЗЛОЧИНИ

В інтерв'ю виданню Politico, опублікованому 9 січня, заступник голови Держспецзв'язку Віктор Жора повідомив, що Україна збирає цифрові докази для суду в Гаазі, щоб виконавців кібератак на критичну інфраструктуру було притягнуто до відповідальності за воєнні злочини.

За його словами, кібератаки, які здійснювала РФ, були зкоординовані з кінетичними атаками, які здійснювалися проти цивільної інфраструктури, що є воєнним злочином, і тому також належать до воєнних злочинів. Як приклад Жора наводить атаки на компанію ДТЕК, коли одночасно атакували фізичні об'єкти та електронну мережу компанії. Якщо Україні вдасться добитися такого покарання, це буде вперше в історії.

УКРАЇНА ЗАКЛИКАЄ ДО СТВОРЕННЯ «КІБЕРООН» НА ТЛІ НАПАДІВ РОСІЇ

15 січня видання Politico повідомило, що Голова ДССЗЗІ Юрій Щиголь закликав до створення «Кібер Організація Об'єднаних Націй» – організації, в рамках якої держави «можуть обмінюватися інформацією, підтримувати одна одну та взаємодіяти». Щиголь вважає, що цивілізовані країни мають мати «один спільний кіберпростір».

ВАДИМ ЛЄДНЄЙ: «МЕТОЮ ДІЯЛЬНОСТІ КІБЕРСИЛ ЗСУ Є ЗАХИСТ СУВЕРЕНІТЕТУ ДЕРЖАВИ ТА ВІДСІЧ ЗБРОЙНОЇ АГРЕСІЇ В КІБЕРПРОСТОРІ»

Збройні сили України займаються питанням діяльності в кіберпросторі з 2010 року, говорить фахівець з кіберборотьби Генштабу ЗСУ Вадим Лєднєй. В інтерв'ю Глобальному центру взаємодії в кіберпросторі він розповідає про українські кібервійська, їхню мету, склад і функції.

8. ПЕРША СВІТОВА КІБЕРВІЙНА

ПОЛЬЩА ПОПЕРЕДЖАЄ ПРО АТАКИ ХАКЕРСЬКОЇ ГРУПИ GHOSTWRITER, ПОВ'ЯЗАНОЇ З РОСІЄЮ

Згідно з офіційним повідомленням на державному сайті Польщі, країна була мішенню для кібератак протягом усього часу від початку агресії рф проти України. Їх кількість збільшилася наприкінці 2022 року. Польський уряд пов'язує цей факт зі своєю постійною підтримкою України, а, також, адвокацією протидії російській агресії на міжнародній арені.

Хакерські групи, «пов'язані з кремлем», використовують програми-вимагачі та DDoS атаки та фішингові атаки з цілями «дестабілізації, залякування та сіяння хаосу», пише польське урядове агентство.

КІЛЬКІСТЬ КІБЕРАТАК, НАЦІЛЕНИХ НА УКРАЇНУ, ЗРОСЛА В 20 РАЗІВ В 4 КВАРТАЛІ 2022 РОКУ – TRELLIX

За даними звіту компанії Trellix, який вони поширили 24 січня, в останньому кварталі 2022 року відбулось 20-кратне збільшення кібератак через електронну пошту на державний і приватний сектори України. Trellix Advanced Research Center вважає цю активність пов'язаною з угрупуванням Gamaredon.

ПОСИЛЕНЕ ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО СТАЛО ВАЖЛИВИМ ЧИННИКОМ ПРОТИДІЇ РОСІЙСЬКІЙ КІБЕРАКТИВНОСТІ – TRELLIX

24 січня кібербезпекова компанія Trellix оприлюднила свій аналіз щодо основних тенденцій кібербезпеки у 2022 році. На думку Trellix, ключовим фактором ландшафту загроз стала російсько-українська кібервійна. Вона проявила і важливий фактор ефективного спротиву – посилене державно-приватне партнерство. Завдяки йому відбувався активний обмін розвідувальною інформацією про загрози, команда швидкого реагування надавали взаємну підтримку та оперативно видаляли зловмисне програмне забезпечення по всьому світу, порушували роботу ботнетів і попереджали небезпечні кібератаки.

