НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

УКРАЇНСЬКА ФУНДАЦІЯ БЕЗПЕКОВИХ СТУДІЙ

CYBER DIGEST.

Огляд подій в сфері кібербезпеки,
січень 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".

Думки автора, висловлені в цій публікації, не обов'язково відображають погляди Агентства США з міжнародного розвитку або Уряду США.

ЗМІСТ

ОСНОВНІ ТЕНДЕНЦІЇ

У фокусі уваги січня – вразливість Ivanti Connect Secure, яка стала інструментом для кібершпигунської активності китайського угрупування UNC5221. Ця вразливість нульового дня настільки потенційно небезпечна, що CISA видала з цього приводу термінову директиву, обов'язкову для всіх федеральних установ. З власним попередженням щодо цієї загрози виступив і британський Національний центр кібербезпеки. Активність китайської кібершпигунської групи вписується у ширший контекст занепокоєння західних країн щодо китайської активності. Наприклад – щодо масового збору вразливостей у ПЗ яке використовується в іноземних компаніях. CISA додатково звертає увагу власників OKI в США щодо обережного використання безпілотних летальних апаратів китайського виробництва та випустила настанову щодо недопущення витоків даних внаслідок цього.

США продовжує шукати ефективні шляхи захисту власних OKI, особливо у тих секторах, які зараз знаходяться під найбільшим тиском – охорона здоров'я та водопостачання. У сфері охорони здоров'я ситуація стає особливо гострою – атаки проти лікарень стали повсякденним явищем, так само як і викрадення даних пацієнтів. Зловмисники шукають все нові інструменти навіть не проведення атак, а змушення атакованих до виплати викупів (федеральна влада ставиться до цього процесу все менш лояльно) шантажуючи не лише атаковані організації, але і пацієнтів. Навіть приватні компанії (наприклад, Palo Alto Network) починають випускати настанови для закладів охорони здоров'я, а урядові структури готуються до запровадження обмежень щодо федерального фінансування для тих медзакладів, які не запровадили мінімальні вимоги кібербезпеки.

Після низки кібератак проти систем водопостачання та водовідведення у грудні 2023 року, організації, які за них відповідають, опинились у центрі уваги безпекових органів та законодавців. В США як на загальнодержавному, так і на місцевому рівні триває дискусія про те, як краще захистити більше ніж 50 тисяч організацій водопостачання, які наразі діють в США. Вже у середині січня CISA разом з партнерами опублікували Керівництво з реагування на інциденти для сектору систем водопостачання та водовідведення яке має допомогти організаціям, але власники таких кампаній кажуть, що у них часто взагалі відсутні ресурси на заходи кіберзахисту. Тим часом атаки на такі організації продовжуються – у січні була атакована Southern Water, компанія, що надає послуги водопостачання 2,5 мільйона споживачів і послуги водовідведення 4,7 мільйона клієнтів у південних регіонах Англії.

Хоча дискусія щодо масштабів впливу штучного інтелекту на сферу кібербезпеки триває, однак майже всі організації вказують на нього як елемент, що змінює ландшафт кібербезпеки. Злочинці готуються використовувати генеративний ШІ (GenAI) з метою узагальнення тих даних, які вони вже вкрали й, фактично, створити нові вектори атак чи можливостей для вимог викупу. Захисники шукають можливості ширше використати ШІ для аналізу кіберзагроз (водночас експерти вказують на певні концептуальні проблеми на цьому шляху, в тому числі пов'язані із масивами даних, на яких відбувається навчання ШІ). Національний центр кібербезпеки Великобританії вийшов із власною довгостроковою оцінкою того, як ШІ впливає на ситуацію – на їх думку ШІ збільшить обсяг і посилить вплив кібератак протягом наступних двох років.

Проблеми квантових обчислень та постквантового шифрування знову турбують безпекові структури. В тому числі як НАТО прийняло свою першу квантову стратегію, кібербезпекові органи європейських країн звертають увагу на необхідність приділити цьому питанню більше уваги й не відволікатися на підходи, які є сумнівними з поглиду ефективності. АНБО США починає відкриті дискусії щодо майбутнього квантових обчислень і як це вплине на сферу безпеки, а IBM вважає, що у 2024 році стане більше кібератак з метою крадіжки зашифрованих даних в надії отримати доступ до їх вмісту із появою квантових комп'ютерів.

Українські організації зазнали у січні декількох потужних кібератак – одна з них була спрямована на банківський центр, а інша помітно вплинула на один з найбільших дата-центрів України. Останнє призвело до порушення доступності послуг декількох державних організацій та інформаційних систем. Загалом це корелюється з підвищенням кіберактивності росії проти українських інформаційних систем – за даними Держспецзв'язку кількість кіберінцидентів минулого року зросла на 62,5%. Як відповідь, Україна завдає контрударів (як, наприклад, дії військової розвідки України проти одного з російських постачальників IT-систем для промисловості), а також активніше співпрацює з партнерами – Данія заявила про надання 12 мільйонів євро на кіберзахист України.

Західні дослідники вивчають досвід російських дій у кіберпросторі та надають власні прогнози та рекомендації. Видання CSO Online описує структуру та методи діяльності проросійської хактивістської групи NoName057(16) та стверджує, що така організація може стати моделлю для кіберзлочинців майбутнього. Разом з тим, видання підкреслює, що поки що діяльність угруповання, яке концентрується в першу чергу на DDoS атаках, не становить серйозної загрози заходу. Дослідниця Моніка Келло стверджує, що публічна ганьба та санкції, яких сьогодні вживають західні уряди, намагаючись впливати на дії рф у кіберпросторі, не є ефективними. На її думку, відповідь має ґрунтуватися на російській стратегічній культурі та включати прозорі розслідування наслідків російських операцій злому та витоків. А також використовувати недовіру, яка панує в російських спецслужбах і суспільстві, щоб внести «тертя» в операційне середовище супротивника.

У січні атак зазнали декілька кібербезпекових компанії та відділи кібербезпеки великих компаній. Серед них компанія Microsoft, яка стала жертвою атаки російського державного нападника Midnight Blizzard. В результаті атаки нападники отримали доступ до «дуже невеликого відсотка корпоративних облікових записів електронної пошти Microsoft, включаючи вище керівництво та співробітників служби кібербезпеки». На початку лютого жертвою нападників став акаунт фірми Mandiant в мережі X. Протягом недовгого часу зловмисники використовували його для популяризації оманливих операцій з криптовалютою. Поштові скриньки кібербезпекового відділу техгіганта HP Enterprise також стали жертвою атаки хакерів, пов'язаних із кремлем. Також російська кібербезпекова компанія Kasperski розкрила деталі атаки, якої зазнали телефони її співробітників.

У співпраці з CRDF Global НКЦК та Мінветеранів працюють над інтеграцією ветеранів до кіберробочої сили, проводячи для них комплексне навчання з кібербезпеки та кібероборони, а також надаючи підтримку у працевлаштуванні в державному або приватному секторі. Паралельно йде розбудова спроможності державного сектору до захисту та реагування на кібератаки. З одного боку, компанія Google у 2024 році надасть 5 тисяч ключів безпеки для захисту облікових записів українських урядовців та надасть їм необхідну підготовку для користування ключами. А з іншого – ДССЗЗІ проводить навчальні заходи для CDTO державних органів та відповідальних за кібербезпеку держслужбовців категорій «Б» і «В» з метою покращення їх співпраці з CERT-UA.

Національний координаційний центр кібербезпеки при РНБО України попередив про високий рівень кіберзагроз для підприємств сектору комунікацій. Основні кібербезпекові органи фіксують зростання кібератак на українську критичну інфраструктуру. Така тенденція відповідає глобальному розвитку ситуації. Очікується, що пік атак в Україні припаде на лютий 2024. Одночасно, інтенсифікується боротьба між Україною та рф у кіберпросторі. рф таргетує українських урядовців, військовослужбовців за допомогою фішингу та намагається посіяти паніку серед населення України. У ГУР МО України розповіли про успішні атаки на далекосхідний науково-дослідний центр космічної гідрометеорології, сервер спецзв'язку міністерства оборони росії, IT-інфраструктуру компанії IPL Consulting, яка спеціалізувалася на впровадженні інформаційних систем у російській промисловості.

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

ФЕДЕРАЛЬНА ТА МІСЦЕВА ВЛАДА США ЗАНЕПОКОЄНА КІБЕРБЕЗПЕКОЮ ПІДПРИЄМСТВ ВОДОПОСТАЧАННЯ ТА ВОДОВІДВЕДЕННЯ

2 січня оглядачі SecurityWeek за матеріалами Associated Press підготували детальний огляд дискусій на рівні федеральних відомств та урядів штатів навколо кіберзагроз, які спрямовані на підприємства водопостачання та водовідведення. Кібератака на кілька місцевих підприємств водопостачання поставили питання наскільки вони захищені від такого роду атак і чи немає загрози громадянам. Наразі в США функціонує понад 50 тисяч водопровідних підприємств і на абсолютній більшості з них є брак кіберфахівців. Деякі штати приймають локальне законодавство, яке висуває більш суворі вимоги до компаній в частині кібербезпеки, однак власники цих організацій вказують на те, що це призведе до більших видатків що може стати непосильним для невеликих організацій.

НАЦІОНАЛЬНА КІБЕРНЕТИЧНА МІСІЯ США ОТРИМАЛА НОВУ ОЧІЛЬНИЦЮ

5 січня Генерал-майор Корпусу морської піхоти Лорна Мехлок прийняла командування Силами кібернаціональної місії (CNMF) під час церемонії зміни командування у Форт-Міді, штат Меріленд. Вона змінила генерал-майора армії Вільяма Хартмана, який очолював сили з 2019 року, а минулого місяця був затверджений новим заступником начальника Кіберкомандування.

США ПЛАНУЄ ЗМІНИТИ ПРАВИЛА ОТРИМАННЯ ДЛЯ ФІНАНСУВАННЯ ЛІКАРЕНЬ: НІЯКИХ КОШТІВ БЕЗ ДОТРИМАННЯ ОСНОВНИХ СТАНДАРТІВ КІБЕРБЕЗПЕКИ

10 січня стало відомо, що Центр медичної допомоги та медичних послуг (CMS), підрозділу Міністерства охорони здоров'я та соціальних служб США, розробляє правила, що пов'язують IT-безпеку лікарень із фінансуванням. Ці правила мають набути чинності до кінця року. Запропоновані правила будуть зосереджені на ключових практиках кібербезпеки, які, на думку представників Мінохорони здоров'я мають значний вплив на безпеку організацій. І федеральне фінансування залежатиме від лікарень, які запровадять ці основні засоби захисту у своїх мережах.

CISA ПРОЗВІТУВАЛА ПРО СВОЇ ДОСЯГНЕННЯ У 2023 РОЦІ

17 січня CISA опублікувала річний звіт про свою діяльність та зусилля щодо захисту критичної інфраструктури. Серед ключових досягнень, які підкреслюються у звіті: просування secure by design; публікація Дорожньої карти щодо ШІ; запуск Ініціативи попереднього сповіщення про програмне забезпечення-вимагач; заохочення кібергігієни; розширення взаємодії з КІ (понад 6700 взаємодій щодо обміну інформацією та для просування послуг з кібербезпеки); покращення екстреного (урядового) зв'язку; запуск Програми грантів з кібербезпеки для місцевого та загальнодержавного рівня; посилення безпеки виборчого процесу; покращення безпеки хімічних об'єктів.

БРИТАНСЬКИЙ НЦК РОЗПОЧАВ НОВУ ІНІЦІАТИВУ ДЛЯ СПІВПРАЦІ З ВОЛОНТЕРАМИ-КІБЕРЕКСПЕРТАМИ – КІБЕРЛІГА

17 січня британський НЦК розпочав нову ініціативу – Кіберлігу. Її метою є залучення до питань кіберзахисту різноманітні групи експертів галузі, які працюють з аналітиками НЦК та один з одним, аби дати ліпше розуміння картини загроз. Учасники Кіберліги будуть залучатись до різноманітних заходів, включаючи аналітичні семінари та дискусійні групи. Кіберліга створена також як доповнення до іншої ініціативи – Industry 100, підходу, за якого співробітники приватних компаній можуть бути направлені з відрядженням для роботи в НЦК.

В США АКТИВІЗУВАЛАСЬ ДИСКУСІЯ ЩОДО МАЙБУТНЬОГО РАДИ З ОГЛЯДУ КІБЕРБЕЗПЕКИ (CSRB)

17 січня у Сенаті США відбулися дискусії про те, як можна покращити роботу CSRB. Раду було створено у 2021 році наказом президента США. Раді доручено розслідувати деякі з найгостріших проблем кібербезпеки, з якими зіштовхується США, але наразі підготовлено лише два звіти: один про Log4J, а інший – про групу LAPSUS$. Представники кібербезпекової сфери висловлюються за більшу незалежність цього органу, перегляд поточного його складу (а також прозорішої процедури обрання її членів), а також створення запобіжників від можливого конфлікту інтересів між учасниками Ради та інцидентами, які вони розслідують. Ключову роль у формування ради наразі відіграє CISA, директор якої призначає її членів відповідно до затвердженого порядку.

