НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

CYBER DIGEST

Огляд подій в сфері кібербезпеки,
березень 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

У березні вийшла нова Національна стратегія кібербезпеки США. Документ визначає 5 основних (стратегічних) сфер інтересів США, серед яких безпека критичної інфраструктури, боротьба з ransomware всіма можливими засобами, більше уваги до освіти кіберспеціалістів. Серед важливих нововведень – вимога до «безпечного кодингу». Експертне ком'юніті дискутує, наскільки ця вимога може вплинути на інноваційні процеси у США та на конкурентоздатність американських IT-компаній на світовому ринку. Деякі експерти наголошують на тому, що у міжнародному аспекті стратегія США у кіберпросторі відрізняється від більш стриманого підходу, який адміністрація Байдена застосовує до російсько-української війни.

ЄС продовжує модифікацію власного законодавства у сфері кібербезпеки, аби створити безпечніший європейський кіберпростір. Зараз основна лінія дискусій стосується норм майбутнього Закону про кіберстійкість – держави-члени продовжують складні дебати щодо жорсткості обмежень, які він може накладати на учасників ринку (в т.ч. щодо обміну інформацією про кіберінциденти та роль в цьому процесі ENISA і національних CSIRT-ів). Однак також у квітні буде презентовано проєкт нового нормативного документа – Закон про кіберсолідарність. Цей документ має створити загальноєвропейську мережу організацій кібербезпеки приватного сектору, яка може прийти на допомогу ЄС у випадку масштабного кіберпротиборства (що є одним з уроків російсько-української кібервійни).

Українські фахівці з Державної служби спеціального зв'язку та захисту інформації відстежують тенденції російських кіберзагроз. Було оприлюднено звіт russia's Cyber Tactics: Lessons Learned 2022, який містить узагальнення досвіду України у протистоянні російській агресії в кіберпросторі протягом 2022 року. Автори звіту дослідили основні угруповання, їхню мотивацію, методи та інструменти атак. У 2023 році фахівці CERT-UA відзначають зростання кількості атак з метою шпигунства з акцентом на утриманні постійного доступу до організації, що може означати, що рф готується до тривалої війни.

Україна продовжує розвивати міжнародну співпрацю для спільної протидії кіберзагрозам. У березні було налагоджено співпрацю між українськими державними органами та міжнародними компаніями. Наприклад, залучено до співпраці австралійську організацію «Інтернет 2.0», відбувається діалог з європейськими аналітичними центрами (Лісабонська рада). Крім того, у співпраці з правоохоронцями Німеччини, Нідерландів, Федерального бюро розслідувань та за підтримки Європолу було викрито учасника хакерської групи, що причетна до функціонування ransomware DoppelPaymer.

США продовжують нарощувати увагу до безпеки OKI та їх OT систем. CISA спільно з іншими суб'єктами (державними та приватними) випускає різноманітні посібники для оцінки стану кібербезпеки підприємств окремих секторів (наприклад, транспорту), тестує окремі OKI на проникнення (за допомогою власної red team), налагоджує процес обміну інформацією про кіберінциденти та навіть запускає програми превентивного інформування про загрози кібербезпеці. Ці ініціативи не лише реалізують прийняті раніше документи, але й відповідають духу та букві нової Національна стратегія кібербезпеки США.

Україна посилює свою теперішню та майбутню стійкість до кіберзагроз. Українські фахівці успішно беруть участь у міжнародних змаганнях (призові місця у NATO TIDE Hackathon 2023). Відбувається постійне підвищення кваліфікації кіберполіцейських та кіберзахисників. Для забезпечення майбутньої кіберстійкості посилюється співпраця з вищими навчальними закладами України.

Збройні Сили США продовжують нарощувати свій кіберпотенціал та можливості: запускають програми навчання власних програмістів (на базі Корпусу морської піхоти), створюють посібники із впровадження окремих політик zero trust, продовжують розгортати команди реагування по всьому світу. Як наслідок – Пентагон просить збільшити фінансування цього напрямку у 2024 році на 21% – до 13,5 млрд доларів США.

У березні активізувались хакерські угрупування пов'язані з КНР. Вони вдаються до традиційних практик кібершпигунства, шукаючи нові методи та вектори атак. У сфері їх першочергової уваги – державні установи, аналітичні центри та ОКІ з різних секторів економіки. Між тим китайські виробники телекомунікаційного обладнання продовжують конкурувати на європейському ринку, вбудовуючись у великі інфраструктурні проєкти (наприклад, як партнерство з Deutsche Bahn). Швидше за все це викличе черговий раунд дебатів щодо меж використання китайський телеком продуктів в різних секторах критичної інфраструктури.

російські хакери продовжують свою кампанію проти союзників України в межах світової кібервійни. CISA попередило про загрозу застосування ransomware Royal проти ОКІ в США, випробовує нові техніки атак, посилює кібератаки проти лікарень, атакує європейські структури та акаунти в соцмережах представників влади. Одночасно з цим росія шукає можливості розширення кадрової бази у сфері кібербезпеки – зокрема, впроваджує спрощені правила отримання посвідки на постійне проживання для таких спеціалістів.

Експерти оцінюють кіберактивність росії як підготовку нею нового етапу протистояння. Вони вже намагались заблокувати функціонування Starlink в зоні бойових дій через радіоелектронну боротьбу, створюють нові ransomware та viper'и. Повідомляється також, що російські військові можуть визначати точне місцеперебування терміналів, що змушує українських військових використовувати їх лише за необхідності. Партнери України нагадують, що російські кіберспроможності хоч і не змогли показати помітного ефекту на перших етапах війни, але їх не варто недооцінювати і сторони мають бути готові до тривалого протистояння в кіберпросторі.

Продовжується протистояння між США та Китаєм у сфері Інтернету та технологій. Відзначається співпраця між приватним та державним сектором США у цьому питанні, а також намір американських законодавців заборонити китайський застосунок TikTok з міркувань приватності громадян США та національної безпеки. На зв'язках китайських технологічних компаній з Комуністичною партією Китаю наголошують і автори звіту, який було подано спеціальному комітету Сенату Австралії щодо іноземного втручання через соціальні мережі. Боротьба між Китаєм та США відбувається й на рівні фізичної інфраструктури Інтернету, про що йдеться у спеціальному звіті Reuters.

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

БІЛИЙ ДІМ ОПУБЛІКУВАВ НАЦІОНАЛЬНУ СТРАТЕГІЮ З КІБЕРБЕЗПЕКИ

Першого березня у США адміністрація Президента Байдена опублікувала нову редакцію стратегії кібербезпеки.

«У це вирішальне десятиліття Сполучені Штати переосмислять кіберпростір як інструмент для досягнення наших цілей у спосіб, який відображає наші цінності: економічна безпека та процвітання, повага до прав людини та основних свобод, довіра до нашої демократії та демократичних інститутів, і справедливе та різноманітне суспільство. Щоб реалізувати це бачення, ми повинні зробити фундаментальні зміни у тому, як Сполучені Штати розподіляють ролі, відповідальність і ресурси в кіберпросторі».

ЄС ГОТУЄТЬСЯ ОПУБЛІКУВАТИ ПРОЄКТ ЗАКОНУ ПРО КІБЕРСОЛІДАРНІСТЬ (CYBER SOLIDARITY ACT), ЯКИЙ ВРАХОВУЄ УРОКИ РОСІЙСЬКО-УКРАЇНСЬКОЇ КІБЕРВІЙНИ

Першого березня видання Euractiv надало першу інформацію про зміст майбутнього європейського Закону про кіберсолідарність. Цей документ розробляється з березня 2022 року і враховує уроки російсько-української кібервійни. Ключова ідея документа – створення надзвичайного фонду кібербезпеки для найму компаній з кібербезпеки («кіберрезерву») для проведення аудитів і реагування на інциденти. Ці компанії мають попередньо отримати статус довірених постачальників, але наразі відсутні подробиці як це буде відбуватись. Текст документи має бути представлено 5 квітня.