РОСІЙСЬКА ЕКОСИСТЕМА КІБЕРБЕЗПЕКИ ПОЛІТИЗУЄТЬСЯ ПІД ВПЛИВОМ САНКЦІЙ ПРОТИ РОСІЇ – BROOKINGS INSTITUTION

12 січня дослідник Джастін Шерман з Brookings Institution надав огляд тенденцій в російській кібербезпековій спільноті на фоні продовження кібервійни та впровадження санкцій проти росії. На прикладі тематик щорічної конференції Positive Hack Days він відзначає зростання націоналістичної риторики та загальної політизації сфери кібербезпеки в росії. Вказує на частішу риторику «відмову від іноземних продуктів», публічну підтримку дій російського уряду та намагання змінити зовнішні вектори розвитку з західного ринку на азійський.

РОСІЙСЬКІ ХАКЕРИ АТАКУВАЛИ АМЕРИКАНСЬКИХ НАУКОВЦІВ – ЯДЕРНИКІВ

Відповідно до електронних записів, перевірених Reuters, і п'ятьма експертами з кібербезпеки, минулого літа російська хакерська група, відома як Cold River, атакувала три ядерні дослідницькі лабораторії у США.

У період із серпня по вересень, коли Путін заявив, що росія готова використати ядерну зброю для захисту своєї території, Cold River завдала ударів по Брукхейвенській (BNL), Аргоннській (ANL) і Ліверморській національній лабораторії Лоуренса (LLNL). Дослідження продемонструвало, що хакери створювали підроблені сторінки входу для кожної установи та надсилали електронні листи науковцям-ядерникам, намагаючись змусити їх відкрити їхні паролі.

УКРАЇНА ВИЯВИЛАСЬ ГОТОВОЮ ДО КІБЕРВІЙНИ НЕ ЛИШЕ ЧЕРЕЗ НАДАНУ ДОПОМОГУ, АЛЕ І ЗАВДЯКИ КОНЦЕНТРАЦІЇ НА ЗАБЕЗПЕЧЕННІ СТІЙКОСТІ НАЙВАЖЛИВІШИХ ФУНКЦІЙ

Союзники України продовжують підбивати підсумки та вивчати уроки російсько-української кібервійни. У своїх виступах вони вказують на те, що фактор західної допомоги Україні дійсно став важливим чинником її готовності до кібератак.

Однак крім цього вдалою була ставка України на забезпечення стійкості найважливіших функцій – тобто розуміння, що навіть найсучасніші засоби захисту можуть підвести, а відтак треба бути готовими надавати основні послуги іншими шляхами.

При цьому деякі дослідники вказують на те, що Україна зараз більш адаптована до кіберпротистояння і нових викликів в кіберпросторі ніж США та її приватний сектор (особливо промисловий).

ДИРЕКТОРКА CISA: США ПОВИННІ БУТИ ПИЛЬНИМИ, «ТРИМАТИ ОБОРОНУ» ВІД РФ

5 січня, виступаючи під час дискусії в рамках CES2023 (найбільша щорічна виставка споживчої електроніки) в Лас Вегасі, директорка CISA Джен Істерлі зазначила, що, попри той факт, що від початку російського вторгнення в Україну, росія не здійснила значних атак на США, не можна вважати, що таких атак і не буде. На думку Істерлі, війна закінчиться не скоро, тому, необхідно залишатися пильними.

ТУРЛА: ГАЛАКТИКА МОЖЛИВОСТЕЙ

Звіт від Mandiant, опублікований 5 січня, стверджує, що російські хакери з угрупування Turla «причепом» використовували в Україні віруси, які інші хакери розповсюджували за допомогою USB. Компанія наголошує, що це перший випадок від початку російського вторгнення, коли Turla таргетує українців. Більш детально про механізми у звіті компанії за посиланням.

KILLNET ПІДДАВ DDOS-АТАКАМ НИЗКУ ІНФОРМАЦІЙНИХ РЕСУРСІВ У НІМЕЧЧИНІ

російське угрупування KillNet взяло на себе відповідальність за низку DDoS-атак проти вебсайтів німецьких аеропортів, органів державного управління та організацій фінансового сектора. Німецькі спеціальні органи (зокрема BSI) відзначають, що атаки не завдали шкоди функціональності чи наданню послуг, і загалом були досить швидко відбиті.

Угрупування закликало до атак як відповідь на заяву канцлера Олафа Шольца про те, що Німеччина надішле Україні танки Leopard 2, щоб допомогти відбити російське вторгнення.