CISA ВИДАЛА НАДЗВИЧАЙНУ ДИРЕКТИВУ ДЛЯ ФЕДЕРАЛЬНИХ ВІДОМСТВ ЩОДО НЕГАЙНИХ ЗАХОДІВ ПРОТИ ВРАЗЛИВОСТЕЙ В IVANTI CONNECT SECURE І POLICY SECURE

19 січня CISA випустила Надзвичайну директиву 24-01 за результатами спостереження за широким та активним використанням вразливостей в пристроях Ivanti Connect Secure та Ivanti Policy Secure зловмисними кіберзагрозами. Директива наказує негайно вжити конкретних заходів безпеки та застосувати вказівки постачальників щодо пом'якшення наслідків для цих пристроїв Ivanti. Директива є обов'язковою лише для федеральних цивільних органів виконавчої влади, однак CISA закликає всі організації, які використовують ці продукти, терміново запровадити пом'якшення, викладені в Директиві.

АВСТРАЛІЯ НАКЛАЛА САНКЦІЇ НА РОСІЙСЬКОГО ЗЛОВМИСНИКА ВІДПОВІДАЛЬНОГО ЗА АТАКУ НА MEDIBANK PRIVATE

23 січня Уряд Австралії вперше застосував режим санкцій за «значні кіберінциденти», який він запровадив у 2021 році, проти росіянина, на ім'я Олександр Єрмаков, якого влада визнала відповідальним за атаку на медичну страхову компанію Medibank Private у 2022 році. Ймовірним виконавцем нападу було назване злочинне угруповання REvil, а влада Австралії звинуватила росію в приховуванні угруповання. Інцидент 2022 року став причиною витоку даних про 9,7 мільйона клієнтів – було викрадено імена, дати народження, адреси, номери телефонів і адреси електронної пошти.

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

CES 2024: АДМІНІСТРАЦІЯ БАЙДЕНА ОГОЛОШУЄ ПРО УГОДУ З ЄС ЩОДО CYBER TRUST MARK

11 січня заступниця радника Білого дому з національної безпеки з питань кібернетичних і нових технологій Енн Нойбергер повідомила, що Сполучені Штати уклали угоду з Європейським Союзом про «спільну дорожню карту» для стандартизованих міток кібербезпеки. Нойбергер сказала, що Білий дім прагне отримати свою добровільну сертифікацію для пристроїв Інтернету речей на споживчі товари U.S. Cyber Trust Mark до кінця року. В результаті появи такого маркування пристрої для інтернету речей вироблені в США або ЄС можна буде продавати на обох ринках без додаткового тестування.

НАТО ОПРИЛЮДНИЛО ПЕРШУ У СВОЇЙ ІСТОРІЇ КВАНТОВУ СТРАТЕГІЮ

Саму Стратегію ще 28 листопада 2023 року схвалили міністри закордонних справ НАТО, але 17 січня було опубліковано її ключові ідеї. Квантова стратегія НАТО має допомогти організації спрямовувати співпрацю НАТО з промисловістю для розвитку трансатлантичної екосистеми квантових технологій, одночасно готуючи НАТО до захисту від зловмисного використання квантових технологій. Ґрунтуючись на своїй новій стратегії, НАТО розпочинає роботу зі створення Трансатлантичної квантової спільноти для взаємодії між урядами, промисловістю та академічними колами з усіх інноваційних екосистем.

ПОНАД СОТНЯ НЕУРЯДОВИХ ОРГАНІЗАЦІЙ ЗАСТЕРІГАЄ ВІД ПРИЙНЯТТЯ КОНВЕНЦІЇ ПРО КІБЕРЗЛОЧИННІСТЬ В ПОТОЧНІЙ РЕДАКЦІЇ

23 січня понад 100 неурядових організацій оприлюднили свій заклик до членів ООН, щоб запропонована наразі Конвенція про кіберзлочинність була вузько зосереджена на боротьбі з кіберзлочинністю, а не використовувалася як інструмент підриву прав людини. А за відсутності суттєвих змін для усунення цих недоліків, Конвенцію пропонують відхилити. На їх думку документ залишається надто широким щодо діапазону свого застосування, не містить формулювання, достатнього для захисту дослідників безпеки, дозволяє надлишковий обмін інформацією для співпраці з правоохоронними органами, виходячи за межі конкретних кримінальних розслідувань і без конкретних чітких гарантій захисту даних і прав людини.

ANSSI, BSI РАЗОМ З НІДЕРЛАНДСЬКИМИ ТА ШВЕЦЬКИМИ ПАРТНЕРАМИ ОПУБЛІКУВАЛИ СПІЛЬНИЙ ПОЗИЦІЙНИЙ ДОКУМЕНТ ЩОДО КВАНТОВОГО РОЗПОДІЛУ КЛЮЧІВ (QKD)

25 січня ANSSI та його партнери з Федерального управління інформаційної безпеки (BSI), Національного агентства безпеки зв'язку Нідерландів (NLNCSA) і Національне управління безпеки зв'язку Швеції, опублікували технічний підсумковий документ щодо квантового розподілу ключів (QKD). Публікація має на меті допомогти особам, які приймають рішення, і політичним лідерам прийняти обґрунтовані рішення в контексті створення середовища, захищеного від квантових атак. Основна ідея матеріалу полягає у тому, що наразі QKD не може використовуватись як замінник традиційним криптографічним практикам чи переходу на постквантову криптографію (PQC).

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

«HOMELAND JUSTICE» АТАКУЄ АЛБАНСЬКІ ОРГАНІЗАЦІЇ ЗА ДОПОМОГОЮ ВАЙПЕРА

На початку січня дослідники компанії ClearSky опублікували звіт, який описує атаку віруса-вайпера, яка наприкінці грудня 2023 року вразила вебсайти, що належать уряду Албанії та інфраструктурним організаціям. ClearSky приписує атаку іранському актору загрози «Homeland Justice», який атакує Албанію з літа 2022 року. Атакувальники стверджують, що знищують тих, хто «підтримує тероризм».

ХАКЕРИ ЗЛАМАЛИ БАЗУ ДАНИХ СУДОВИХ ЗАСІДАНЬ АВСТРАЛІЇ

2 січня the Record Media повідомило, що судова система другого за чисельністю населення штату Австралії постраждала від атаки програм-вимагачів, в процесі якої, вірогідно, було викрадено конфіденційні записи деяких судових засідань.

Court Services Victoria (CSV) – адміністративний орган, який підтримує роботу суддів у штаті Вікторія – виявив атаку 21 грудня 2023 року. Інцидент призвів до збою аудіовізуальної технологічної мережі в суді, що вплинуло на відеозаписи, аудіозаписи та послуги транскрипції, за словами генерального директора CSV Луїзи Андерсон. Хакери, яких CSV не ідентифікував, залишили записку про викуп, погрожуючи опублікувати файли, викрадені з судової системи.

АКАУНТ КОМПАНІЇ MANDIANT НА ПЛАТФОРМІ X БУЛО ЗЛАМАНО ДЛЯ ПРОСУВАННЯ ОМАНЛИВИХ ОПЕРАЦІЙ З КРИПТОВАЛЮТАМИ

3 січня видання BleepingComputer повідомило, що акаунт компанії Mandiant, що є дочірньою компанією Google в системі X, напередодні було зламано, і за його допомогою просували оманливі операції з криптовалютами. Хакер змінив ім'я користувача акаунту на phantomsolw і поширював посилання на вебсайт, який автоматично очищав гаманці користувачів від криптовалюти, видаючи себе за сайт Phantom. Система Phantom визначила цей сайт як зловмисний, а Mandiant відновила контроль над акаунтом протягом шести годин.

КІБЕРЗЛОЧИНЦІ ВПРОВАДИЛИ ШТУЧНИЙ ІНТЕЛЕКТ (ШІ) ДЛЯ ОБМАНУ З ВИКОРИСТАННЯМ ФАЛЬШИВИХ РАХУНКІВ

3 січня, компанія Resecurity, яка відстежує кіберзлочинне угруповання GXC Team, яке розробляє та продає інструменти для крадіжки коштів в онлайн-банкінгу та атак соціальної інженерії, опублікувала звіт. У ньому йдеться, що у листопаді минулого року угруповання почало продавати інструмент, який використовує штучний інтелект для створення фальшивих рахунків для використання в атаках бізнес-електронною поштою. Ці рахунки можуть перехоплювати бізнес-транзакції, замінюючи банківську інформацію в легітимних рахунках. Цей інструмент є останнім у широкому спектрі платформ соціальної інженерії, розроблених цим угрупованням.

ТРАНСПОРТНИЙ ГІГАНТ ESTES ВІДМОВЛЯЄТЬСЯ ВИКОНУВАТИ ВИМОГИ ВИМАГАЧІВ ТА ПОВІДОМЛЯЄ, ЩО БУЛИ ВИКРАДЕНІ ОСОБИСТІ ДАНІ

3 січня один із найбільших американських приватних вантажовідправників Estes Express Lines повідомив понад 20 тисяч клієнтів про те, що злочинці вкрали їхню особисту інформацію. Атаку на свою мережу компанія виявила на початку жовтня минулого року. Згідно зі стандартною рекомендацією ФБР і фінансових регуляторів, Estes відмовилася платити викуп. Компанія не пояснила мотивацію такого рішення. Estes стверджує, що «їй не відомо про будь-яку крадіжку ідентичності, шахрайство або фінансові втрати (для її клієнтів – ред.) в результаті цього інциденту». Компанія також оплатить постраждалим особам 12 місяців послуг з моніторингу особистих даних від компанії Kroll.

ЗЛОВМИСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ВИКОРИСТОВУЄ ЕКСПЛОЙТ GOOGLE MULTILOGIN ДЛЯ ПІДТРИМКИ ДОСТУПУ, ПОПРИ СКИДАННЯ ПАРОЛЯ

Як 3 січня повідомило видання The Hacker News з посиланням на звіт компанії CloudSEK, зловмисне ПЗ, що викрадає інформацію, активно використовує незадокументовану кінцеву точку Google OAuth під назвою MultiLogin, щоб захоплювати сеанси користувачів і зберігати постійний доступ до служб Google навіть після скидання пароля. Згідно з CloudSEK, критичний експлойт полегшує збереження сеансу та створення файлів cookie, дозволяючи суб'єктам загрози підтримувати доступ до дійсного сеансу несанкціонованим способом.

ЄВРОПЕЙСЬКИЙ ЦЕНТРАЛЬНИЙ БАНК ПІДДАСТЬ БАНКИ КІБЕР-СТРЕС-ТЕСТУ

Починаючи з січня, Європейський центральний банк проведе кібер-стрес-тести банків, щоб визначити їхню стійкість до кібератак. ЦБ вимагає від 109 банків у Європі провести оцінку вразливості та реагування на інциденти до середини 2024 року.

У кожному тесті банківський регулятор моделюватиме руйнівну кібератаку, здатну негативно вплинути на бізнес-операції. Тоді він відстежуватиме, як фінансова установа реагує на атаку та відновлюється після атаки, а також наскільки швидко вона відновлює надання послуг клієнтам.

ДОКУМЕНТИ ВПС ШВЕЙЦАРІЇ ЗЛИТО У ВІДКРИТИЙ ДОСТУП ЧЕРЕЗ КІБЕРАТАКУ НА ТРЕТЮ СТОРОНУ

6 січня Військово-повітряні сили Швейцарії повідомили про серйозний виток даних, спричинений компрометацією постачальника – американської охоронної компанії Ultra Intelligence & Communications.

Відповідальність за злам взяла на себе хакерська група ALPHV, опублікувавши дані після того, як їх вимога про викуп була відхилена. Зловмисники отримали доступ і злили близько 30 гігабайтів конфіденційних документів, включаючи секретну інформацію та контракти з Міністерством оборони Швейцарії та оборонним підрядником RUAG. Витік викликає занепокоєння через конфіденційність військових і розвідувальних даних.

ВИПУЩЕНО БЕЗКОШТОВНИЙ ДЕШИФРАТОР ДЛЯ ЖЕРТВ ПРОГРАМ-ВИМАГАЧІВ BLACK BASTA ТА BABUK'S TORTILLA

10 січня Cisco Talos випустила дешифратор для варіанту Tortilla вимагача Babuk, що дозволяє жертвам, на які потрапило зловмисне ПЗ, відновити доступ до своїх файлів. Компанія заявила, що дані про загрози, якими вони поділилися з правоохоронними органами Нідерландів, дозволили заарештувати зловмисника, який стоїть за операціями зловмисного ПЗ.