АГЕНТСТВО ОХОРОНИ НАВКОЛИШНЬОГО СЕРЕДОВИЩА США ВСТАНОВИЛО ВИМОГИ ЩОДО КІБЕРБЕЗПЕКИ СИСТЕМ ВОДОПОСТАЧАННЯ

Третього березня Агентство охорони навколишнього середовища США встановило вимоги щодо кібербезпеки систем водопостачання. Правила вимагають від штатів «оцінювати кібербезпеку операційної технології, яка використовується PWS (системою громадського водопостачання) під час проведення санітарних досліджень PWS або в рамках інших державних програм». Меморандум містить різноманітні ресурси, у тому числі запропоновані підходи до включення кібербезпеки в санітарні обстеження та посилання на найкращі практики кібербезпеки EPA для водного сектору. EPA також пропонуватиме віртуальне навчання та технічну допомогу.

АДМІНІСТРАЦІЯ БЕЗПЕКИ НА ТРАНСПОРТІ США ВИДАЛА НАДЗВИЧАЙНІ РОЗПОРЯДЖЕННЯ ЩОДО КІБЕРБЕЗПЕКИ ДЛЯ АЕРОПОРТІВ ТА ОПЕРАТОРІВ ПОВІТРЯНИХ СУДЕН

7 березня Управління транспортної безпеки США (TSA) опублікувало нові протоколи кібербезпеки в надзвичайних ситуаціях для аеропортів і операторів повітряних суден, які вимагають від них попередньо схвалених планів впровадження посилених заходів безпеки.

TSA заявило, що видає поправки щодо кібербезпеки «через постійні загрози кібербезпеці щодо критично важливої інфраструктури США, включаючи авіаційний сектор», але не повідомило, які конкретні проблеми спонукали до цього заходу. Очільник TSA Девід Пекоске повідомив, що Адміністрація працюватиме з компаніями, щоб допомогти їм «знизити ризики кібербезпеки та підвищити кіберстійкість для підтримки безпечних, надійних та ефективних подорожей».

Серед іншого, компанії повинні розробити політику сегментації мережі, яка відокремлює IT-системи від операційних, щоб у разі кібератаки послуги могли продовжуватись. Заходи контролю доступу також повинні бути запроваджені разом із системами постійного моніторингу, які можуть «захищатися від загроз і аномалій кібербезпеки, виявляти та реагувати на них».

ЄС ЗАПРОВАДЖУЄ ЗАГАЛЬНІ ВИМОГИ БЕЗПЕКИ У ВСІХ СВОЇХ УСТАНОВАХ

9 березня Комітет промисловості Європейського парламенту проголосував за проєкт звіту депутата Європарламенту Хенни Віркунен, який пропонує запровадити загальні стандарти кібербезпеки в установах ЄС. Мета – «створити високий спільний рівень кібербезпеки в установах, органах, офісах та агентствах Союзу». Документ розширює можливості та фінансування Групи реагування на інциденти комп'ютерної безпеки ЄС (CERT-EU), її додаткові обов'язки як, наприклад, виконання координаційної ролі в розкритті вразливостей. Відповідно до звіту, організації повинні подати раннє попередження про інцидент протягом 24 годин після того, як їм стало відомо, і офіційне повідомлення про інцидент із зазначенням початкової оцінки його серйозності та впливу протягом 72 годин.

ЕКС-ПРЕЗИДЕНТ МІКРОНЕЗІЇ ЗВИНУВАТИВ КНР У ПІДКУПІ ПОЛІТИЧНОГО КЛАСУ ТА БАЖАННІ КОНТРОЛЮВАТИ ПІДВОДНІ ОПТИЧНІ КАБЕЛІ ОСТРОВА

9 березня екпрезидент Федеративних Штатів Мікронезії Девід Пануело написав листа, у якому звинуватив КНР у хабарництві, шпигунстві та інших тактиках, включаючи спробу взяти під контроль національні підводні кабелі та телекомунікаційну інфраструктуру країни. Лист включає великий пакет звинувачень, які на думку Д. Пануело реалізуються КНР в межах функціонування підписаних між Пекіном та іншими країнами регіону Меморандумів про взаєморозуміння щодо поглиблення блакитної економіки.

CISA ЗАСНУВАЛА ПІЛОТНУ ПРОГРАМУ ПОПЕРЕДЖЕННЯ ПРО ВРАЗЛИВОСТІ ПЕРЕД RANSOMWARE

13 березня CISA анонсувала запуск пілотної програми попередження про вразливості перед ransomware (RVWP). Ця програма спирається на завдання, поставлені у Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). RVWP буде виявляти організації (використовуючи різні методи та інструменти), що мають вразливості, якими часто користуються оператори ransomware. Це надасть змогу попередити численні атаки на організації та поліпшити готовність критичної інфраструктури до викликів їх безпеці. Програма вже працює у тестовому режимі та CISA використовує її – попередження вже отримали 93 організації, у яких було ідентифіковано запущені версії Microsoft Exchange Service з уразливістю під назвою «ProxyNotShell».

ПЕНТАГОН ЗБІЛЬШИВ БЮДЖЕТНИЙ ЗАПИТ НА 2024 РІК НА 21%

13 березня було повідомлено, що новий бюджетний запит Пентагону на 2024 рік буде включати підвищений запит на питання кібербезпеки. У 2023 році бюджет складав 11,2 млрд доларів, в той час, як новий запит складає 13,5 млрд доларів. Ці кошти потрібні Пентагону на продовження модернізації мережевого захисту, побудови безпечної та стійкої кіберархітектури, а також підтримку 147 Cyber Mission Force, які створені та підтримуються Кіберкомандуванням США.

ЄС ПРОДОВЖУЄ ДИСКУСІЇ ЩОДО ПОЛОЖЕНЬ ЗАКОНУ ПРО КІБЕРСТІЙКІСТЬ

Держави-члени ЄС продовжують діалог щодо положень майбутнього Закону про кіберстійкість. Його попередні положення викликали помітні суперечки між країнами й наразі триває діалог щодо їх корегування.

15 березня Швеція оприлюднила нову версію компромісного тексту документа. Він містить:
- скасування п'ятирічного ліміту життєвого циклу продукту (раніше передбачалось, що продукти мають проходити систематичну оцінку);
- уточнює сферу застосування регламенту (наприклад, він не буде поширюватись на сайти, які не підтримують функціональні можливості підключених пристроїв, і хмарні сервіси);
- робить автоматичні оновлення безпеки параметром за замовчуванням для підключених пристроїв.

Також законодавці відмовились від ідеї створення на базі ENISA єдиної бази всіх вразливостей, адже учасники ринку непокоїлись про можливість витоків з неї. Тепер цими питаннями має опікуватись національний CSIRT, який також буде зобов'язаний передавати інформацію про вразливість виробнику.

КОМІСІЯ З ЦІННИХ ПАПЕРІВ І БІРЖ США ПРОПОНУЄ НОВІ ПРАВИЛА ЗВІТУВАННЯ ПРО КІБЕРІНЦИДЕНТИ ДЛЯ ФІНАНСОВИХ ОРГАНІЗАЦІЙ

15 березня Комісія з цінних паперів і бірж США (SEC) запропонувала нові правила кібербезпеки для низки фінансових організацій, які змусять їх повідомляти про інциденти протягом 48 годин після виявлення та запровадити певні політики безпеки.
Правила поширюватимуться на брокерів-дилерів, клірингові агентства, основних учасників свопів на основі цінних паперів, муніципальну раду з регулювання цінних паперів, національні асоціації та біржі цінних паперів, сховища даних та дилерів свопів на основі цінних паперів, агентів з передачі.

Не всі члени комісії вважають пропозиції необхідними. Зараз правила проходить період громадського обговорення протягом 60 днів, перш ніж регулятори приймуть рішення, чи рухатися далі у цьому напрямку.

ПРИ ПРЕЗИДЕНТІ США СТВОРЕНО РОБОЧУ ГРУПУ З ПИТАНЬ КІБЕРФІЗИЧНОЇ СТІЙКОСТІ

15 березня 2023 Рада консультантів з питань науки та технологій при Президенті США (PCAST) сформувала робочу групу з кіберфізичної стійкості для консультацій експертів з усього державного та приватного секторів і наукових кіл щодо напрацювання рекомендацій для створення стійкої до збоїв критичної інфраструктури. Протягом наступних шести місяців група консультуватиметься з численними організаціями та експертами, щоб сформулювати відповідні рекомендації Джо Байдену. Крім прямих консультацій, група запрошує всі зацікавлені сторони подавати свої письмові пропозиції.