ЗВЕРНЕННЯ ЗЕЛЕНСЬКОГО ПОКАЗАЛИ ПО ТЕЛЕБАЧЕННЮ В РОСІЇ ТА У КРИМУ

25 січня телевізійне звернення Президента Зеленського протягом певного часу транслювалось по телебаченню в окупованому Криму та у російському Бєлгороді. Влада Криму пояснила інцидент хакерською атакою, представники Бєлгородської області — «несанкціонованою заміною телесигналу».

ПОЛЬЩА ГОТУЄТЬСЯ ДО ЗРОСТАННЯ РОСІЙСЬКОЇ КІБЕРАКТИВНОСТІ У ЗВ'ЯЗКУ З РОСІЙСЬКО-УКРАЇНСЬКОЮ ВІЙНОЮ

Керівник наукового відділу Фонду Казимира Пуласького А. Козловський закликає владу Польщі активніше готуватись до російських кібератак, зважаючи на логістичну роль Польщі у постачанні зброї Україні.

Він вказує, що наявний досвід кібератак доводить необхідність вживати додаткові заходи, в т.ч. активніше залучати Кіберкомандування США до безпеки польських мереж, налагоджувати обмін інформацією з приватним сектором, бути готовими підвищити рівень попередження про кібербезпеку до найвищого рівня DELTA, що передбачатиме посилені заходи фізичної безпеки окремих установ і додаткових перевірок мереж.

ПИТАННЯ ЮРИДИЧНОГО СТАТУСУ ТА МАЙБУТНЬОГО IT-АРМІЇ БУДЕ ПОТРЕБУВАТИ ВИРІШЕННЯ – WIRED

У статті від 23 січня оглядач видання Wired Вікторія Бейнс підіймає питання щодо юридичного статусу учасників волонтерського об'єднання IT-Армія України. Вона підкреслює, що хоча в умовах протистояння це питання не буде підійматись, але досвід схожих традиційних конфліктів вказує на те, що не регулярні сили, які долучені до конфлікту мають проблеми із юридичним статусом та захистом після його завершення.

Щодо IT-Армії, то можуть виникнути питання до тих осіб, які брали участь у наступальних операціях (DDoS) або які матимуть бажання використати набуті знання хактивізму у злочинних цілях.

ЛАТВІЯ ПІДТВЕРДЖУЄ ФІШИНГОВУ АТАКУ НА МІНІСТЕРСТВО ОБОРОНИ, ПОВ'ЯЗУЮЧИ ЇЇ З РОСІЙСЬКОЮ ХАКЕРСЬКОЮ ГРУПОЮ

Російське кібершпигунське угруповання, відоме як Gamaredon, могло стояти за фішинговою атакою на Міністерство оборони Латвії минулого тижня, повідомили в міністерстві 27 січня виданню The Record. Хакери розіслали шкідливі листи кільком співробітникам міністерства, видаючи себе за українських урядовців. Спроба кібератаки була невдалою, додали в відомстві.

Дослідники приписують цю фішингову кампанію Gamaredon, оскільки хакери використовували той самий домен (admou[.]org), що й під час попередніх кібератак. Раніше у грудні компанія з кібербезпеки Unit 42 також пов'язала цей домен із Gamaredon.

РОСІЯ ВЕРБУВАЛА УКРАЇНСЬКИХ ДІТЕЙ ЧЕРЕЗ МОБІЛЬНУ ГРУ

8 січня Міністр оборони Олексій Резніков повідомив у Твіттері, спецслужби рф намагалися вербувати українських дітей, щоб ті несвідомо надавали інформацію про розташування стратегічно важливих об'єктів через мобільну гру.

ДІПФЕЙКИ ТА МІЖНАРОДНИЙ КОНФЛІКТ

Brookings оприлюднив дослідження щодо діп фейків та їх можливого використання у міжнародних конфліктах. Дослідники наголошують, що технологію вже намагалась використати у російсько-українській війні. Хоча цього разу нападники успіху не мали, технологія швидко розвивається, і, швидше за все, становитиме виклик для аналітиків та полісімейкерів у сфері національної безпеки з огляду на широкий спектр можливостей її використання.