БРИТАНСЬКИЙ НЦК ПОПЕРЕДЖАЄ КОМПАНІЇ ПРО ЗАГРОЗУ ВІД ВРАЗЛИВОСТЕЙ В IVANTI CONNECT SECURE І POLICY SECURE

11 січня НЦК Великобританії надав термінові рекомендації британським компаніям як захиститись від вразливостей, виявлених в Ivanti Connect Secure і Policy Secure. Наразі мова йде про дві серйозні вразливості:

- CVE-2023-46085 – вразливість обходу аутентифікації у вебкомпоненті ICS (9.x, 22.x) і IPS, яка дозволяє віддаленому зловмиснику отримати доступ до обмежених ресурсів, минаючи контрольні перевірки.
- CVE-2024-21887 – вразливість впровадження команд у вебкомпоненти ICS (9.x, 22.x) і IPS, яка дозволяє автентифікованому адміністратору надсилати спеціально створені запити та виконувати довільні команди на пристрої.

Якщо CVE-2024-21887 використовується в поєднанні з CVE-2023-46805, експлуатація не потребує автентифікації та дає змогу загрозливій особі створювати зловмисні запити та виконувати довільні команди в системі.

КИТАЙСЬКА UNC5221 АКТИВНО ВИКОРИСТОВУЄ ВРАЗЛИВІСТЬ В IVANTI

13 січня кібербезпекова компанія Mandiant повідомила, що відстежує підвищену активність китайського угрупування UNC5221 з використання вразливість в серверному пристрої VPN Ivanti. Станом на середину січня було відомо про щонайменше 20 організацій, які постраждали від використання цієї вразливості. Наразі недостатньо даних як саме зловмисники використовують вразливість крім повідомлень про те, що ця хакерська група намагалась закріпитись в уражених системах.

CISA ТА ФБР ВИПУСТИЛИ ІНСТРУКЦІЇ З КІБЕРБЕЗПЕКИ ДЛЯ ОКІ, ЯКІ ВИКОРИСТОВУЮТЬ БЕЗПІЛОТНІ СИСТЕМИ КИТАЙСЬКОГО ВИРОБНИЦТВА

17 січня фахівці CISA та ФБР підготували та оприлюднили інструкції для власників OKI, які використовують у своїй діяльності безпілотні системи вироблені в КНР. Автори інструкцій вказують, що через особливості законодавства КНР дані OKI можуть опинитись під загрозою. Інструкції містять набір підходів, вжиття яких призведе до зменшення таких ризиків.

НОВИЙ ХАКЕРСЬКИЙ ЗАСІБ ПЕРЕТВОРЮЄ ЕКРАН ТЕЛЕФОНУ НА ПРИХОВАНУ ШПИГУНСЬКУ КАМЕРУ

Як 19 січня повідомило видання Forbes з посиланням на дослідження в Science Advances, дослідники з Лабораторії комп'ютерних наук і штучного інтелекту Массачусетського технологічного інституту показали, як хакери можуть перетворити смартфон на пристрій для шпигунства. Датчики світла, які використовуються для регулювання яскравості екрана, здатні приховано фіксувати взаємодію користувача завдяки нещодавно розробленому алгоритму обчислювального зображення. Поєднавши екран дисплея смартфона з датчиком навколишнього освітлення, дослідники зрозуміли, що знімати зображення перед цим екраном можна без використання камери пристрою. Програми можуть використовувати датчики освітлення без необхідності запитувати дозвіл у користувача. Відсутність контролю за дозволом не дивує, адже такі датчики не вважалися ризиком для конфіденційності чи безпеки.

AERCAP БУЛО АТАКОВАНО RANSOMWARE

22 січня найбільший у світі орендодавець літаків AerCap Holdings заявив, що постраждав від інциденту кібербезпеки, пов'язаного з програмами-вимагачами, йдеться в заяві компанії. Однак компанія зберігає повний контроль над IT-системами. Водночас компанія намагається оцінити ступінь впливу кібератаки на його дані.

У США ЗАСУДИЛИ ДО П'ЯТИ РОКІВ УВ'ЯЗНЕННЯ РОСІЯНИНА, ЯКИЙ РОЗРОБИВ ВІРУС TRICKBOT

25 січня стало відомо, що колишнього розробника Trickbot Володимира Дунаєва відправили на п'ять років і чотири місяці до в'язниці за його участь у зараженні американських лікарень і підприємств ransomware Trickbot, що коштувало жертвам збитків у десятки мільйонів доларів. За даними Національного агентства зі злочинності Великобританії, банда виманила щонайменше 180 мільйонів доларів США (145 мільйонів фунтів стерлінгів) у людей і організацій по всьому світу. У 2021 році Дунаєва екстрадували до Америки з Південної Кореї.

КІБЕРШПИГУНСЬКА КАМПАНІЯ SEA TURTLE НАЦІЛЕНА НА ГОЛЛАНДСЬКІ IT ТА ТЕЛЕКОМУНІКАЦІЙНІ КОМПАНІЇ

Телекомунікаційні, медіа, інтернет-провайдери (ISP), постачальники послуг інформаційних технологій (IT) і курдські вебсайти в Нідерландах стали мішенню в рамках нової кампанії кібершпигунства, яку організував загрозливий агент, пов'язаний з Туреччиною, відомий як Sea Turtle.

Sea Turtle, також відомий під іменами Cosmic Wolf, Marbled Dust (раніше Silicon), Teal Kurma та UNC1326, була вперше задокументована Cisco Talos у квітні 2019 року з детальним описом спонсорованих державою атак на державні та приватні організації на Близькому Сході та Північній Європі та Африці.

ХАКЕРИ З КНДР ВИКРАЛИ КРИПТОВАЛЮТУ НА 600 МІЛЬЙОНІВ ДОЛАРІВ У 2023 РОЦІ

На початку січня аналітична компанія TRM Labs заявила, що КНДР «була відповідальною за майже третину всіх коштів, викрадених під час криптоатак минулого року, попри 30% скорочення в порівнянні з сумою у 850 мільйонів доларів США, яку було викрадено у 2022 році». «Зломи, вчинені КНДР, були в середньому в десять разів більш збитковими, ніж ті, які не пов'язані з Північною Кореєю», заявили в компанії.

АТАКА ПРОГРАМИ-ВИМАГАЧА ВПЛИВАЄ НА ПОСЛУГИ TIETOEVRY ДЛЯ ДЕЯКИХ КЛІЄНТІВ У ШВЕЦІЇ

Один із кількох дата-центрів Tietoevry у Швеції частково піддався атаці програм-вимагачів у ніч з 19 на 20 січня. Після атаки Tietoevry негайно ізолював уражену платформу, і атака не вплинула на інші частини інфраструктури компанії. Попри те, що загалом надання послуг поступово відновлювалося, послуги для клієнтів, яких зачепила атака, залишаються недоступними.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

ХАКЕРИ ШУКАЮТЬ НОВІ ШЛЯХИ ПРИМУСИТИ ЖЕРТВИ ПЛАТИТИ ВИКУП. Є РИЗИК, ЩО ЦЕ ПРИЗВЕДЕ ДО ФІЗИЧНОГО НАСИЛЛЯ

5 січня оглядач the Register у своїй статті описує поступову негативну зміну у поведінці хакерських груп, що займаються ransomware. Якщо на певних етапах зловмисники брали односторонні зобов'язання не атакувати заклади охорони здоров'я, то тепер це стало їх постійною тактикою. Занепокоєння викликає те, що вони не просто вимагають викуп, але тиснуть на власників медзакладів різними шляхами, намагаючись змусити їх до дій. Серед таких додаткових методів тиску: погрози пацієнтам лікарень (наприклад, оприлюднити їх персональні дані чи продати їх в Dark Web), тиск на родичів керівників медзакладів. Є занепокоєння, що на певному етапі загальні погрози можуть призвести до фізичного насильства як методу примушування. Цьому сприяють величезні суми викупів, які злочинці можуть отримати внаслідок використання ransomware.

ШТУЧНИЙ ІНТЕЛЕКТ ТА ЯДЕРНА СТАБІЛЬНІСТЬ

16 січня, War on the Rocks опублікував статтю, у якій обговорюються проблеми та можливості, пов'язані з інтеграцією ШІ у системи ядерного командування та управління. Автор наголошує на потенційних глобальних наслідках, неналежного використання ШІ у ядерних операціях, але також підкреслює потенційні переваги, такі як краще раннє попередження та виявлення за умови правильного впровадження ШІ. Підкреслюється необхідність міжнародних угод з іншими ядерними державами для пом'якшення ризиків, пов'язаних із ШІ в ядерних системах.

У статті йдеться про те, що американським військовим необхідно розробити вказівки для забезпечення ефективного прийняття рішень людиною, враховуючи обмеження автоматизації та потенційну упередженість автоматизації. Обговорюється занепокоєння, що його викликають системи «мертвої руки» та розміщенням ядерної зброї на безпілотних засобах, таких як повітряні безпілотники та автономні підводні апарати.

У висновку підкреслюється важливість продуманих і зважених підходів ядерних держав, які виступають за міжнародне співробітництво для встановлення відповідальних обмежень для ШІ в ядерних операціях і побудови більш безпечного та стабільного майбутнього.

ФРАНЦУЗЬКА ANSSI ПУБЛІКУЄ ПАКЕТ НАСТАНОВ ДЛЯ ВІДНОВЛЕННЯ ПІСЛЯ КІБЕРІНЦИДЕНТІВ

17 січня французька ANSSI опублікувала збірник з трьох настанов (стратегічного, тактичного та оперативного рівня), які організації можуть використовувати для відновлення після кіберінцидентів. Посібники розроблено разом з представниками приватного сектору і враховують їх коментарі та пропозиції.

ЯК КОМПАНІЯ OPENAI, ЩО ЗРОБИЛА CHATGPT, ПЛАНУЄ ЗАПОБІГТИ ДЕЗІНФОРМАЦІЇ ПРО ВИБОРИ У 2024 РОЦІ

17 січня видання Security Week повідомило, що OpenAI окреслив заходи для запобігання використанню своїх генеративних інструментів ШІ, таких як ChatGPT і DALL-E, для поширення дезінформації про вибори. Ці кроки включають заборону створення чат-ботів, які видають себе за реальних кандидатів або уряди, запобігання зловживанню технологією для політичної реклами чи лобіювання, доки не будуть проведені подальші дослідження її переконливої сили, а також додавання цифрових водяних знаків до зображень ШІ для ідентифікації їх походження. OpenAI також співпрацює з Національною асоціацією державних секретарів (National Association of Secretaries of State), щоб спрямовувати користувачів, які шукають інформацію про голосування, на непартійний вебсайт. Цей крок компанії розглядається як позитивний, але ще належить побачити, наскільки добре заходи будуть реалізовані та забезпечені.

NIST ПРОПОНУЄ НОВІ НАСТАНОВИ ЩОДО ВИМІРЮВАННЯ ТА ВДОСКОНАЛЕННЯ ПРОГРАМИ КІБЕРБЕЗПЕКИ ОРГАНІЗАЦІЇ

17 січня NIST опублікувала проєкт NIST Special Publication (SP) 800-55 Revision 2: Measurement Guide for Information Security, який надає вказівки щодо розробки ефективної програми вимірюваних заходів інформаційної безпеки. Мета публікації – допомогти керівникам підрозділів інформаційної та кібербезпеки спростити процес вимірювання прогресу їх підрозділу і допомогти представити результати керівництву компанії та споживачам за допомогою значущих числових деталей. Документ повністю узгоджений із NIST's Cybersecurity Framework та Risk Management Framework. Фактично документ має допомогти організаціям перейти від загальних заяв про визначення та врахування рівня ризику до більш узгодженої картини, заснованої на надійних даних.

ЕКСПЕРТИ CISA ЗАКЛИКАЮТЬ ДО ЗМІН В ОСВІТІ ПРОГРАМІСТІВ – КІБЕРБЕЗПЕКА МАЄ ПЕРЕСТАТИ БУТИ ФАКУЛЬТАТИВНОЮ ДИСЦИПЛІНОЮ

24 січня старший технічний радник CISA Джек Кейбл у своєму дописі на сайті CISA підкреслив, що шлях покладання кібербезпеки лише на кібербезпекових фахівців ніколи не дасть потрібного безпекового ефекту. На його думку, ключова зміна, яка має відбутись в освіті – при навчанні програмістів кібербезпека має перестати бути факультативною, не обов'язковою дисципліною. Він вказує на декілька проблем, чому така ситуація зберігається:

- безпека є вибірковим предметом;
- університети мають обмежені ресурси;
- викладачі не мають відповідного досвіду;
- галузь не висуває потреби в таких знаннях.