ENISA ЗАПУСТИЛА ТЕМАТИЧНИЙ САЙТ ПРО СЕРТИФІКАЦІЮ ЄС У СФЕРІ КІБЕРБЕЗПЕКИ

19 березня ENISA запустила сайт, який має надати максимум інформації зацікавленим сторонам про питання сертифікації ЄС у сфері кібербезпеки. Серед тем, на яких акцентується сайт:

- Європейська схема сертифікації кібербезпеки (EUCC) на основі загальних критеріїв, призначена для продуктів інформаційно-комунікаційних технологій (ІКТ);
- схема сертифікації кібербезпеки для хмарних сервісів (EUCS);
- схема ЄС 5G для мережевих пристроїв та ідентифікації.

БРИТАНСЬКИЙ NCSC ЗАПУСКАЄ ОНЛАЙН ІНСТРУМЕНТИ КІБЕРБЕЗПЕКИ ДЛЯ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ

21 березня NCSC оголосив про запуск серії онлайн інструментів кібербезпеки, що орієнтовані на потреби малого та середнього бізнесу. Це прості системи самооцінки (наразі доступна перевірка безпеки браузера та IP адрес чи вебсайтів), а на підході перевірка безпеки електронних скриньок. NCSC підкреслює, що малий бізнес є традиційною мішенню для кіберзлочинців. Останнє урядове опитування про кіберзломи показало, що 38% малих підприємств Великобританії постраждали від кіберінцидентів протягом 12 місяців. А 20% малих підприємств вважають кіберзлочинність найвпливовішими як з точки зору витрат, так і з точки зору зриву їх діяльності.

БАЙДЕН ПІДПИСАВ УКАЗ, ЩО ОБМЕЖУЄ ВИКОРИСТАННЯ УРЯДОМ ДЕЯКИХ КОМЕРЦІЙНИХ ШПИГУНСЬКИХ ПРОГРАМ

Президент Джо Байден 27 березня підписав указ, спрямований на обмеження використання деяких видів таргетованого комерційного шпигунського програмного забезпечення урядом США через занепокоєння щодо загроз національній безпеці та конфіденційності.

Виконавчий наказ, який поширюється на всі агентства США, включаючи розвідувальну спільноту та правоохоронні органи, встановлює перелік факторів для оцінки типів шпигунського програмного забезпечення, яке має використовувати уряд США. Він забороняє використовувати шпигунське програмне забезпечення, яке використовувалося іноземним урядом для стеження за цивільними особами США, або якщо воно використовувалося іноземним урядом, залученим у порушеннях прав людини.

Ці кроки гарантують, що виконавчий наказ все одно дозволить уряду США використовувати деякі форми стеження, але, ймовірно, виключає використання технологій таких компаній, як суперечлива ізраїльська компанія NSO Group.

УРЯД ВЕЛИКОБРИТАНІЇ ОПУБЛІКУВАВ СВОЄ БАЧЕННЯ КІБЕРБЕЗПЕКИ НАЦІОНАЛЬНОЇ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я

Уряд Великої Британії опублікував нову стратегію, спрямовану на підвищення кіберстійкості в секторі охорони здоров'я та соціальної допомоги до 2030 року, стверджуючи, що вона є ключовою для побудови стійкої, орієнтованої на пацієнтів NHS.

Хоча деталі будуть готові лише влітку, уряд оприлюднив п'ять основних аспектів нової стратегії, розробленої для мінімізації кіберризику та покращення реагування на інциденти:

- визначте, де збій завдасть найбільшої шкоди пацієнтам, наприклад, збій у роботі критично важливих послуг;
- об'єднайте сектор, щоб скористатися перевагами масштабу, використовувати національні ресурси та досвід й прискорити реагування;
- переконайтеся, що лідери залучені, співробітники знають основи кібербезпеки та набирають більше спеціалістів із безпеки;
- вбудуйте засоби безпеки у нові технології, щоб краще захистити їх від кіберзагроз;
- підтримуйте кожну організацію охорони здоров'я та догляду, щоб мінімізувати вплив інцидентів і час відновлення.

В основі плану лежить Система оцінки кібербезпеки (CAF) Національного центру кібербезпеки (NCSC), яка сама по собі має чотири цілі: управляти ризиками, захистити від нападів, виявляти події безпеки й мінімізувати вплив інцидентів.

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

ЄВРОПЕЙСЬКА ПОЛІЦІЯ ТА ФБР ВИКРИЛИ МІЖНАРОДНУ КІБЕРЗЛОЧИННУ ГРУПУ

Німецька поліція 6 березня заявила, що зупинила діяльність пов'язаної з росією банди кіберзлочинців, яка роками шантажувала великі компанії та установи із застосуванням програм-вимагачів, отримуючи мільйони євро.

Працюючи з партнерами з правоохоронних органів, включаючи Європол, ФБР і владу в Україні, поліція Дюссельдорфу заявила, що їм вдалося ідентифікувати 11 осіб, пов'язаних з групою, яка діяла у різних формах принаймні з 2010 року.
Банда, яка ймовірно стоїть за програмою-вимагачем, відома як DoppelPaymer, пов'язана з російським синдикатом Evil Corp, який займався крадіжками з онлайн-банків задовго до того, як програми-вимагачі стали глобальним лихом.

США ПРОВОДЯТЬ КІБЕРОБОРОННУ МІСІЮ В АЛБАНІЇ

23 березня Кіберкомандування США оприлюднило дані про діяльність команди кібероператорів із Сил національної кібермісії США (CNMF) в Албанії. Після масштабних кібератак проти цієї країни у 2022 році, CNMF спільно з Албанією розгорнуло групу Hunt Forward для проведення заходів із захисту мережі разом із країною-партнером для виявлення, моніторингу та аналізу тактики, техніки та процедур противника.

Під час таких операцій американські оператори працюють поруч з колегами з приймаючої країни лише в тих мережах, які партнер визначив і надав доступ. З 2018 року CNMF розгортав такі місії 44 рази у 22 країнах і проводив пошукові операції у майже 70 мережах по всьому світу.

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

ЕКСПЕРТИ ІДЕНТИФІКУВАЛИ ПОВНОФУНКЦІОНАЛЬНИЙ INFO STEALER І TROJAN У ПАКЕТІ PYTHON НА PYPI

Як 2 березня повідомило видання The Hacker News, було виявлено, що шкідливий пакет Python, завантажений до індексу пакетів Python (PyPI), містить повнофункціональний троян для викрадення інформації та віддаленого доступу. Пакет під назвою colourfool ідентифікувала команда Kroll Cyber Threat Intelligence, а компанія назвала зловмисне програмне забезпечення Colour-Blind.

«Зловмисне програмне забезпечення Colour-Blind вказує на демократизацію кіберзлочинності, яка може призвести до посилення ландшафту загроз, оскільки численні варіанти можуть бути породжені з коду, отриманого від інших», – заявили дослідники Kroll Дейв Трумен і Джордж Гласс у звіті, опублікованому першого березня.

SYSUPDATE ВІД IRON TIGER ПОВЕРТАЄТЬСЯ І ТЕПЕР ВМІЄ ПРАЦЮВАТИ З LINUX

Другого березня видання The Tech Monitor повідомило, що підтримувані державою китайські хакери APT27, також відомі як Iron Tiger, розробили набір шкідливих програм під назвою SysUpdate. Він спрямований на пристрої, що працюють на операційній системі Linux.

Злочинці, які спеціалізуються на кібершпигунстві, є частиною китайського синдикату під назвою TiltedTemple, який атакує цілі по всій Європі. Попередні версії інструментарію зловмисного програмного забезпечення SysUpdate розроблені для ухилення від безпекового програмного забезпечення та протидії зворотному інжинірингу, і ця остання версія може бути небезпечнішою, ніж будь-коли, повідомляє Trend Micro у своєму звіті.

КИТАЙСЬКІ ХАКЕРИ АТАКУЮТЬ ЄВРОПЕЙСЬКІ ОРГАНІЗАЦІЇ ЗА ДОПОМОГОЮ НОВОГО БЕКДОРУ MQSTTANG – КОМПАНІЯ WE LIVE SECURITY

Як третього березня повідомило видання The Hacker News, актора Mustang Panda, що діє в інтересах Китаю, спостерігали за використанням досі небаченого спеціального бекдору під назвою MQsTTang у рамках кампанії соціальної інженерії, яка розпочалася в січні 2023 року.