Аналітики Brookings зазначають, що хоча сьогодні та можливо навчити алгоритм розпізнавати діп фейки, у довгостроковій перспективі таке рішення не буде працювати, адже будь-які технічні рішення, що допомагають визначити діп фейки зараз можуть бути включені у наступний алгоритм з їх створення.

Автори звіту також наголошують, що демократичним країнам час почати обговорювати етичні рамки застосування діп фейків у конфлікті та механізмів контролю над їх використанням. Одним з можливих рішень автори звіту вважають створення міжнародного договору на рівні ООН.

9. РІЗНЕ

РОЗВИТОК ДРОНІВ В УКРАЇНІ МОЖЕ ПРИНЕСТИ СВІТАНОК РОБОТІВ-ВБИВЦЬ

4 січня Associated Press написала, що в Україні вже є напівавтономні ударні безпілотники та протидронове озброєння, оснащене ШІ. росія також стверджує, що володіє зброєю з ШІ, хоча ці заяви є недоведеними. Але немає підтверджених випадків, коли держава використовувала в бою роботів, які вбивали б цілком самостійно.

Безпілотники вже можуть розпізнавати такі цілі, як бронетехніка, використовуючи каталогізовані зображення. Але існують розбіжності щодо того, чи достатньо надійна ця технологія, щоб гарантувати, що машини не помиляються і не заберуть життя тих, хто не воює.

Занепокоєння використанням автономної зброї у війні рф проти України висловила кампанія Stop Killer Robots, зокрема щодо використання KUB-BLA, який є «безпілотним боєприпасом (loitering munition)». Це фактично невеликий безпілотник, який може шукати й потім вибухати в призначену ціль. Боєприпаси можуть бути наведені на ціль оператором по відеозв'язку або бортовою «системою наведення на ціль».

КОЛИ РОБОТ МОЖЕ ВБИТИ? НОВА ПОЛІТИКА МІНІСТЕРСТВА ОБОРОНИ США НАМАГАЄТЬСЯ ПОЯСНИТИ

25 січня набирає чинності оновлена версія політики Сполучених Штатів щодо роботів-вбивць. Як пише видання Defense One, найбільшою зміною в новій версії доктрини Міністерства оборони від 2012 року щодо летальної автономної зброї є більш чітко сформульоване твердження, що її можна створювати та розгортати безпечно та етично, але не без значного нагляду.

IARPA РОЗРОБИТЬ НОВУ ПРОГРАМУ, БАЗОВАНУ НА ШІ, ЯКА АВТОМАТИЧНО ГЕНЕРУВАТИМЕ ПІДКАЗКИ ДЛЯ ПОКРАЩЕННЯ РОЗВІДУВАЛЬНИХ ЗВІТІВ

Видання Fedscoop повідомляє, що ключовий дослідницький центр розвідувальної спільноти США запускає нову програму для створення інструментів, які використовують останні досягнення в галузі ШІ, щоб допомогти аналітикам, яки працюють у розвідці, писати звіти з більш переконливими доказами та кращою аргументацією.

Інструмент, який планують назвати REASON, допомагатиме не стільки з мовою та стилістикою, скільки аналізувати фактичну інформацію, з якою працюють аналітики, та надаватиме рекомендації у разі, якщо автор(ка) звіту не звернув увагу на якусь важливу деталь, яка підкріплює, або послаблює його(її) висновки. А також оцінюватиме логічність аргументів.

ІНТЕРВ'Ю З GUCCIFER 1.0

Видання The Intercept взяло інтерв'ю у Guccifer 1.0 – хакера, якого російські оперативники підставили за вплив на президентські вибори в США у 2016 році. Румунський хакер Марсель Лехел Лазар провів понад 4 роки за ґратами та вперше розповів про своє життя після звільнення та про слід, який він залишив в історії США.

МИНУЛОГО РОКУ КІЛЬКІСТЬ ПРОПОЗИЦІЙ ФАЛЬШИВИХ БАНКНОТ У ДАРК ВЕБ ЗРОСЛА НА 91%

Як 27 січня повідомила Cybersixgill News, попри розмови про те, що готівкові гроші відмирають, чорний ринок фальшивих грошей процвітає. Минулого року кількість пропозицій зросла на 91%, а кількість унікальних продавців зросла на 82%. Таку тенденцію можна пояснити удосконаленням технологій друку, що робить виробництво фальшивих банкнот легким та не надто дорогим.