PALOALTO NETWORK ОПУБЛІКУВАЛА ПОСІБНИК З КІБЕРБЕЗПЕКИ ДЛЯ ЦИФРОВИХ ТРАНСФОРМАЦІЙ В СЕКТОРІ ОХОРОНИ ЗДОРОВ'Я

26 січня фахівці PaloAlto Network оприлюднили Посібник, що має допомогти CISO закладів охорони здоров'я ефективно вбудувати політики кіберзахисту у процеси цифрової трансформації їх організацій. Посібник звертає особливу увагу на три проблеми, з якими стикаються зараз заклади охорони здоров'я: зростання обсягів дистанційної допомоги (а отже і зростанні поверхні кіберзагроз), збільшення кількості підключених пристроїв (як IT пристроїв персоналу, так і різноманітного спеціального обладнання на кшталт МРТ), а також застаріле обладнання у персоналу, яке вже неможливо ефективно захищати від кіберзагроз.

У СФЕРІ КВАНТОВИХ ОБЧИСЛЕНЬ ПОЧИНАЄТЬСЯ БОРОТЬБА З ЇЇ НАЙБІЛЬШОЮ ПРОБЛЕМОЮ: ШУМОМ

Як пише видання MIT Technology Review, попри перспективний потенціал, ландшафт квантових обчислень сповнений як обіцянок, так і хайпу. Здатність використовувати квантові можливості залежить від подолання таких проблем, як шумові перешкоди, які становлять загрозу для делікатних квантових систем. Проте нещодавні прориви в теоретичній та експериментальній сферах свідчать про те, що прогрес урозв'язанні проблем, пов'язаних із шумом, може бути не за горами. Серед напрацьованих підходів – придушення помилок, пом'якшення помилок і квантова корекція помилок (QEC), що стає приводом для нового оптимізму і прокладає шлях для більш надійних квантових обчислень.

РЕГУЛЮВАННЯ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ ТА КІБЕРБЕЗПЕКА: ГЛОБАЛЬНИЙ ПОГЛЯД НА ФОРМУВАННЯ ПОЛІТИКИ

Оскільки організації та окремі особи довіряють цифровим системам все більше конфіденційних даних, питання належних заходів кібербезпеки ніколи не було настільки нагальним. Регуляторні дії щодо технологій штучного інтелекту, які вживають сьогодні уряди та організації, закладуть основу, яка визначатиме, хто отримуватиме більше вигоди від нових можливостей – зловмисники чи захисники. Попри те, що штучний інтелект і кібербезпека є наскрізними та глобальними проблемами, розробка цих принципів і рамок управління також повинна враховувати місцеві історичні, культурні та політичні контексти.

У своїй першій публікації Глобальна група з кібербезпеки Інституту Аспена описує низку поточних заходів із розробки політики в цій сфері та надає рекомендації та застереження для урядів, які слід враховувати, коли вони борються з ризиками та можливостями генеративного ШІ для кібербезпеки.

5. КРИТИЧНА ІНФРАСТРУКТУРА

КАМПАНІЯ ASYNCRAT СПРЯМОВАНА НА ІНФРАСТРУКТУРУ США

5 січня AT&T Alien Labs повідомила, що виявила кампанію з доставлення AsyncRAT на комп'ютері нічого не підозрюючих жертв. Протягом принаймні 11 місяців цей загрозливий актор працював над доставленням RAT через початковий файл JavaScript, вбудований у фішингову сторінку. Жертви та їхні компанії ретельно відбираються, щоб розширити вплив кампанії. Деякі з визначених цілей керують ключовою інфраструктурою в США. AsyncRAT – це інструмент віддаленого доступу з відкритим кодом, випущений у 2019 році та все ще доступний на Github.

УРАЗЛИВОСТІ У BOSCH NUTRUNNER МОЖУТЬ СПРИЯТИ ХАКЕРСЬКИМ АТАКАМ НА АВТОМОБІЛЬНІ ВИРОБНИЧІ ЛІНІЇ

9 січня фірма з кібербезпеки OT Nozomi Networks, повідомила про виявлення вразливостей у продукті Bosch Rexroth NXA015S-36V-B – акумуляторному ручному пневматичному динамометричному ключі, призначеному для важливих для безпеки операцій затягування. Використання вразливостей може дозволити зловмисникам отримати повний контроль над цим ключем. Лабораторні випробування, проведені компанією з кібербезпеки, продемонстрували, як зловмисник може запустити атаку програмного забезпечення-вимагача, яка передбачає виведення пристрою з ладу та відображення повідомлення про викуп на його вбудованому екрані. Що ще гірше, таку атаку можна автоматизувати, щоб зламати всі динамометричні ключі компанії, викликаючи значні збої у виробничій лінії.

АНАЛІЗ КІБЕРАТАК НА ЕНЕРГЕТИЧНУ ІНФРАСТРУКТУРУ ДАНІЇ ТА УКРАЇНИ

11 січня компанія Forescout опублікував аналіз двох хвиль кібератак, які вразили енергетичний сектор Данії у травні 2023 року. Компанія спростовує висновки данського CERT критичної інфраструктури, SektorCERT, який приписав інциденти російській загрозі Sandworm. У звіті також досліджено дві аварійні події на українській підстанції в середині жовтня 2022 року.

RAPID SCADA МАЄ ВРАЗЛИВОСТІ, ЯКІ НАРАЖАЮТЬ ПРОМИСЛОВІ ОРГАНІЗАЦІЇ НА КІБЕРАТАКИ

11 січня CISA опублікувало консультацію, щоб повідомити промисловим організаціям про сім вразливостей, виявлених дослідниками Claroty в Rapid SCADA. Одну з вад було класифіковано як «критичну», а дві – як «високої серйозності», але розробники ще не випустили виправлень, попри те, що вони були повідомлені про них ще на початку липня 2023 року. Деякі з вразливостей можуть бути використані зловмисниками для віддаленого виконання коду, і існує кілька десятків екземплярів Rapid SCADA, до яких можна отримати прямий доступ з Інтернету, що робить організації вразливими до атак. Rapid SCADA позиціонується як ідеальна система для розробки моніторингу та управління, зокрема систем промислової автоматизації та систем IoT, систем обліку енергії та систем керування процесами.

CISA РАЗОМ З ПАРТНЕРАМИ ОПУБЛІКУВАЛИ КЕРІВНИЦТВО З РЕАГУВАННЯ НА ІНЦИДЕНТИ ДЛЯ СЕКТОРУ СИСТЕМ ВОДОПОСТАЧАННЯ ТА ВОДОВІДВЕДЕННЯ

18 січня CISA, FBI та EPA (Агентство з охорони навколишнього середовища) опублікували Керівництво з реагування на інциденти для сектору систем водопостачання та водовідведення. Посібник має допомогти власникам і операторам у секторі систем водопостачання та водовідведення (WWS) ефективно реагувати на кіберінциденти. Також посібник надає інформацію про ролі федеральних відомств, наявні ресурси та відповідальність на кожному етапі життєвого циклу реагування. До розробки документа були залучені понад 25 галузевих, некомерційних та державних/місцевих партнерів сектору WWS. Документ з'явився на фоні декількох помітних кіберінцидентів з об'єктами сектору водопостачання та водовідведення які сталися наприкінці 2023 року.

У ПОШУКАХ РІШЕННЯ З НУЛЬОВОЮ ДОВІРОЮ ДЛЯ КРИТИЧНОЇ ОБОРОННОЇ ІНФРАСТРУКТУРИ

Використання пристроїв Інтернету речей (IoT) у військових операціях, відомих як Military IoT (MIoT), значно зросло, і очікується, що ринок досягне 109 мільярдів доларів до 2030 року. Пристрої MIoT використовуються для ситуаційної обізнаності, кібербезпеки та зв'язку. Однак їх широке впровадження, яке часто віддає перевагу ціні над безпекою, призвело до постійної появи кібервразливостей. Попри те, що пристрої MIoT є критичною зоною для атак, вони створюють унікальні проблеми безпеки через різноманітні екосистеми, протоколи та обмеження обчислювальної потужності, пам'яті та часу автономної роботи. Структура безпеки з нульовою довірою, яка зосереджена на безперервній перевірці та захисті даних, орієнтованих на програмне забезпечення, не справляється з такими апаратними пристроями, як MIoT, на підприємстві. У статті наголошується на необхідності включення MIoT у комплексну стратегію нульової довіри, враховуючи вразливі місця, пов'язані з цими пристроями, і закликаючи до узгоджених зусиль для підвищення їх безпеки для ефективності національної оборони.

RANSOMWARE BLACK BASTA УСПІШНО АТАКУВАЛА БРИТАНСЬКОГО ВОДНОГО ГІГАНТА SOUTHERN WATER

23 січня компанія Southern Water підтвердила, що злочинці зламали її IT-системи, отримавши доступ до «обмеженої кількості даних». Black Basta заявив, що вкрав дані на загальну суму 750 ГБ, які складаються з особистих даних і корпоративних документів, що відповідає невеликій вибірці, витоку в Інтернеті. Southern Water надає послуги водопостачання 2,5 мільйона споживачів і послуги водовідведення 4,7 мільйона клієнтів у південних регіонах Англії.

6. АНАЛІТИЧНІ ОЦІНКИ

КІЛЬКІСТЬ ФАХІВЦІВ У СВІТІ, ЩО ПРАЦЮЮТЬ У СФЕРІ КІБЕРБЕЗПЕКИ, ДОСЯГЛА 5,5 МІЛЬЙОНА

Відповідно до результатів дослідження ISC2 2023 року (оприлюднених 3 січня), кількість кіберфахівців у світі досягла рекордного показника – 5,5 мільйона фахівців, які працюють в цій сфері. Однак те саме дослідження показало, що все ще існує серйозний дефіцит фахівців. Щоб якнайкраще впоратися з проблемами ландшафту загроз, робоча сила має зростати на 12,6% на рік. У дослідженні 2023 року показане зростання лише на 8,7%. Фактично мова йде про нестачу 4 млн кіберфахівців. Ще одна тенденція пов'язана із робочою силою у сфері кібербезпеки у 2023 році – уповільнення найму нових фахівців і за попередніми оцінками ця тенденція продовжиться і у 2024 році. Цьому сприяє очікування економічного спаду, а відтак – обережності роботодавців в питаннях розширення кадрового потенціалу.

ТЕНДЕНЦІЇ 2024 РОКУ У ПРОГНОЗАХ IBM

9 січня IBM оприлюднив власне бачення кібертенденцій 2024 року. Серед них:

- сплеск кіберактивності на фоні декількох виборчих кампаній та Олімпіади у Парижі;
- зловмисники спробують використати можливості ШІ для узагальнення та класифікації тих персональних даних, які вони отримали під час своїх кібератак – це створить для них додаткові можливості для проведення кібератак;
- збільшення кількості атак для компрометації ідентичності з метою отримання даних для нових атак;
- висока ймовірність появи першого вірусу, який створений та адмініструється ШІ;
- зміна акценту атак ransomware з великого на середній і малий бізнес;
- використання ШІ в аналітиці кіберзагроз стане більш масштабним;
- стане більше кібератак з метою викрадення зашифрованих даних в надії отримати доступ до їх вмісту із появою квантових комп'ютерів.

ЗРОСТАЄ КІЛЬКІСТЬ АТАК, ПОВ'ЯЗАНИХ ІЗ КОМПРОМЕТАЦІЄЮ ІДЕНТИЧНОСТІ – ДАНІ КОМПАНІЇ PROOFPOINT

9 січня фахівці компанії Proofpoint оприлюднили свій аналіз тенденцій у сфері компрометації ідентичності – традиційному виді злочинів, що набув нової сили за останні роки. Кіберексперти підкреслюють, що останнім часом зловмисники все частіше вдаються саме до таких атак, використовуючи скомпрометовані ними дані користувачів як основний вектор атаки. Наприклад, такі дані можуть бути використані для обходу MFA, атак на Active Directory, автоматизації фішингових атак тощо. Вже зараз є принаймні два великих кейси (Capita та Uber) де саме скомпрометовані дані стали основою для довготривалої атаки.

ЗЛОВМИСНИКИ ВСЕ ЧАСТІШЕ ВИКОРИСТОВУЮТЬ GITHUB У СВОЇХ ЦІЛЯХ

Згідно з звітом Insikt Group, опублікованому 11 січня, широке поширення GitHub в IT середовищах дозволяє суб'єктам загрози легко розміщувати та доставляти зловмисне корисне навантаження, а також використовувати його як розв'язувачів, командно-контрольних точок і точок викрадення даних. За словами дослідників, використання служб GitHub, як зловмисної інфраструктури, дозволяє зловмисникам змішуватись із законним мережевим трафіком, часто обходячи традиційні засоби захисту та ускладнюючи відстеження інфраструктури та атрибуцію акторів.