Згідно зі звітом словацької компанії We Live Security, «на відміну від більшості зловмисних програм групи, MQsTTang, схоже, не базується на наявних сімействах або загальнодоступних проєктах».

Після повномасштабного вторгнення росії в Україну ланцюги атак, організовані групою, більш активно таргетують європейські політичні організації. Також було зафіксовано атаку на державну установу на Тайвані, що вказує на більшу увагу до Європи та Азії.

ЕСТОНСЬКА ВЛАДА ПОВІДОМИЛА, ЩО ПАРЛАМЕНТСЬКІ ВИБОРИ БУЛИ ПІД ПРИЦІЛОМ КІБЕРАТАК

Естонія успішно провела вибори 5 березня (де більшість голосувань відбувається онлайн), попри масштабні DDoS атаки російських зловмисників на виборчу інфраструктуру та інші державні служби. Як повідомила ЗМІ Прем'єр-міністрка Естонії Кая Каллас, попри те, що росіянам не вдалось зірвати вибори, можна було спостерігати очевидні ознаки того, що вони навчаються та намагаються адаптувати свої підходи.

ПЕНТАГОН ВВАЖАЄ ГІГАНТСЬКІ ВАНТАЖНІ КРАНИ КИТАЙСЬКОГО ВИРОБНИЦТВА МОЖЛИВИМ КИТАЙСЬКИМ ІНСТРУМЕНТОМ ШПИГУНСТВА

Уряд США стурбований тим, що китайські крани «судно-берег» можуть становити загрозу національній безпеці. Про це 5 березня повідомило видання Wall Street Journal. Крани, про які йде мова, виробляє китайська компанія ZPMC, яка, за словами американських чиновників, виробляє близько 80% кранів типу «судно-берег», що використовуються в портах США. Ці крани «містять складні датчики, які можуть реєструвати та відстежувати походження та призначення контейнерів. Це викликає занепокоєння, що Китай може отримати інформацію про матеріальні засоби, які відправляються в країну або вивозяться з неї для підтримки військових операцій США по всьому світу».

TRANSPARENT TRIBE ЗАМАНЮЄ ІНДІЙСЬКИХ І ПАКИСТАНСЬКИХ ЧИНОВНИКІВ

7 березня дослідники ESET повідомили, що виявили активну кампанію Transparent Tribe, орієнтовану в основному на користувачів Android з Індії та Пакистану, які, імовірно, пов'язані з військовою чи політичною сферою.

Жертви, ймовірно, стали мішенню через шахрайство на романтичному ґрунті, коли з ними спочатку зв'язувалися на іншій платформі, а потім переконували використовувати нібито «більш безпечні» програми, до встановлення яких потім спонукали. Швидше за все, активна з липня 2022 року кампанія поширювала бекдори CapraRAT через принаймні два вебсайти. Вони видавали себе за центри дистрибуції, представляючи їх як безпечні версії захищених програм обміну повідомленнями. Бекдор здатний робити знімки екрана та фотографії, записувати телефонні дзвінки та навколишнє аудіо, а також вилучати будь-яку іншу конфіденційну інформацію.

ЗЛАМ СЕРВІСУ МЕДИЧНОГО СТРАХУВАННЯ ПРИЗВІВ ДО ВИТОКУ КОНФІДЕНЦІЙНИХ ДАНИХ ЧЛЕНІВ КОНГРЕСУ ТА ПЕРСОНАЛУ

Порушення безпеки даних, пов'язане з платформою обміну медичними послугами у Вашингтоні, включає конфіденційну інформацію членів і співробітників Конгресу. Про це 9 березня повідомила законодавчому органу головний адміністративний директор Палати Кетрін Шпіндор.

Хакери стверджують, що серед викраденої інформації мають імена, ідентифікаційні номери, поліси, номери соціального страхування, назви страхових планів, роботодавців, адреси та багато іншого. Крім того, вони продають викрадені дані, що може призвести до збільшення випадків викрадення віртуальної особи, фінансових злочинів та фізичних погроз.

ФБР розслідує, які дані було викрадено. Зараз виглядає так, що дані конгресменів не були основною метою хакерів.

KASPERSKY ВИПУСТИВ ДЕШИФРУВАЛЬНИК ПРОГРАМ-ВИМАГАЧІВ НА ОСНОВІ ВИХІДНОГО КОДУ CONTI

16 березня компанія Kaspersky випустила дешифратор, який може допомогти жертвам, чиї дані були заблоковані однією з версій рансомвер Conti. Спеціалістам компанії вдалося отримати приватні ключі програми-вимагача, тобто інструменти, які надають жертвам рансомвер, щоб вони могли розблокувати свої файли.

«Наприкінці лютого 2023 року експерти Kaspersky виявили нову порцію витоку даних, опублікованих на форумах», – заявили в компанії. «Після аналізу даних, які містили 258 закритих ключів, вихідний код і деякі попередньо скомпільовані дешифратори, Kaspersky випустив нову версію загальнодоступного дешифратора, щоб допомогти жертвам цієї модифікації програми-вимагача Conti. Компанія також заявила, що лише у 14 з 257 проаналізованих ними кейсів, жертви атак рансомвер заплатили викуп.

РОСІЙСЬКІ ОПЕРАТОРИ ВИКОРИСТОВУЮТЬ ВРАЗЛИВІСТЬ OUTLOOK

Як 16 березня повідомило видання Cybersecurity Dive з посиланням на звіт Deep Instinct, APT28, Fancy Bear ГРУ, використав уразливість Outlook проти своїх цілей. Cybersecurity Dive повідомляє, що атаки з використанням експлойту застосовувалися проти організацій в Україні, Туреччині, Румунії та Польщі з квітня минулого року. Deep Instinct закликає користувачів вжити заходів, щоб убезпечити свої системи: «Оскільки атака не вимагає взаємодії з користувачем, ми закликаємо всіх, хто використовує програму Outlook, якомога швидше виправити свої системи. Ми також пропонуємо запустити сценарій PowerShell, наданий Microsoft, щоб заднім числом знаходити шкідливі електронні листи на сервері обміну».

КИТАЙСЬКІ ХАКЕРИ СКОРИСТАЛИСЬ ПОМИЛКОЮ FORTINET, ЩОБ ВИКРАДАТИ ДАНІ ВЕЛИКИХ ОРГАНІЗАЦІЙ

17 березня компанія Mandiant повідомила про те, що зловмисники з китайської UNC3886 використали критичну вразливість у FortiOS для того, щоб атакувати великі організації, викрасти їхні дані та спричинити пошкодження FortiOS або файлів.

«Складність експлойту свідчить про досвідченого зловмисного актора та про те, що він націлений на урядові чи пов'язані з урядом цілі», – відзначили у компанії Mandiant. На початку березня 2023 року Fortinet виправив цю вразливість.

FERRARI ПОВІДОМИЛО ПРО ІНЦИДЕНТ З RANSOMWARE

20 березня італійський виробник спортивних автомобілів Ferrari SpA заявив, що хакери вимагали від компанії викуп за контактні дані клієнтів. Представник зауважив, що злом не вплинув на діяльність компанії. Ferrari повідомили своїх клієнтів про потенційний доступ до їх даних і характер інциденту.

США СПІЙМАЛИ ТА ВИСУНУЛИ ЗВИНУВАЧЕННЯ КЕРІВНИКУ ХАКЕРСЬКОГО САЙТУ BREACHFORUMS

24 березня Міністерство юстиції США висунуло звинувачення засновнику BreachForums, великого підпільного вебсайту для комп'ютерних хакерів, який опублікував великі обсяги даних, викрадених з Twitter. Власником виявився 20-річний Конор Браян Фітцпатрік. Протягом останнього року BreachForums був одним із провідних хакерських сайтів темної мережі, віртуальним ринком, де люди купували, продавали та торгували викраденими даними.

APT УГРУПОВАННЯ WINTER VIVERN НАЦІЛИЛОСЯ НА ОФІЦІЙНИХ ОСІБ ІНДІЇ, ЛИТВИ, СЛОВАЧЧИНИ ТА ВАТИКАНУ

17 березня видання The Hacker News повідомило з посиланням на звіт SentinelOne, що APT, відому як Winter Vivern, пов'язали з кампаніями, з 2021 року населеними на урядовців в Індії, Литві, Словаччині та Ватикані.

Попередні публічні звіти, що описують групу, показують, що вона використовувала документи Microsoft Excel, що містять макроси XLM, для розгортання імплантів PowerShell на скомпрометованих хостах.

Хоча джерела загрози невідомі, схеми атак свідчать про те, що кластер пов'язаний з цілями, які підтримують інтереси урядів Білорусі та росії.

Winter Vivern, також відстежуваний як UAC-0114, привернув до себе увагу минулого місяця після того, як Група реагування на комп'ютерні надзвичайні ситуації України (CERT-UA) детально розповіла про нову кампанію зловмисного програмного забезпечення, націлену на державні органи України та Польщі з метою доставлення шкідливого програмного забезпечення під назвою Aperetif.

КИТАЙСЬКІ ТА РОСІЙСЬКІ ХАКЕРИ ВИКОРИСТОВУЮТЬ SILKLOADER, ЩОБ УНИКНУТИ ВИЯВЛЕННЯ

16 березня видання The Hacker News повідомило з посиланням на компанію WithSecure, що кластери загрозливої активності, пов'язані з екосистемами кіберзлочинців Китаю та росії, були виявлені у використанні нового шкідливого програмного забезпечення, призначеного для завантаження Cobalt Strike на заражені машини.

Зловмисне програмне забезпечення, яке фінська компанія з кібербезпеки WithSecure назвала SILKLOADER, використовує методи бокового завантаження DLL для доставлення комерційного програмного забезпечення для моделювання противника.

ПРОІРАНСЬКІ ХАКЕРИ ВСЕ ЧАСТІШЕ ВДАЮТЬ ІЗ СЕБЕ РЕПОРТЕРІВ АБИ ПРОНИКНУТИ У МЕРЕЖІ ЖЕРТВИ – WIRED

21 березня у виданні Wired вийшла стаття «Тактика випаленої землі кіберармії Ірану» присвячена діяльності хакерських груп (таких як TA453 і APT42), пов'язаних із Корпусом стражів ісламської революції. Автори вказують, що ці угрупування (які орієнтовані проти західних журналістів, науковців і експертів) все частіше використовують один і той самий метод соціальної інженерії – вони видають себе за журналістів, які хочуть взяти інтерв'ю, а в запитах на такі інтерв'ю вбудовують фішингові посилання. Щоб їх звернення виглядали правдивіше, спочатку вони компрометують акаунти справжніх журналістів, від імені яких ведуть комунікацію.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

BLACKMAMBA: ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ СТВОРЕННЯ ПОЛІМОРФНИХ ШКІДЛИВИХ ПРОГРАМ

Як зазначається у звіті HYAS Labs, опублікованому 7 березня, поява ChatGPT минулого року ознаменувала перший випадок, коли синтез коду нейронною мережею став вільно доступним для широкого загалу. Цей потужний і універсальний інструмент можна використовувати для всього: від відповідей на прості запитання до миттєвого написання письмових робіт або розробки оригінального програмного забезпечення, включно зі зловмисним – останнє з яких створює потенціал для нового небезпечного роду кіберзагроз.

У своєму звіті HYAS Labs представляє нову концепцію зловмисного програмного забезпечення кейлоггера BlackMamba, який використовує ШІ для створення поліморфного коду, який змінюється під час виконання, щоб уникнути виявлення.

МОЖЛИВОСТІ CHATGPT ДЛЯ ДОПОМОГИ У НАСТУПАЛЬНИХ КІБЕРДІЯХ ПЕРЕБІЛЬШЕНІ – TRELLIX

9 березня старший дослідник Trellix з наступальних засобів Джон Родрігез опублікував колонку, у якій оцінює поточні та перспективні можливості застосування таких AI систем як ChatGPT для написання коду, що може бути використаний зі зловмисною метою (в наступальних діях). Він вказує, що наразі такі системи неспроможні генерувати дійсно новаторські ідеї в цій сфері, а все що вони створюють на запити, є компіляцією зрозумілих та звичайних для безпекових продуктів рішень.

DEUTSCHE BAHN ПРОДОВЖУЄ СПІВПРАЦЮ З HUAWEI ЩОДО ЦИФРОВІЗАЦІЇ ЗАЛІЗНИЦІ, ПОПРИ ПРОБЛЕМИ БЕЗПЕКИ

10 березня агентство Reuters повідомило, що ще у грудні 2022 року оператор німецьких залізниць Deutsche Bahn уклав контракт на 64 млн євро на створення нової IP-мережі. Більшість обладнання в цій закупці буде виробництва Huawei.

Представник Deutsche Bahn у своєму коментарі відзначив, що не знає про існування нормативних документів, які б визначали IP-системи Deutsche Bahn як «критичних компонентів». Певні обмеження на використання обладнання китайських виробників є лише для телекомунікаційного сектору. Голова парламентського комітету, який наглядає за спеціальними службами, К. фон Нойтс зауважив, що «якщо це правда, що компанія робить ставку на китайське обладнання, то це викликає серйозне занепокоєння».

ПЕРЕГОВОРИ ПРО ВИКУП ПІД ЧАС КІБЕРАТАК НЕ Є ТАКИМИ ПРОСТИМИ

Оскільки атаки програм-вимагачів стають дедалі складнішими та витонченими, рішення платити чи не платити викуп також стає складнішим. Однак надзвичайно важливо бути готовим до переговорів із загрозливими суб'єктами, незалежно від того, чи ви в результаті вирішите заплатити. Адже переговори передбачають забезпечення найкращих можливих умов і досягнення сприятливого результату, попри вроджену ненадійність залучених зловмисників. У своєму коментарі, Віцепрезидент служби кібербезпеки Sygnia в Азійсько-тихоокеанському регіоні Гі Сегал (Guy Segal) зважує міркування, що стоять за рішення виплачувати чи не виплачувати викуп.

RANSOMWARE TRACKER: ОСТАННІ ЦИФРИ [БЕРЕЗЕНЬ 2023]

Сервіс з відслідковування атак вимагачів Ransomware tracker компанії Recorded Future оновлюється кожного десятого числа місяця та відображає дані за попередній місяць. Згідно з даними компанії, у лютому 2023 року зменшилася кількість атак на організації, що надають послуги у сфері охорони здоров'я, попри загальне зростання кількості атак. Протягом лютого програмами-вимагачами було атаковано шість постачальників медичних послуг – це найнижчий показник за місяць з січня 2020 року.

Для порівняння, кількість жертв у лютому 2022 року становила 17, а у лютому 2021 року постраждали 25 організацій охорони здоров'я.

В інших секторах справи склалися не так добре. У лютому було скоєно 11 нападів на державні та місцеві органи влади, у порівнянні з лише трьома нападами у попередньому місяці. Загалом протягом місяця групи вимагачів опублікували інформацію про 204 жертви на своїх сайтах, порівняно зі 163 у січні.

КОРПУС МОРСЬКОЇ ПІХОТИ США РОЗПОЧИНАЄ ПІДГОТОВКУ ВЛАСНИХ ПРОГРАМІСТІВ

14 березня Корпус морської піхоти США повідомив, що в Остіні створено і запущено трирічну пілотну програму підготовки морських піхотинців як розробників з метою швидкого створення застосунків для флоту. Передбачається, що морські піхотинці пройдуть річне навчання з розробки програмного забезпечення й отримають військово-професійну спеціальність розробника застосунків. Потім вони витратять два роки на розробку програмних рішень для Корпусу.

НОВА КІБЕРШПИГУНСЬКА ГРУПА YOROTROOPER ЗОСЕРЕДЖЕНА НА ЕНЕРГЕТИЧНОМУ СЕКТОРІ КРАЇН СНД – CISCO TALOS

14 березня кібербезпекова компанія Cisco Talos оприлюднила результати свого дослідження нової зловмисної групи YoroTrooper. За даними компанії це угрупування почало проводити свої операції з червня 2022 року і основні її зусилля спрямовані на державні та енергетичні організації в Азербайджані, Таджикистані, Киргизстані та інших країнах Співдружності Незалежних Держав. Під час успішних зламів викрадаються облікові дані з кількох програм, історія вебпереглядача, файли cookie, інформація про систему та знімки екрана.