ЕФЕКТИВНІСТЬ ВПРОВАДЖЕННЯ ШІ ДЛЯ АНАЛІЗУ ДАНИХ У СФЕРІ КІБЕРБЕЗПЕКИ СИЛЬНО ЗАЛЕЖИТЬ ВІД ЯКОСТІ ДАНИХ ДЛЯ НАВЧАННЯ СИСТЕМИ – RAND CORPORATION

13 січня RAND Corporation оприлюднив один з 5 томів своїх досліджень щодо впливу ШІ на сферу безпеки. Другий том стосується питань того, які саме можуть бути обмеження у застосування ШІ для аналізу наборів кіберданих – виявлення мережевих вторгнень і виявлення зловмисного програмного забезпечення в мережах. Ключовий висновок – хоча перспективи застосування ШІ в цьому аспекті дуже добрі, але ключовою проблемою можуть стати ті набори даних, на яких відбувається навчання ШІ. Якщо дані з цих наборів будуть істотно відрізнятися від тих ситуацій, з якими буде стикатись ШІ на практиці, то його можливості будуть дуже обмежені. Фактично мова йде про оперативне та постійне оновлення тих наборів даних, на базі яких здійснюється навчання. Інакше не варто очікувати помітних результатів від ШІ.

К ВИКОРИСТАТИ РОСІЙСЬКУ СТРАТЕГІЧНУ КУЛЬТУРУ ДЛЯ ЕФЕКТИВНОЇ ВІДПОВІДІ НА ХАКЕРСЬКІ ОПЕРАЦІЇ РФ ЗА КОРДОНОМ

У статті від 15 січня Моніка Келло, яка досліджує культурні сили, що стоять за закордонними кібероперaціями росії, аналізує реакцію Великобританії на дії російських зловмисників. Вона стверджує, що національне агентство з боротьби зі злочинністю Сполученого Королівства розкрило багаторічну кіберкампанію Центру 18 Федеральної служби безпеки росії, що здійснювалася з метою впливу на демократичні процеси за допомогою операцій «злому та витоку». Відповідь уряду Великої Британії, що передбачає публічну ганьбу та економічні санкції проти окремих учасників операції, навряд чи вплине на рішення, що їх прийматиме росія.

російське хакерство ґрунтується на стратегічній культурі, що полягає в уявленнях про зовнішню загрозу існуванню, відчутті національної параної та культі самовпевнених дій. Відповідь Великої Британії має включати прозорі розслідування наслідків російських операцій злому та витоків, використовуючи російську культурну параною. Національні кіберсили Великобританії могли б використати недовіру, яка панує в російських спецслужбах і суспільстві, вносячи «тертя» в операційне середовище супротивника та націлюючись на ключових осіб і тих, хто з ними співпрацює. Ця стратегія, мабуть, ефективніша, ніж публічна ганьба чи цілеспрямовані санкції.

ТРИ НОВІ ГРУПИ ПРОГРАМ-ВИМАГАЧІВ, НА ЯКІ ВАРТО ЗВЕРНУТИ УВАГУ У 2024 РОЦІ

15 січня видання The Hacker News розповіло про три нових групи програм-вимагачів, які відкрила компанія Cyberint. До них належать 3AM, Rhysida та Akira Group. Більш детальну інформацію щодо них можна знайти у звіті компанії.

ТЕНДЕНЦІЇ 2024 РОКУ У ПРОГНОЗАХ PROOFPOINT

23 січня фахівці компанії Proofpoint оприлюднили свої прогнози щодо ландшафту кіберзагроз у 2024 році. До ключових вони віднесли:

- QR будуть ще активніше використовуватись для фішингу;
- основні злочинні групи будуть динамічніше змінювати свої TTP, вдаючись до нових, нетипових для них тактик;
- зростанні ролі ШІ у кібератаках (передусім – фішинг та соціальна інженерія);
- обмін інформацією між кіберфахівцями у попереджені кібератаки буде зростати.

ВІД МЕГАБІТА ДО ТЕРАБІТІВ: GCORE RADAR ПОПЕРЕДЖАЄ ПРО НОВУ ЕРУ DDOS-АТАК

За висновками компанії Gcore Radar, опублікованими The Hacker News 23 січня, дані за другу половину 2023 року вказують на тривожну тенденцію в ландшафті DDoS-атак. Збільшення потужності атаки до 1,6 Тбіт/с викликає особливу тривогу, сигналізуючи про новий рівень загрози, до якого повинні підготуватися організації. Постійне націлювання на ігровий, фінансовий сектори, телекомунікації та індустрію IaaS відображає стратегічну спрямованість зловмисників у виборі надавачів послуг, збій у яких має значний економічний та операційний вплив.

RANSOMWARE ЗАЛИШАЄТЬСЯ КЛЮЧОВОЮ ЗАГРОЗОЮ У ЧЕТВЕРТОМУ КВАРТАЛІ 2023 РОКУ – ЗВІТ CISCO TALOS

24 січня кібербезпекова компанія Cisco Talos оприлюднила свій звіт TALOS INCIDENT RESPONSE за 4-й квартал 2023 року. Основний результат – ransomware все ще залишається ключовою кіберзагрозою для організацій. Зі всієї загальної кількості відстежених інцидентів на ransomware припадає 28%. Основні цілі: виробничі компанії, освітні та медичні заклади. Виразною рисою організацій, які стали жертвами цих атак, є відсутність MFA, але в деяких випадках зловмисники обходили MFA шляхом атаки типу «втома від MFA» (надсилання великої кількості push повідомлень в надії, що користувач відреагує на одне з них).

ШТУЧНИЙ ІНТЕЛЕКТ ЗБІЛЬШИТЬ ОБСЯГ І ПОСИЛИТЬ ВПЛИВ КІБЕРАТАК ПРОТЯГОМ НАСТУПНИХ ДВОХ РОКІВ - ОЦІНКА НЦК ВЕЛИКОБРИТАНІЇ

24 січня британський Національний центр кібербезпеки Великобританії оприлюднив свою оцінку можливого впливу ШІ на сферу кібербезпеки. Серед ключових суджень:

- ШІ майже напевно збільшить обсяг і посилить вплив кібератак протягом наступних двох років. Однак вплив на кіберзагрозу буде нерівномірним;
- загрози походять від еволюції та вдосконалення існуючих тактик, методів і процедур (TTP);
- ШІ забезпечує підвищення можливостей у розвідці та соціальній інженерії;
- ШІ майже напевно зробить кібератаки на Велику Британію більш ефективними, оскільки суб'єкти загрози зможуть швидше й ефективніше аналізувати викрадені дані та використовувати їх для навчання моделей ШІ;
- ШІ знижує бар'єр для початківців кіберзлочинців, найманих хакерів і хактивістів для здійснення ефективних операцій доступу та збору інформації.

У 2024 РОЦІ ЦІНА КІБЕРСТРАХУВАННЯ ЗРОСТЕ – ОЦІНКА CISCO TALOS

25 січня Cisco Talos оприлюднила свої прогнози щодо розвитку ринку кіберстрахування. За їх оцінками, зростання ролі ШІ у новій хвилі атак ransomware призведе до більшого занепокоєння приватних компаній щодо можливих наслідків і як наслідок – до зростання попиту на послугу страхування. Однак страховики вже знають, що ransomware можуть становити непередбачувані масштабні ризики для страхових бізнесів, тому вартість послуг може зрости.

НЕОБХІДНА МІЖНАРОДНА ВІДПОВІДЬ, ЩОБ СТРИМУВАТИ ЗРОСТАЮЧУ ЗАГРОЗУ АТАК НА ОКІ

Еміліо Есаело, який має майже 20 років досвіду роботи аналітиком стратегічної кіберрозвідки, наголошує, що сучасний глобальний ландшафт характеризує зростання кількості кіберзагроз, націлених на ОКІ. Попри збільшення нападів, системи ефективного глобального стримування немає, і міжнародна спільнота виглядає пасивною у розв'язанні цієї проблеми. Кібератаки на критичну інфраструктуру зросли на 140% у 2022 році, причому приблизно 60% приписуються національним державам, що вказує на потенційно підступні мотиви. Останні приклади включають атаки на нафтогазові об'єкти, телекомунікації, лікарні/медичні центри та об'єкти водопостачання, в яких беруть участь різні загрозливі особи, такі як The Predatory Sparrow, Solntsepek, AGRIUS та іранські кіберактори. Відсутність встановлених норм або договорів щодо кіберповедінки погіршує ситуацію, змушуючи держави реагувати незалежно та ризикуючи ескалацією без скоординованої глобальної стратегії кіберзахисту.

НАСТАВ 2024 РІК. ЧАС ЗАПРОВАДИТИ СТАНДАРТИ АТРИБУЦІЇ В КІБЕРПРОСТОРІ

У тексті йдеться про сумнівність атрибуції кібератаки Sony Pictures у 2014 році Північній Кореї. Дехто ставить під сумнів докази та припускає, що нападників могло бути кілька, що ставить під сумнів винуватість тільки Північної Кореї. У статті наголошується на необхідності вищого стандарту при атрибуції кіберінцидентів, вказуючи на випадки, коли атрибуція була поспішна або неправильна. У ньому також відзначається відсутність відповідальності за неправильні атрибуції та потенційне зловживання кібератрибуцією державами для різних цілей. Стаття закликає до посиленого контролю, підзвітності та підвищення планки для визначення кібератрибуції в мінливому ландшафті державної та недержавної кібердіяльності.

ЯК СТВОРИТИ КРАЩІ КІБЕРСИЛИ

У статті на War on the Rocks, директор програм нових технологій Командно-штабного коледжу Корпусу морської піхоти США Майкл П. Кройцер розглядає варіанти створення кіберсил. Він наголошує, що відзначення п'ятої річниці Космічних сил у 2014 році призвело до збільшення кількості закликів до створення нового роду військ, які б діяли у кіберпросторі. Однак існують проблеми, оскільки кіберпростір суттєво відрізняється від традиційних сфер ведення війни. Закон про асигнування на національну оборону від 2024 року містить пропозицію вивчити можливість створення незалежних кіберсил, але занепокоєння щодо цілеспрямованості, культури та операційного середовища викликають сумніви щодо їх життєздатності.

У статті пропонується вийти за рамки військових інституцій і розглянути альтернативні моделі, такі як Берегова охорона США, Служба громадської охорони здоров'я, Національний офіцерський корпус Національного управління океанічних і атмосферних досліджень та Академія торгового флоту США. У ньому пропонується створити Кіберакадемію США та кіберслужбу США, щоб відповідати унікальним вимогам кіберпростору, наголошуючи на кіберпрофесіоналізмі над військовим професіоналізмом і сприяючи державно-приватному партнерству. Цей підхід спрямований на інтеграцію кіберпотенціалу в управління, уникаючи обмежень військово-орієнтованої моделі.

У 2023 РОЦІ КІЛЬКІСТЬ КІБЕРАТАК ПОДВОЇЛАСЯ – ARMIS

Згідно з результатами звіту, опублікованого компанією Armis в середині січня, хвиля глобальних атак зросла на 104% у 2023 році, і галузі з критичною інфраструктурою – особливо комунальні послуги та виробництво – взяли на себе основний тягар. Атаки на комунальні підприємства зросли більш ніж на 200%, тоді як атаки на виробництво зросли на 165%.

ЛАНДШАФТ КІБЕРЗАГРОЗ: КЛЮЧОВІ ВИСНОВКИ ТА ТЕНДЕНЦІЇ НА 2024 РІК

Звіт Axur Threat Landscape Report за 2023/2024 рр. містить поглиблений аналіз ландшафту кібербезпеки, поєднуючи дані спостереження Surface, Deep і Dark Web з уявленнями команди розвідки загроз. У звіті висвітлюються важливі тенденції, зокрема інтеграція кіберризику з бізнес-ризиком, на яку впливають геополітичні фактори. Помітні висновки включають потрійне збільшення витоків даних кредитних і дебетових карток, зміну витоків облікових даних зі сплеском використання буфера обміну та великих витоків, а також зростання зловживання брендом і нових тактик кібершахрайства. У звіті також наголошується на важливості швидкої ліквідації, аналізу діп та дарк веб та зростаючої ролі штучного інтелекту в кіберзлочинності. Платформа Polaris, керована штучним інтелектом, від Axur представлена як рішення для автоматизованого керування загрозами.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

НКЦК, МІНВЕТЕРАНІВ ТА CRDF GLOBAL ЗАПУСТИЛИ ПРОГРАМУ «КІБЕРЗАХИСНИКИ» ДЛЯ РЕІНТЕГРАЦІЇ УКРАЇНСЬКИХ ВЕТЕРАНІВ

Національний координаційний центр кібербезпеки при РНБО України та Міністерство у справах ветеранів України спільно з Фондом цивільних досліджень та розвитку США (CRDF Global) розпочали реінтеграційну програму «Кіберзахисники».