MITRE ПРАЦЮЄ НАД НОВОЮ МАСШТАБНОЮ АРХІТЕКТУРОЮ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ОРГАНІЗАЦІЙ

15 березня аналітично-дослідницька компанія MITRE повідомила про те, що її спеціалісти (спільно з партнерськими організаціями серед університетів) працюють над проєктом Adaptive Cyber Resiliency. Його мета – створити налаштовану для будь-якої організації кібербезпекову архітектуру, застосування якої має дозволити організації продовжувати надавати свої послуги, навіть якщо зловмисник вже проник у мережі організації. За задумом MITRE ця архітектура має допомогти будь-якій організації оптимально спланувати заходи безпеки відповідно до різних видів загроз.

П'ЯТЬ ОСНОВНИХ ТЕНДЕНЦІЙ У СФЕРІ RANSOMWARE – PROOFPOINT

23 березня компанія Proofpoint опублікувала перелік з п'ять основних тенденцій щодо ситуації з розвитком ransomware у світі. Вони вказують на такі тенденції:

- через загальне посилення заходів кібербезпеки ransomware все частіше націлюється на OKI, які часто не мають можливостей швидко впроваджувати нові рішення;
- здирники все частіше намагаються отримати викуп декілька разів поспіль або окремо за розблокування даних та окремо за непоширення викрадених даних конкурентам;
- суми викупів стабілізувались, а подекуди – знижуються;
- зловмисники все частіше шукають інсайдерів в компаніях аби скомпрометувати їх;
- ransomware активно еволюціонує, шукаючи нові вразливості.

5. КРИТИЧНА ІНФРАСТРУКТУРА

УРЯД США ПОПЕРЕДИВ ПРО АТАКИ ПРОГРАМ-ВИМАГАЧІВ ROYAL НА КРИТИЧНУ ІНФРАСТРУКТУРУ

ФБР та CISA 2 березня опублікували спільний документ, у якому попередили вразливі організації про підвищену загрозу, яку становить програма-вимагач Royal.

Це вже друге попередження від уряду США щодо програм-вимагачів Royal за останні місяці. У грудні Міністерство охорони здоров'я та соціальних служб США (HHS) попередило лікарні та організації у секторі охорони здоров'я, що вони мають бути напоготові захищатися від атак програм-вимагачів Royal.

Хакери, які стоять за вимагачем Royal, сумно відомі тим, що вимагають непомірні викупи від своїх жертв, часто від одно до 11 мільйонів доларів США в біткойнах. До того ж програмне забезпечення Royal важче виявити, ніж інші штами.

КОМПАНІЯ WAGO ВИПРАВИЛА КРИТИЧНІ ВРАЗЛИВОСТІ, ЯКІ ДОЗВОЛЯЮТЬ ОТРИМАТИ ПОВНИЙ КОНТРОЛЬ НАД ЇЇ PLC

Шостого березня було повідомлено, що німецька компанія Wago, яка виготовляє численні засоби для автоматизації підприємств, випустив виправлення вразливості для кількох своїх програмованих логічних контролерів (PLC). Ці вразливості дозволяли потенційним зловмисникам отримати повний контроль над цільовим пристроєм. Вразливості було виявлено, серед іншого, у вебінтерфейсі керування, призначеному для адміністрування, введення в експлуатацію та оновлення пристроїв.

НОВА СТРАТЕГІЯ КІБЕРБЕЗПЕКИ США СПРЯМОВАНА НА ФОРМУВАННЯ ВІДПОВІДАЛЬНОЇ БЕЗПЕКИ – CSIS

Шостого березня спеціалістка аналітичного центру CSIS Емілі Гардінг оприлюднила аналіз нової Стратегії кібербезпеки США. У своєму аналізі вона зосереджується на одному з аспектів нової стратегії – підвищення відповідальності розробників ПЗ за безпеку їх продуктів.

На її думку, ситуація, коли інновації стояли в основі руху відходять, адже змінилась структура користування ПЗ. У перші роки розвитку програмування вплив програм на життя звичайної людини був мінімальний і не міг призвести до катастрофічних наслідків. Однак сьогодні кожен з нас залежить від належного і безпечного функціонування програм, які знаходяться, наприклад, на нашому мобільному телефоні. Нова стратегія вказує на необхідність ставитись до безпеки громадян відповідально, а не як до можливої опції продукту.

НЕЗВАЖАЮЧИ НА ПЛУТАНИНУ В МЕТОДОЛОГІЯХ ПІДРАХУНКУ, КІЛЬКІСТЬ ВРАЗЛИВОСТЕЙ ICS ЗРОСТАЄ – SECURITYWEEK

13 березня журналісти спеціалізованого видання SecurityWeek випустили власне невелике дослідження щодо наявної плутанини із різними звітами кібербезпекових компаній щодо кількості вразливостей ICS. Вони звернули увагу, що деякі звіти вказують на зростання кількості вразливостей, однак інші звіти демонструють протилежні тенденції.

В результаті дослідження вони з'ясували, що на ці цифри впливає обрана методологія дослідження і дані, які використовуються для обрахунку. З урахуванням уточнень методів підрахунку, тенденція залишається однозначною – кількість вразливостей ICS продовжує зростати.

CISA ОПРИЛЮДНИЛА ПОСІБНИК З ОЦІНКИ СТІЙКОСТІ МОРСЬКОГО ТРАНСПОРТУ

15 березня CISA спільно з Інженерним корпусом Армії США оприлюднили Посібник з оцінки стійкості морського транспорту для федеральних установ, локальних урядів, а також осіб, що приймають рішення у сфері підвищення стійкості критичної інфраструктури. MTS Guide надає структуру послідовного процесу оцінювання стійкості складних систем, які складають систему морського транспорту. Він також містить поради щодо процесу проведення консультацій між державними та приватними стейкхолдерами, і надає посилення на важливі ресурси, що можуть допомогти підтримати процес оцінки стійкості.

ОСНОВНІ ЗАГРОЗИ ПРОМИСЛОВОМУ СЕКТОРУ ВІД КІБЕРАТАК: ОГЛЯД ЗА 2022 РІК

16 березня компанія Security Intelligence опублікувала свій звіт про загрози промисловому сектору у 2022 році та базові кроки, до яких мають вдатись компанії аби зменшити їх.
До загроз віднесено:

- появу угрупувань, які орієнтовані на ICS системи;
- зростання кількості випадків ransomware проти промислових компаній;
- збільшення кількості крадіжок інтелектуальної власності;
- спроби саботажу обладнання через кібератаки на нього.

До першочергових кроків для зменшення загроз компанія відносить: уважне ставлення до GDPR, проведення оцінки відповідності рівня кіберзрілості організації по CMMC та впровадження системи оцінки безпеки промислових систем управління (ICS).

ОПУБЛІКОВАНО НАЙКРАЩІ ПРАКТИКИ ЩОДО КЕРУВАННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ ДЛЯ АДМІНІСТРАТОРІВ (IAM)

21 березня ESF Partners, NSA та CISA оприлюднили збірку найкращих практик щодо керування ідентифікацією та доступом для адміністраторів (IAM). Проблеми налаштувань IAM (в т.ч. збереження неактивних облікових записів і відсутність багатофакторної автентифікації) може створювати серйозні загрози для організацій. Приклад таких загроз – інцидент із Colonial Pipeline у 2021 році. У документі наведено найкращі практики та засоби пом'якшення для протидії загрозам IAM, пов'язаних із п'ятьма напрямами:

- управління ідентифікацією;
- посилення середовища;
- розподілена ідентифікація/єдиний вхід; багатофакторна автентифікація;
- IAM аудит і моніторинг.

МАЙЖЕ В КОЖНОМУ ОТ ПРОДУКТІ ВЕЛИКИХ КОМПАНІЙ Є ВРАЗЛИВОСТІ КІБЕРБЕЗПЕКИ – ДОСЛІДНИКИ БЕЗПЕКИ

23 березня три дослідники кібербезпеки опублікували препринт свого дослідницького матеріалу «Небезпечна конструкція в основі критичної інфраструктури». В ньому вони наводять результати свого дослідження більше ніж 50 продуктів ОТ (які використовуються в уряді, охороні здоров'я, водопостачанні, виробництві електроенергії, роздрібній торгівлі) від великих виробників, таких як Bently Nevada, Emerson, Honeywell, JTEKT, Motorola, Omron, Phoenix Contact, Siemens, Yokogawa та Schneider Electric. Майже у кожному були знайдені вразливості, а чимало продуктів використовують слабкий криптографічний захист у продуктах.

6. АНАЛІТИЧНІ ОЦІНКИ

CISA ОПРИЛЮДНИЛА РЕЗУЛЬТАТИ РОБОТИ ЇЇ RED TEAM ПРОТИ ОДНОГО З ОБ'ЄКТІВ OKI

Наприкінці лютого CISA поширила інформаційне повідомлення про одну з операцій її red team щодо великого територіально розподіленого OKI. Діяльність red team відбувалась на запит самої організації.

У інформаційному повідомлені підкреслено, що red team отримала постійний доступ до мережі організації, могла переміщуватись по численних територіально розділеним елементам організації та зрештою отримала доступ до систем, суміжних із конфіденційними бізнес-системами організації (SBS). Багатофакторна автентифікація (MFA) завадила команді отримати доступ до однієї з SBS, і команда не змогла завершити своє завдання – скомпрометувати другу SBS протягом періоду оцінювання.

Хоча рівень кіберзрілості OKI оцінювався як високий, організація не виявила активності red team протягом усього періоду оцінювання. За результатами підготовлено перелік заходів, до яких можуть вдатись OKI з метою запобігання таких вторгнень.

ПОБУДОВА СТІЙКОСТІ? ВПЛИВ ВИМОГ ЩОДО ІМУНІТЕТУ ДО ХМАРИ НА КІБЕРБЕЗПЕКУ, ЕКОНОМІКУ ТА ТОРГІВЛЮ

Німецький економіст і директор Європейського центру міжнародної політичної економії Матіас Бауер досліджує вплив вимог імунітету в запропонованій схемі сертифікації хмарних технологій ЄС на економіку і торгівлю.

Автор зазначає, що вимоги імунітету в EUCS ЄС ризикують відкрити скриньку Пандори, проклавши шлях для локалізації даних, обмежень на іноземну власність і вимог до місцевих установ у цифрових галузях у всьому світі, що призведе до зростання напруженості в торгівлі. Також вимоги підвищать ризики кібербезпеки для користувачів хмарних технологій і є дискримінаційними за своєю побудовою.

На його думку, постачальники з ЄС наразі не в змозі керувати широким переходом до хмари, а, отже, такі вимоги уповільнять значне підвищення ефективності та безпеки, яке можуть запропонувати поточні іноземні постачальники. Як наслідок, хмарна схема сертифікації ENISA має бути обмежена технічними вимогами та вимогами прозорості.

ЩО РОБИТИ У ВІДПОВІДЬ НА ІНЦИДЕНТИ З ВИКРАДЕННЯМ ДАНИХ

У статті, опублікованій CSO Online 2 березня, Ніл Вайнберг розглядає декілька прикладів реагування на атаки з викраденням даних з боку відомих компаній, які сталися протягом останніх років. Він підкреслює, що варто, а що не потрібно робити у подібних ситуаціях.

ІНФРАСТРУКТУРА ЗАРЯДКИ ЕЛЕКТРОМОБІЛІВ ВРАЗЛИВА ДО МОЖЛИВИХ КІБЕРАТАК

Як третього березня написало видання Dark Reading, у відповідь на те, що зловмисники вже раніше атакували станції для зарядки електромобілів, експерти закликають створити стандарти кібербезпеки, щоб захистити цей необхідний компонент електрифікованого майбутнього.

У лютому дослідники компанії Saiflow, що займається кібербезпекою енергетичних мереж, виявили дві вразливості в протоколі Open Charge Point Protocol (OCPP), які можна було використовувати для DDoS атак і для викрадення конфіденційної інформації. А Національна лабораторія штату Айдахо нещодавно виявила, що кожен зарядний пристрій, який вона перевірила, офіційніше відомий як обладнання для живлення електромобілів (EVSE), працює на застарілих версіях Linux.

Зважаючи на швидкий розвиток галузі й на те, що зарядні пристрої з одного боку є частиною інтернету речей, а іншого – частина операційних технологій, дослідники вважають, що держава має встановити для них стандарти кібербезпеки.

ПЛАН КІБЕРБЕЗПЕКИ БІЛОГО ДОМУ СУПЕРЕЧИТЬ РЕАЛЬНОСТІ SECOPS

Як стверджує авторка публікації на IT Operations Beth Pariseau, дослідження ринку свідчать про те, що багато IT-організацій все ще не впоралися із запровадженням базових найкращих практик SecOps. Це затьмарює перспективи заклику адміністрації Байдена радикально покращити стан кібербезпеки країни. Адже індустрія відчуває складнощі із запровадження менш жорстких вимог щодо безпеки.

Вона також критикує документ за відсутність детальної інформації щодо того, як організації можуть досягти поставлених цілей. А також федерального законодавства, яке Білий дім планує запропонувати Конгресу, і рівня фінансування, яке федеральний уряд готовий виділити на ці ініціативи.

ЛІБЕРАЛЬНИЙ СВІТОВИЙ КІБЕРПОРЯДОК У СТРАТЕГІЇ КІБЕРБЕЗПЕКИ США

Аналізуючи нещодавно прийняту США Стратегію кібербезпеки у статті, опублікованій War on the Rocks 13 березня, професор American University Джошуа Ровнер наголошує, що нова стратегія акцентує публічно-приватне партнерство, а також наголошує на необхідності підсилювати державне регулювання. Він також схвально відгукується про принцип Міністерства оборони «Defend Forward», який базується на ідеї, що найкращий спосіб покращити кібербезпеку – це пом'якшити загрози якомога ближче до точки їхнього походження.

Автор стверджує, що на відміну від позиції США у російсько-українській війні, де адміністрація Байдена демонструє стриманість, кіберпростір є «місцем ідеологічної конкуренції між великими державами-суперниками. Сполучені Штати та їхні демократичні союзники борються за підтримку вільного Інтернету та кіберекосистеми, яка заохочує торгівлю та захищає права людини. росія та Китай, навпаки, борються за демонтаж цієї системи, замінюючи ліберальні норми концепцією кіберсуверенітету, яка виправдовує політичне гноблення всередині країни та політичні маніпуляції за кордоном.

За словами автора, у цій боротьбі адміністрація Байдена не демонструє жодної стриманості, адже слова «стримування» та «ескалація» у документі взагалі не зустрічаються. Він також вітає намагання Білого дому запровадити методи оцінки ефективності прийнятої стратегії та пропонує декілька додаткових можливостей такого оцінювання.

NSA ВИПУСТИЛО НАСТАНОВИ, ЯКІ МАЮТЬ ДОПОМОГТИ У ВПРОВАДЖЕНІ ПОЛІТИКИ ZERO TRUST

14 березня NSA опублікувало інформаційний листок з кібербезпеки (CSI) під назвою «Підвищення зрілості zero trust по всій системі користувачів». Він має допомогти системним операторам розвинути можливості ідентифікації, облікових даних і керування доступом (ICAM), щоб ефективно пом'якшувати певні методи кіберзагроз. Впровадження моделі zero trust є частиною національної стратегії кібербезпеки США.

ШІСТЬ НЕБЕЗПЕК ДЛЯ СПЕЦІАЛІСТІВ З КІБЕРБЕЗПЕКИ ПРИ ПОБУДОВІ ДІЄВОЇ СТРАТЕГІЇ ЗАХИСТУ ОРГАНІЗАЦІЇ – NIST

20 березня спеціалістка NIST Джулі Хейні оприлюднила матеріал, у якому виділяє шість основних проблем, з якими стикаються фахівці з кібербезпеки, коли розробляють та впроваджують стратегію кібербезпеки у своїй організації. До таких ситуацій відносяться:

- вважати користувачів «нерозумними» (що призводить до відносин »ми – вони»);
- надмірне використання технічного жаргону, який не зрозумілий аудиторії;
- збільшення правил безпеки може призвести до неоднозначних спроб користувачів зробити їх «зручними» (наприклад, політика компанії щодо складних паролів може призвести до бажання користувачів використовувати один складний пароль всюди);
- «забагато безпеки»;
- брак «позитивних стимулів» до використання безпечних рішень на користь покарань;
- відсутність реального зворотного зв'язку на численні навчання кібербезпеці в організації.