Головна мета програми – створити умови для здобуття ветеранами необхідних навичок та знань для успішної кар'єри в галузі кібербезпеки. Ініціатива передбачає комплексне навчання з кіберзахисту та кібероборони, а також підтримку у працевлаштуванні в державному секторі або можливість працювати в інституціях сектору кібербезпеки України.

GOOGLE НАДАЄ УКРАЇНСЬКИМ ДЕРЖСЛУЖБОВЦЯМ 5 ТИСЯЧ КЛЮЧІВ БЕЗПЕКИ ДЛЯ ЗАХИСТУ ОБЛІКОВИХ ЗАПИСІВ

Під час зустрічі команди Мінцифри з керівництвом Google в Давосі компанія анонсувала, що продовжить співпрацю з Україною у сфері кібербезпеки. Зокрема, у 2024 році надасть 5 тисяч ключів безпеки для захисту облікових захистів українських урядовців. Окрім цього, Google також планує проводити навчання та тренінги, щоб українські урядовці навчилися користуватися цими пристроями й ефективно використовувати весь функціонал. Також Google та український Уряд працюватимуть над спільними семінарами з кібербезпеки, щоб обмінюватися передовим досвідом і розробляти нові стратегії для захисту даних.

ЗАСТУПНИЦЯ МІНІСТРА ОБОРОНИ КАТЕРИНА ЧЕРНОГОРЕНКО ЗАКЛИКАЛА УРЯДИ КРАЇН НАТО ПОСИЛЮВАТИ СПІВПРАЦЮ В ОБОРОННИХ ІННОВАЦІЯХ

Катерина Черногоренко взяла участь у засіданні Комітету з інновацій та гібридних загроз у штаб-квартирі НАТО в межах діяльності Ради Україна-НАТО. Заступниця Міністра оборони ознайомила учасників Комітету з пріоритетами Міністерства у сфері інновацій та кіберзахисту. Окремо звернула увагу на технології, яких потребує Україна, щоб змінити «правила гри» на полі бою.

IT-КОАЛІЦІЯ: ДОЄДНАЛИСЬ НІДЕРЛАНДИ, НОВІ ВНЕСКИ КРАЇН-ПАРТНЕРІВ

На засіданні Контактної групи з оборони України у форматі «Рамштайн» до IT-коаліції доєдналася ще одна країна – Нідерланди. Новий учасник коаліції вже зробив внесок у розмірі 10 мільйонів євро.

Також в ході роботи Контактної групи Данія виділила 91 мільйон данських крон (понад 12 мільйонів євро) на кіберзахист України у межах IT-коаліції. Кошти підуть на проєкти з кібербезпеки Збройних сил України та Міністерства оборони України і є важливим внеском у довгострокову підтримку кіберзахисту держави.

УКРАЇНА ТА РУМУНІЯ УКЛАЛИ УГОДУ ПРО СПІВПРАЦЮ У СФЕРІ ЦИФРОВІЗАЦІЇ ТА КІБЕРЗАХИСТУ

Міністерство цифрової трансформації України й Міністерство досліджень, інновацій та цифровізації Румунії уклали угоду про розвиток електронних комунікацій і співпрацю у сфері цифровізації та кіберзахисту. Угода дасть змогу обмінюватися досвідом між українськими й румунськими спеціалістами. А також упроваджувати спільні проєкти для розвитку телеком-інфраструктури, цифровізації та кіберзахисту. Крім того, завдяки укладеній угоді Україна зможе брати участь у програмах фінансової підтримки ЄС.

СЕРВЕРИ І МЕРЕЖІ ДЕРЖАВИ-АГРЕСОРА РОСІЇ — ЗАКОННА ЦІЛЬ ДЛЯ НАШИХ КІБЕРФАХІВЦІВ, — АНДРІЙ ЧЕРНЯК

Представник Головного управління розвідки Міністерства оборони України Андрій Черняк у коментарі Суспільному 31 січня 2024 року повідомив, що продовжується операція у кіберпросторі держави-агресора росії, внаслідок якої зламано сервер міноборони рф та припинено функціонування спецзв'язку між підрозділами ворога.

Він додав, що атаки у кіберпросторі росії триватимуть і надалі. Адже «Подібні сервери і мережі — законна ціль для наших кіберфахівців та Сил безпеки й оборони України».

ДЕРЖСПЕЦЗВ'ЯЗКУ ОНОВИЛА ПОРЯДОК І ВИДИ ПРОВЕДЕННЯ РОБІТ З ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ВЛАСНИХ ПОТРЕБ ДЕРЖОРГАНІВ

ДССЗЗІ оновила порядок і види проведення державними органами робіт з технічного захисту інформації для власних потреб. Відповідний наказ розміщено на сайті Держспецзв'язку. За новим порядком дозвіл Держспецзв'язку потрібен тільки з метою проведення для власних потреб робіт з оцінювання захищеності інформації та робіт з виявлення закладних пристроїв. Також документ забезпечує уніфікацію у сфері технічного захисту інформації, впроваджуючи однакові види робіт як за дозволом, так і за відповідною ліцензією.

БЕЗПЕЧНИЙ КІБЕРПРОСТІР МАЄ СПИРАТИСЯ НА СПІЛЬНУ ВІДПОВІДЬ КІБЕРЗАГРОЗАМ – ЮРІЙ МИРОНЕНКО

Під час міжнародної конференції «Кіберстійкість у сучасному світі. Досвід України». голова Держспецзв'язку Юрій Мироненко повідомив, що Урядова команда реагування на комп'ютерні надзвичайні ситуації України (CERT-UA) лише за другу половину 2023 року зафіксувала та розслідувала 1462 кіберінциденти. Такі цілеспрямовані атаки здебільшого були спрямовані на міністерства та інші органи державної влади, а також на об'єкти критичної інфраструктури. За його словами, війна також продемонструвала, що на відміну від своєї кінетичної складової, агресія в кіберпросторі має глобальний характер. Усі поєднані між собою єдиним віртуальним простором, тому напади на Україну часто стосуються й інших країн світу.

ДЕРЖСПЕЦЗВ'ЯЗКУ ПРОВЕЛА ПРАКТИЧНИЙ СЕМІНАР З РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ДЛЯ ФАХІВЦІВ ДЕРЖОРГАНІВ ТА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Державна служба спеціального зв'язку та захисту інформації України за підтримки партнерів провела одноденний офлайн семінар «Реагування на кіберінциденти» для заступників керівників державних органів та об'єктів критичної інфраструктури з питань цифрового розвитку, цифрових трансформацій і цифровізації (CDTO) та відповідальних за кібербезпеку держслужбовців категорій «Б» і «В». У заході взяло участь близько 80 учасників. Метою заходу стало посилення взаємодії між Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA та фахівцями з кібербезпеки установ і підприємств.

РОСІЙСЬКЕ УГРУПОВАННЯ APT28 ЗДІЙСНЮЄ ФІШИНГОВІ АТАКИ ПРОТИ ВІЙСЬКОВОСЛУЖБОВЦІВ УКРАЇНИ

На фоні відсутності успіхів на полі бою рф посилює зусилля із кібершпигунства та продовжує спроби отримання доступу до українських військових систем ситуаційної обізнаності та управління військами шляхом викрадення облікових даних військовослужбовців. Хакерське угруповання APT28, пов'язане з ГУ ГШ ЗС рф (ГРУ), поширює фішингові html-сторінки поштового сервісу ukr[.]net. Шпигунська кампанія, що містить декілька варіантів фішингу, спрямована також на отримання доступу до поштових скриньок військовослужбовців та підрозділів Сил оборони України.

НКЦК ПОПЕРЕДИВ ПРО ЗРОСТАННЯ РІВНЯ КІБЕРЗАГРОЗ

У зв'язку з низкою кібератак на операторів мобільного зв'язку, інтернет-провайдерів, центри обробки даних, Національний координаційний центр кібербезпеки при РНБО України попереджає про високий рівень кіберзагроз для підприємств сектору комунікацій. Також основні суб'єкти забезпечення кібербезпеки фіксують зростання шкідливої деструктивної кіберактивності щодо української критичної інфраструктури. Пік кібератак очікується на лютий 2024 року.

Окрім пошкодження інфраструктури російські спецслужби намагаються використовувати будь-який інцидент у своїх інформаційних операціях.

СБУ ЗАТРИМАЛА РОСІЙСЬКОГО ІНФОРМАТОРА, ЯКИЙ ШПИГУВАВ ЗА БОЙОВИМИ ЛІТАКАМИ ЗСУ НА КІРОВОГРАДЩИНІ

Кіберфахівці Служби безпеки затримали ще одного інформатора російських спецслужб, який збирав розвіддані про Повітряні Сили ЗСУ на території Кіровоградської області. Отримані відомості зловмисник надсилав до спеціалізованих Телеграм-каналів, які були створені спецслужбами рф для збору розвідувальної інформації про українських захисників. Для маскування злочинних дій він періодично змінював нікнейм профілю у месенджері та використовував проксі-сервер для анонімізації. Зловмиснику загрожує до 8 років тюрми.

СБУ ПОПЕРЕДИЛА ПРО ФІШИНГОВУ РОЗСИЛКУ НІБИТО ВІД ЇЇ ІМЕНІ ТА ЗАКЛИКАЄ НЕ ЗАВАНТАЖУВАТИ ШКІДЛИВІ ФАЙЛИ

Служба безпеки України фіксує фішингові розсилки електронних листів нібито від імені СБУ. Розсилка спрямована переважно на органи державної влади. На перший погляд, ці листи здаються правдоподібними, однак насправді вони не мають жодного відношення до СБУ. Ці листи містять шкідливі файли і додатки, які при запуску завантажують на комп'ютер користувача шкідливе програмне забезпечення, щоб збирати конфіденційні дані. Подібні фейкові розсилки можуть використовуватися російськими спецслужбами для шпигунства та збору інформації.

СБУ ВИКРИЛА РОСІЙСЬКУ ІПСО, ЯКА ЧЕРЕЗ EMAIL-РОЗСИЛКУ НАМАГАЄТЬСЯ ПОСІЯТИ ПАНІКУ СЕРЕД УКРАЇНЦІВ

Служба безпеки попереджає про поширення масштабної email-розсилки на електронні адреси українців, у тому числі представників органів державної влади та приватних компаній. Вона здійснюється із великої кількості електронних скриньок, які перед тим були зламані російськими хакерами. Розсилка має всі ознаки цілеспрямованої інформаційно-психологічної операції. У листах пропонується співпраця з російськими спецслужбами за винагороду. Таким чином ворог вкотре намагається дестабілізувати ситуацію всередині нашої країни.

СБУ ЗАТРИМАЛА ХАКЕРА, ЯКИЙ ГОТУВАВ КІБЕРАТАКИ НА УРЯДОВІ САЙТИ УКРАЇНИ ТА НАВОДИВ РОСІЙСЬКІ РАКЕТИ НА ХАРКІВ

Кіберфахівці Служби безпеки викрили у Харкові учасника російського хакерського угруповання «народна cyberармія рф», яке підконтрольне фсб. Зловмисник коригував ворожий вогонь по місту та виконував завдання фсб щодо підготовки серії DDoS-атак на сайти держпідприємств та органів влади України. Отримані відомості він надсилав до фсб через популярний месенджер у вигляді скріншотів електронних карт з координатами потенційних цілей. Наразі зловмисник перебуває під вартою. Йому загрожує до 12 років тюрми.

2023 РОКУ КІЛЬКІСТЬ ЗАРЕЄСТРОВАНИХ КІБЕРІНЦИДЕНТІВ ЗРОСЛА НА 62,5%: ЗВІТ ОПЕРАТИВНОГО ЦЕНТРУ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ДЦКЗ

Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Держспецзв'язку оприлюднив звіт за результатами роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (СВВ) у 2023 році.

Протягом 2023 року за допомогою засобів СВВ було опрацьовано близько 18 мільярдів подій, отриманих за допомогою засобів моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки. Крім того, безпосередньо аналітиками безпеки було зафіксовано та оброблено 1105 кіберінцидентів, що на 62,5% більше ніж за результатами 2022 року.

Повний текст звіту ДЦКЗ: https://scpc.gov.ua/uk/articles/334

ХАКЕРИ РОЗСИЛАЮТЬ ВІЙСЬКОВОСЛУЖБОВЦЯМ ЗСУ ПОВІДОМЛЕННЯ ЗІ ШКІДЛИВИМ ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ ПІД ВИГЛЯДОМ РЕКРУТИНГУ ДО 3 ОШБР ТА ЦАХАЛ

CERT-UA вжила заходів щодо серії кібератак, в ході яких зловмисники розсилали в месенджері Signal військовослужбовцям ЗСУ повідомлення зі шкідливим програмним забезпеченням на тему рекрутингу до третьої окремої штурмової бригади ЗСУ та Армії оборони Ізраїлю (ЦАХАЛ). Виявили підозрілу активність фахівці американо-японської компанії Trendmicro в кінці грудня 2023 року, про що повідомили CERT-UA. Детальніше про технічну сторону атаки можна прочитати в повідомленні CERT-UA: https://cert.gov.ua/article/6276988

100 ГІГАБАЙТІВ СЕКРЕТІВ, ВАРТІСТЮ $1,5 МЛРД — ГУР ПРОІНФОРМУВАЛО ПРО ОТРИМАННЯ МАСИВУ ТАЄМНИХ ДАНИХ ПРО ВПК ОКУПАНТІВ

Головне управління розвідки МОУ проінформувало про отримання 100 гігабайтів секретних даних з російського підприємства ООО «специальный технологический центр» («СТЦ»). Вказане російське підприємство перебуває під санкціями з 2016 року. На його потужностях виробляють військове обладнання та техніку, що використовується армією рф у війні проти України.

Масив переданої для ГУР МО України інформації містить документацію на 194 номенклатурні одиниці. За попередніми оцінками, вартість одержаних даних може складати 1, 5 мільярди доларів. Це суттєвий удар по терористичній москві: вказаний архів уже використовується в цілях зміцнення обороноздатності України та ослаблення держави-агресора.

КІБЕРПОЛІЦІЯ ТА СЛІДЧІ НАЦПОЛУ ВИКРИЛИ ХАКЕРА, ЯКИЙ ЗАВДАВ ПРОВІДНІЙ СВІТОВІЙ КОМПАНІЇ СОТНІ МІЛЬЙОНІВ ЗБИТКІВ

Мешканець Миколаєва інфікував сервери відомої американської компанії вірусом-майнером. У ході міжнародної поліцейської операції правоохоронці провели обшуки та припинили діяльність хакера. Встановлено, що за понад два роки злочинної діяльності чоловік вивів на підконтрольні електронні гаманці майже два мільйони доларів США у криптовалюті, що в еквіваленті становить понад 75 мільйонів гривень. Тривають слідчі дії з метою встановлення можливих спільників фігуранта та його причетності до хакерських угруповань проросійського характеру.

ГОЛОВНЕ УПРАВЛІННЯ РОЗВІДКИ МОУ РОЗПОВІЛО ДЕТАЛІ УСПІШНОЇ ОПЕРАЦІЇ УКРАЇНСЬКИХ КІБЕРВОЛОНТЕРІВ

Головне управління розвідки МОУ інформує про успішну кібератаку на російське “федеральное государственное унитарное предприятие “главное военно-строительное управление по специальным объектам” (ФГУП “ГВСУ по специальным объектам”).

Вдалу операцію здійснили фахівці української організації Blackjack — кіберволонтери майстерно проникли до бази даних російської держкомпанії та здобули 1,2 терабайта цінних даних. Серед отриманого масиву — технічна документація на понад 500 об’єктів міноборони рф. У межах кібероперації усі вказані дані були видалені із серверів підприємства рф, що на певний час паралізує будівництво нових об’єктів московських терористів.

ГУР МОУ ІНФОРМУЄ ЩОДО КІБЕРАТАКИ НА СЕРВЕР СПЕЦЗВ'ЯЗКУ МІНІСТЕРСТВА ОБОРОНИ РОСІЇ

Головне управління розвідки Міністерства оборони України інформує — 30 січня 2024 року внаслідок кібератаки «ліг» сервер міністерства оборони держави-агресора росії, який використовувався для спецзв'язку. У результаті кібератаки припинено обмін інформацією між підрозділами міноборони рф, які користувались вказаним розташованим у москві сервером.

Програмне забезпечення на атакованому сервері було затверджене фсб рф як таке, що відповідає державним стандартам захисту інформації. Відповідний софт встановлювали на різних стратегічних об'єктах державного сектору росії, зокрема — військових.

РОСІЙСЬКІ ХАКЕРИ МІСЯЦЯМИ ПЕРЕБУВАЛИ В МЕРЕЖАХ УКРАЇНСЬКОГО ТЕЛЕКОМУНІКАЦІЙНОГО ГІГАНТА КИЇВСТАР

4 січня керівник Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ Ілля Вітюк розкрив деякі деталі кібератаки проти оператора мобільного зв'язку «Київстар». За його словами, хакерська атака спричинила «катастрофічні» руйнування та мала на меті завдати психологічного удару та зібрати розвіддані. Атака знищила «майже все», включаючи тисячі віртуальних серверів і ПК, і, на його думку це є, ймовірно, першим прикладом деструктивної кібератаки, яка «повністю знищила ядро телекомунікаційного оператора». За його інформацією хакери були присутні в системі принаймні з травня 2023 року.

УКРАЇНСЬКИЙ MONOBANK ЗАЗНАВ МАСОВАНОЇ DDOS-АТАКИ

21 січня співзасновник і генеральний директор Monobank Олег Гороховський підтвердив атаку на Monobank і заявив, що вона включала 580 млн запитів. Він також заявив, що Monobank є однією з найбільш атакованих IT-цілей в Україні.

Атака не порушила роботу послуг онлайн-банку і стала другою після аналогічної DDoS-атаки попереднього тижня.

ХАКЕРИ АТАКУВАЛИ ДАТА-ЦЕНТР «ПАРКОВИЙ»: ПОСТРАЖДАЛИ СИСТЕМА «ШЛЯХ», НАФТОГАЗ, УКРПОШТА, УЗ

У четвер, 25 січня, Нафтогаз України, Державна служба України з безпеки на транспорті, Укрпошта, та Укрзалізниця повідомили про технічні збої у роботі своїх сайтів та електронних послуг. Також відомо про проблеми з сайтом державного російськомовного телеканалу FreeДом, який перестав оновлюватися. Як виявилося, причиною стала кібератака на дата-центр «Парковий». Про відновлення сервісів Нафтогазу було оголошено лише 28 лютого.

USAID НАДАВ ДОПОМОГУ З ПОЛІПШЕННЯ КІБЕРЗАХИСТУ ЕНЕРГОСИСТЕМ УКРАЇНИ

26 січня було презентовано результати допомоги з боку USAID для НЕК «Укренерго» щодо зміцнення кіберзахисту сервісів, які забезпечують роботу енергосистеми. Допомога включає низку заходів для підвищення рівня кіберзахисту, доступності важливих сервісів та інформаційних потоків для безперебійної роботи оператора системи передачі. Зокрема закуплено обладнання та програмне забезпечення, що дозволить посилити стійкість системи та її готовність до протидії кібервикликам відповідно до міжнародних стандартів.

КООРДИНАЦІЙНИЙ ШТАБ З ПИТАНЬ ПОВОДЖЕННЯ З ВІЙСЬКОВОПОЛОНЕНИМИ ЗАЗНАВ КІБЕРАТАКИ

29 січня Координаційний штаб з питань поводження з військовополоненими повідомив, що після належної перевірки IT-фахівцями всі його сервіси, які попереднього дня були піддані DDoS-атаці, працюють у штатному режимі та доступні онлайн. Хакерська група, яка стоїть за інцидентом, не була ідентифікована, але штаб вказує на москву, пов'язуючи атаку з нещодавньою катастрофою російського транспортного літака, який, нібито, перевозив українських військовополонених.

8. ПЕРША СВІТОВА КІБЕРВІЙНА

ЯК РОСІЙСЬКИЙ NoName057(16) МОЖЕ СТАТИ НОВОЮ МОДЕЛЛЮ ДЛЯ ХАКЕРСЬКИХ ГРУП

У статті видання CSO Online йдеться про проросійську хактивістську групу NoName057(16) та її еволюцію від «маловідомої хакерської групи» до організованого колективу кіберпартизанів-добровольців. Група, яка здійснила значну кількість DDoS атак, успішно побудувала онлайн-спільноту з фінансовими стимулами для волонтерів. NoName057(16) спочатку націлювалася на українські вебсайти, але розширила свій фокус, включивши всі країни, які підтримують Україну. Методи роботи групи включають дезінформацію, залякування та створення хаосу. Зокрема, вона спирається на краудсорсинговий проєкт ботнету DDoSia та винагороджує волонтерів криптовалютою.

Попри її можливості, що розвиваються, автор статті сумнівається, чи становить NoName057(16) серйозну загрозу безпеці для Заходу, наголошуючи, що її вплив наразі низький. Унікальний підхід групи щодо інтеграції фінансових стимулів для волонтерів створює нову нішу в хакерській спільноті, піднімаючи питання щодо її майбутнього розвитку, потенційних імітаторів та її ролі після російсько-української війни.

БЕКДОР «ТРІАНГУЛЯЦІЯ» ЗАРАЗИВ ДЕСЯТКИ IPHONE, ЩО НАЛЕЖАТЬ СПІВРОБІТНИКАМ КАСПЕРСЬКОГО

Як повідомило видання Ars Technica, нещодавнє розслідування, проведене компанією Kaspersky, розкрило подробиці просунутої та складної атаки під назвою «Операція Тріангуляція», націленої на iPhone, якої зазнала сама компанія. Протягом чотирьох років зловмисники використовували невідому апаратну функцію, ймовірно, для налагодження чи тестування, що дозволяло їм досягти безпрецедентного рівня доступу. Зловмисники надсилали повідомлення iMessage, використовуючи чотири вразливості нульового дня для встановлення шпигунського ПЗ на iPhone, Mac, iPod, iPad, Apple TV і Apple Watch. Унікальні характеристики кампанії ускладнюють атрибуцію, а зловмисники залишаються невідомими. Дослідники Kaspersky виявили та повідомили про понад 30 вразливостей нульового дня у різних продуктах, але назвали цей ланцюг атак найдосконалішим з усіх, які вони бачили.

ПОМСТА ЗА «КИЇВСТАР»: УКРАЇНСЬКІ ХАКЕРИ ЗАЛИШИЛИ ЧАСТИНУ МОСКВИ БЕЗ ІНТЕРНЕТУ – ДЖЕРЕЛО

9 січня джерела в правоохоронних органах повідомили, що хакери угрупування Blackjack, зламали московського інтернет-провайдера «М9ком» й позносили його сервери. Як наслідок – частина жителів москви залишилася без Інтернету та ТБ. За словами джерела, хакери заявили, що це одна з «тренувальних атак» перед більшою, що буде серйозною помстою за «Київстар».

УКРАЇНСЬКІ ХАКЕРИ УСПІШНО АТАКУВАЛИ ПЛАТІЖНИЙ САЙТ ОДНІЄЇ З ОБЛАСНИХ ЕНЕРГЕТИЧНИХ КОМПАНІЙ РОСІЇ

13 січня Хакери з IT-армії України успішно атакували приймальню платежів «Перменерго» Пермського краю росії. Вони заявили, що зупинили роботу сайту та платіжних шлюзів. Можливе порушення внутрішніх операцій «Перменерго».

ДОДАТОК BANGLADESH ELECTION ВИЙШОВ З ЛАДУ ЧЕРЕЗ ЙМОВІРНУ КІБЕРАТАКУ, ЗВИНУВАТИЛИ УКРАЇНУ ТА НІМЕЧЧИНУ

Україну та Німеччину звинувачують у кібератаці з метою збою програми, яка використовувалася під час загальних виборів у Бангладеш 6-7 січня. Офіційний секретар виборчої комісії Бангладеш Мохаммед Джахангір Алам не уточнив тип нападу чи його причину. Застосунок не використовувався для голосування, лише для надання інформації виборцям.

КИТАЙ ЗБИРАЄ ДАНІ ПРО ВРАЗЛИВОСТІ, ЯКІ Є В ПЗ, ЯКИМ КОРИСТУЮТЬСЯ ІНОЗЕМНІ КОМПАНІЇ

18 січня у виданні NEWSWEEK вийшов оглядовий матеріал про наслідки застосування в КНР «Положення про керування вразливістю мережевих продуктів», яке було опубліковано у липні 2021 року органом із контролю за кіберпростором Китаю. Згідно з цим документом китайські компанії мають повідомляти про вразливості у ПЗ або в продуктах, які вони використовують, протягом 48 годин після виявлення. В багатьох випадках це ж ПЗ використовується іноземними компаніями, а відтак уряд КНР збирає значну базу про такі вразливості. Особливістю процедури є те, що таке повідомлення уряду має відбуватись раніше, ніж будуть вжиті заходи для усунення вразливості чи інформування про неї громадськості.

MICROSOFT СТАЛА ЖЕРТВОЮ АТАКИ РОСІЙСЬКОГО ДЕРЖАВНОГО НАПАДНИКА MIDNIGHT BLIZZARD

19 січня Microsoft повідомила, що 12 січня 2024 року виявила атаку національного рівня на свої корпоративні системи, та визначила загрозу як російське угруповання Midnight Blizzard, також відоме, як Nobelium. За повідомленням самої корпорації, починаючи з кінця листопада 2023 року, зловмисник використовував атаку розпилення пароля, щоб скомпрометувати застарілий невиробничий тестовий обліковий запис клієнта та закріпитися, а потім використав дозволи облікового запису для доступу до дуже невеликого відсотка корпоративних облікових записів електронної пошти Microsoft, включаючи вище керівництво та співробітників служби кібербезпеки, юридичних та інших відділів. Також було викрадено деякі електронні листи та вкладені документи.

Розслідування вказує на те, що спочатку зловмисники шукали інформацію, пов'язану з самою Midnight Blizzard. Компанія наголошує, що атака не була результатом уразливості в продуктах або службах Microsoft. Тим часом пізніше (27 січня) компанія визнала, що зламаний корпоративний обліковий запис, який використовувався в основі пограбування, навіть не мав багатофакторної автентифікації (MFA). Компанія також опублікувала настанови для тих, хто відповідатиме на атаки з боку державних загроз, базовані на її досвіді.

УКРАЇНСЬКІ ХАКЕРИ ЗЛАМАЛИ РОСІЙСЬКИЙ ДОСЛІДНИЦЬКИЙ ЦЕНТР КОСМІЧНОЇ ГІДРОМЕТЕОРОЛОГІЇ

23 січня українське хакерське угруповання BO Team зламало великий російський дослідницький центр космічної гідрометеорології- науково-дослідний центр космічної гідрометеорології «Планета». В такий спосіб було завдано суттєвого удару по безпосередніх споживачах «Планети»: Міністерству оборони і Генштабу рф, службам МНС рф, Сєверному флоту».

Повідомляється, що українські хакери отримали первинний доступ до двох серверів «Планети», а після цього атакували всі її пристрої та сервіси. У результаті було знищено безпрецедентний за масштабами для такого роду акцій масив інформації – сумарно близько 2 петабайт (приблизно 2 млн гігабайтів) даних. Часто це або стаття, або який документ, який фейковий акаунт нібито збирається опублікувати, та просить про коментарі.

РОСІЙСЬКА ГРУПА ЗАГРОЗ COLDRIVER РОЗШИРЮЄ КОЛО ЗАСОБІВ, ЩО ВОНА ЗАСТОСОВУЄ ПРОТИ ЗАХІДНИХ ЧИНОВНИКІВ

18 січня Threat Analysis Group компанії Google опублікувала звіт, в якому йдеться про те, що російське угруповання COLDRIVER продовжує збір облікових даних за допомогою фішингу, який стосується України, країн НАТО, академічних установ і неурядових організацій. Щоб завоювати довіру своїх цілей, COLDRIVER часто використовує облікові записи, що видають себе за іншу особу, наприклад, експерта в певній галузі або людини, якимось чином пов'язаної з мішенню фішингової атаки. Потім фальшивий обліковий запис використовується для встановлення стосунків із ціллю, що підвищує ймовірність успіху фішингової кампанії, і зрештою надсилає фішингове посилання або документ, що містить посилання. Окрім фішингу облікових даних, угруповання останнім часом доставляє зловмисне програмне забезпечення через документи PDF.

ТЕХГІГАНТА HP ENTERPRISE ЗЛАМАЛИ РОСІЙСЬКІ ДЕРЖАВНІ ХАКЕРИ

25 січня, The Hacker News повідомило, що хакерів, пов'язаних із Кремлем, підозрюють у проникненні в хмарне середовище електронної пошти компанії Hewlett Packard Enterprise (HPE) з метою викрадення даних поштових скриньок.
Згідно з поданням компанії до регуляторних органів США, починаючи з травня 2023 року, зловмисники отримали доступ і викрадали дані з невеликого відсотка поштових скриньок HPE, що належать особам, які займаються кібербезпекою, виходом на ринок, бізнес-сегментами та іншими функціями.

Вторгнення приписують російській державній групі, відомій як APT29, яка також відстежується під іменами BlueBravo, Cloaked Ursa, Cozy Bear, Midnight Blizzard (раніше Nobelium) і The Dukes.

У ГРУЗІЇ РОСІЙСЬКІ ХАКЕРИ АТАКУВАЛИ САЙТ ПРЕЗИДЕНТА

26 січня офіційний сайт президента Грузії Саломе Зарубішвілі зазнав кібератаки з боку групи російських хакерів. На сторінці з'явилося зображення черепа і напис «зламано Cozy Bear, Слава росії». Окрім цього, хакерського нападу зазнав сайт опозиційної грузинської телекомпанії «Формула»: сторінка була недоступна кілька годин, після чого роботу сайту відновили.

ВІЙСЬКОВА РОЗВІДКА УКРАЇНИ ПРОВЕЛА НАСТУПАЛЬНУ ОПЕРАЦІЮ ПРОТИ РОСІЙСЬКОЇ КОМПАНІЇ, ЩО СПЕЦІАЛІЗУЄТЬСЯ НА ВПРОВАДЖЕННІ ІНФОРМАЦІЙНИХ СИСТЕМ У РОСІЙСЬКІЙ ПРОМИСЛОВОСТІ

27 січня Головне управління розвідки Міністерства оборони України проінформувало про те, що її фахівці провели успішну кібератаку проти IT-інфраструктури компанії IPL Consulting, яка спеціалізувалася на впровадженні інформаційних систем у російській промисловості. Вся її IT-інфраструктура розміром понад 60 терабайтів, а також десятки серверів і баз даних були знищені.

9. РІЗНЕ

ЩО ТАКЕ «КІБЕРВИКРАДЕННЯ» І ЩО ВИ МОЖЕТЕ ЗРОБИТИ, ЩОБ ЗАЛИШАТИСЯ В БЕЗПЕЦІ В ІНТЕРНЕТІ?

Китайського студента за обміном, який проживав у приймаючій сім'ї, знайшли після інциденту, який влада називає «кібервикрадення». В його процесі жертва та викрадачі не зустрічалися фізично. Натомість викрадачі зв'язалися зі студентом онлайн і наказали йому тихо піти й залишитися на самоті у наметі в горах, неподалік від місця проживання приймаючої родини. Викрадачі погрожували завдати шкоди його родині в Китаї. Після цього вони також надіслали онлайн його родині вимогу про викуп, 80 тисяч доларів з якого родина заплатила.

Deseret News визначає «кібервикрадення» як «форму злочину, в якій жертви стають мішенню онлайн-зловмисників і змушені ізолюватися, щоб зловмисники вимагали викуп від їх сімей». Це форма викрадення повністю ґрунтується на погрозах жертвам, без прямого фізичного контакту, необхідного для злочину. Як захиститися? Якщо з вами зв'язалися кібервикрадачі, не виконуйте їхні вказівки, а замість цього негайно викликайте поліцію, йдеться у матеріалі.

FTC ПРИЙНЯЛА РІШЕННЯ У БЕЗПРЕЦЕДЕНТНІЙ СПРАВІ ПРОТИ БРОКЕРА ГЕОЛОКАЦІЙНИХ ДАНИХ

9 січня Федеральна торгова комісія (FTC) досягла першої в історії мирової угоди з брокером даних Outlogic (раніше відомий як X-Mode Social) у справі про продаж даних про точне місцеперебування споживачів без відповідних запобіжників. Угода містить такі положення, як заборона обміну конфіденційними даними про місцеперебування, вимога знищити раніше зібрані дані та впровадження програм для запобігання подальшим зловживанням. FTC стверджувала, що Outlogic не застосувала розумних запобіжників і не вжила заходів, щоб запобігти використанню інформації третіми сторонами. Компанію звинувачують у продажу необроблених даних, прив'язаних до конкретних мобільних телефонів, включаючи відвідування конфіденційних місць, без належного інформування споживачів. Outlogic заперечує, що описані FTC наслідки настали, і зазначає, що не виявила жодного випадку зловживання даними. Прихильники конфіденційності вважають угоду безпрецедентною, але наголошують на необхідності більш суворого регулювання діяльності брокерів даних.

ПЕРЕД ВИБОРАМИ ТАЙВАНЬ ЗАЗНАВ МАСОВАНИХ КІБЕРАТАК

11 січня Politico повідомило, що Тайвань переживає безпрецедентний сплеск кібератак, як вважають, організованих Китаєм, лише за кілька днів до важливих президентських виборів 13 січня. Mandiant від Google Cloud повідомив про значне збільшення китайських шпигунських операцій проти уряду Тайваню, технологій та критична інфраструктура. В останньому кварталі 2023 року кількість кібератак, спрямованих на перевантаження та збій мереж на Тайвані, зросла на 3370%. Ці атаки в поєднанні з контентом на основі штучного інтелекту створюють проблеми з оцінкою їх впливу. Експерти припускають, що стратегія Китаю включає «кампанію, спрямовану на створення відчуття сорому», в рамках якої актори проникають в системи для публікації принизливих заяв проти інституцій Тайваню. Зростання напруженості збігається зі збільшенням використання ШІ Китаєм для кібероперацій. Уряд Китаю спростував звинувачення в кібератаках і висловив надію на мирні вибори на Тайвані.

КИТАЙ ЗАЯВЛЯЄ, ЩО ЙОГО ДЕРЖАВНІ ЕКСПЕРТИ ЗЛАМАЛИ AIRDROP ВІД APPLE

Міська влада Пекіна повідомила, що китайські експерти розробили метод ідентифікації користувачів зашифрованої служби AirDrop від Apple, що дозволяє отримати доступ до номерів телефонів і облікових записів електронної пошти. Методика, розроблена в Інституті юстиції в Пекіні, спрямована на відстеження анонімних комунікацій, що сприяє поліцейським розслідуванням. Хоча в заяві не згадується про арешти, звіти свідчать про те, що AirDrop використовувався для поширення антиурядових листівок у Китаї. У відповідь Apple оновила AirDrop у Китаї, дозволивши користувачам отримувати файли лише від відомих контактів протягом певного періоду часу, потенційно обмежуючи поширення несанкціонованого вмісту. Дії Apple у Китаї викликали критику за поступки уряду щодо посилення контролю над інакодумцями, особливо після впровадження суворого закону про національну безпеку в Гонконзі, який було придушено громадську опозицію.

ГОЛЛАНДСЬКИЙ ІНЖЕНЕР ВИКОРИСТАВ ВОДЯНУ ПОМПУ, ЩОБ ДОСТАВИТИ ЗЛОВМИСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ STUXNET НА ІРАНСЬКУ ЯДЕРНУ УСТАНОВКУ

Опубліковане 8 січня розслідування голландської газети De Volkskrant показало, що голландський інженер, завербований розвідувальними службами Нідерландів, AIVD, ймовірно, зіграв роль у розгортанні шкідливого програмного забезпечення Stuxnet на іранському ядерному об'єкті. Ерік ван Саббен, завербований AIVD, нібито встановив зловмисне програмне забезпечення Stuxnet на водяну помпу на ядерному комплексі в Натанзі. Хоча подробиці щодо його обізнаності чи точного методу розгортання зловмисного програмного забезпечення залишаються незрозумілими, це відкриття відкриває новий кут для розповіді Stuxnet. Раніше повідомлялося, що нідерландська розвідка завербувала іранського інженера з подібною метою. Обставини смерті Ван Саббена в аварії на мотоциклі в Об'єднаних Арабських Еміратах через кілька тижнів після атаки Stuxnet додають цій історії моторошний аспект. Попри відкриття розслідування, ключові деталі, такі як точний метод доставлення Stuxnet, залишаються непідтвердженими.

АМЕРИКАНСЬКІ ВІЙСЬКОВІ ВИКОРИСТОВУЮТЬ УКРАЇНСЬКИЙ ДОСВІД ПРИ ВПРОВАДЖЕННІ НОВИХ ІТ НА ПОЛІ БОЮ

24 січня стало відомо, що американські військові активно тестують додаток ATAK на базі Android. Окрім нанесення позицій сил на реальну карту, програмне забезпечення дозволяє солдатам створювати групи чатів і передавати зв'язок через радіо, серед інших функцій. Система схожа на українську систему «Кропива», яка також побудована на базі Android. І хоча на думку експертів пристрої, на яких працює програма, є бажаною ціллю для захоплення ворогом, але як і в ситуації із «Кропива» їх можна дистанційно заблокувати, якщо їх захоплять.