ENISA ПУБЛІКУЄ СВІЙ ПЕРШИЙ ЗВІТ ПРО КІБЕРЗАГРОЗИ, ПРИСВЯЧЕНИЙ ТРАНСПОРТНОМУ СЕКТОРУ

21 березня ENISA оприлюднила звіт «Ландшафт загроз від ENISA: Сектор транспорту». Звіт містить аналіз кіберінцидентів, пов'язаних з авіаційним, морським, залізничним та автомобільним транспортом за період із січня 2021 року по жовтень 2022 року. У ньому зазначено оцінку суб'єктів загроз та аналіз їх мотивації. Лідерами серед загроз сектору є ransomware (кількість атак зросла майже вдвічі, з 13% у 2021 році до 25% у 2022 році), DDoS та атаки через ланцюги постачання.

ENISA підкреслює, що інформація про інциденти залишається обмеженою лише тими з них, про які офіційно повідомлено та інформацію про які було оприлюднено.

КІЛЬКІСТЬ ВИПАДКІВ КОМПРОМЕТАЦІЇ КОРПОРАТИВНОЇ ЕЛЕКТРОННОЇ ПОШТИ ЗРОСТАЄ – PROOFPOINT

23 березня компанія Proofpoint поширила статистку щодо одного з видів кіберзлочинної активності – компрометації корпоративної електронної пошти. Дослідники вказують, що стратегія зловмисників зосередитись на цьому сегменті була вдалою – минулого року компанії втратили понад 2,7 мільярда доларів через ці шахрайства. Це на 300 мільйонів доларів більше, ніж у 2021 році. Про небезпеку таких атак каже і наступний показник – фактичні втрати від таких атак для бізнесу у 80 вищі, ніж від ransomware.

КІБЕРСТІЙКІСТЬ США ПОТРЕБУЄ КРАЩОЇ КООРДИНАЦІЇ ВІДОМСТВ ТА ІНВЕСТИЦІЙ У СТІЙКІСТЬ, А НЕ СТВОРЕННЯ ЄДИНОГО КІБЕРБЕЗПЕКОВОГО МОНСТРА – CSIS

23 березня група експертів CSIS опублікували своє дослідження «Інновації для стійкості». Воно висвітлює низку тем, включаючи питання освіти працівників, кліматичних змін, захисту ланцюжків постачання та кібербезпеку.

В кібербезпековому розділі вони звертаються до низки проблемних питань, пов'язаних із забезпеченням стійкості критичної інфраструктури (в т.ч. спираючись на український досвід), але при цьому зосереджуючись на проблемах взаємодії різних кібербезпекових урядових структур в США. Один з їх основних висновків: хоча деякі фахівці закликають до створення однієї великої організації з кібербезпеки, однак це завдання може створити більше проблем, ніж дасть рішень. Наразі США більше потребують належної координації, ніж централізації.

РІК З МОМЕНТУ ПРИЙНЯТТЯ CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022 (CIRCIA): ОСНОВНІ РЕЗУЛЬТАТИ

24 березня заступник директора CISA Брендон Уолес опублікував статтю із підсумками першого року функціонування Закону про повідомлення щодо кіберінцидентів для критичної інфраструктури (CIRCIA). Він зауважує, що CISA обережно та вдумливо підходить до його імплементації, консультуючись з партнерами з приватного сектору.

На виконання закону було запущено Об'єднану робочу групу з програм-вимагачів (JRTF), запроваджено пілотну програму попередження про вразливості програм-вимагачів (RVWP). Також у фокусі постійної уваги Агенції стимулювання OKI повідомляти про інциденти не через примус, а через розуміння важливості цього.

ЗВІТ ПРО БЕЗПЕКУ ВЕББРАУЗЕРІВ ЗА 2023 РІК РОЗКРИВАЄ ОСНОВНІ РИЗИКИ ВЕБПЕРЕГЛЯДУ ТА СЛІПІ ЗОНИ

Перший щорічний звіт компанії LayerX щодо безпеки веббраузерів, опублікований на початку березня, містить такі висновки:

- Більша частина всіх браузерів у корпоративному секторі неправильно налаштовані. Хоча налаштований браузер майже неможливо скомпрометувати, вкрасти дані із неправильно налаштованих вебпереглядачів дуже легко.
- З кожних 10 SaaS-застосунків є некорпоративними тіньовими SaaS, і жодне рішення SaaS для безпеки не може впоратися з ризиками. Shadow SaaS і більше того тіньові ідентифікатори є джерелом номер один для втрати корпоративних даних. Жоден наявний інструмент захисту даних не має доступу або контролю над тим, що працівники можуть робити зі своїми особистими програмами.
- Зловмисники використовують методи обхідної атаки, які не можуть виявити ні інструменти безпеки електронної пошти, ні засоби безпеки мережі.
- Традиційні інструменти безпеки пропускають більша частина цих векторів атак у нульову годину, що робить цільові атаки на вебпереглядачі основною причиною зламу корпоративних даних.
- Більшість ризиків браузера можуть призвести до крадіжки особистих даних. Слабкі паролі, неправильні конфігурації та проблеми з безпекою SaaS – усе це циркулює навколо цифрової ідентифікації. Цей висновок окреслює головну болючу точку – цифрові ідентифікатори все ще є корпоративною ахіллесовою п'ятою.

НАСТУПАЛЬНІ КІБЕРОПЕРАЦІЇ І ВІДПОВІДАЛЬНЕ ВИКОРИСТАННЯ КІБЕРПОТУЖНОСТЕЙ

Старший радник з питань кібербезпеки у Міжнародному інституті стратегічних досліджень Маркус Віллетт розглядає виклики, які становлять наступальні кібероперації, та пропонує 8 принципів відповідального використання кіберпотужностей з боку держав.

Відповідальні держави:

1. Визнають, що наявне міжнародне право може бути ефективно застосоване до використання кібероперацій як у мирний час, так і під час війни, і демонструють це на практиці.
2. Співпрацюють з іншими щодо покращення колективної кібербезпеки.
3. Ретельно контролюють спосіб проведення наступальних кібероперацій.
4. Важають певні цілі забороненими для виведення з ладу та руйнівних наступальних кібероперацій, але залишаються реалістичними щодо параметрів, які вони використовують, враховуючи різні правові заборони, які застосовуються під час миру та війни.
5. Протидіють і контролюють поширення наступальних кіберспроможностей.
6. Є прозорими щодо того, як вони мінімізують ризик для глобальної кібербезпеки під час розвитку наступальних спроможностей.
7. Припиняють небезпечну недержавну наступальну кіберактивність, що походить з їхніх територій, і співпрацюють на міжнародному рівні для боротьби з недержавними кіберзагрозами.
8. Заохочують і беруть участь у громадських дебатах щодо відповідального використання кіберпотужності, включаючи власне використання агресивних кібероперацій.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

УКРАЇНСЬКІ КОМАНДИ ЗДОБУЛИ ПРИЗОВІ МІСЦЯ У NATO TIDE HACKATHON 2023

У TIDE Hackathon 2023 взяли участь понад сто кіберфахівців з 26 команд, які представляли 13 країн-членів і партнерів НАТО. Україну представляли переможці Національного оборонного хакатону 2022 – по дві команди з Департаменту кіберполіції Національної поліції України (First-C.O.P і NEXT-C.O.P) та від компанії SoftServe (Валькірія-1 і Валькірія-2). Також у змаганні брали участь дві команди Державної служби спеціального зв'язку та захисту інформації України (KRAB та SSSCIP LAB) та команда Військового інституту телекомунікацій та інформатизації імені Героїв Крут.

За результатами Хакатону команда «Валькірія-1» посіла перше місце у завданні зі створення дашборду для аналізу показників ефективності учасників навчання CWIX щодо їхнього прогресу у досягненні взаємосумісності. Друге місце у цьому завданні посіла команда ДССЗЗІ – KRAB. А команда з Військового інституту телекомунікацій отримала приз за найінноваційніше рішення за результатами розв'язання завдання із побудови концепції візуальної навігації для малих БПЛА.

СЕКРЕТАР НКЦК НАТАЛІЯ ТКАЧУК НА ФОРУМІ PHOENIX CHALLENGE ЗАКЛИКАЛА ЗАХІДНИХ ПАРТНЕРІВ ОБ'ЄДНАТИ ЗУСИЛЛЯ ДЛЯ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ

Керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України, секретар НКЦК Наталія Ткачук взяла участь у форумі Phoenix Challenge 2023, який відбувся у Лондоні 27 лютого – 3 березня цього року. Захід організований Офісом заступника міністра оборони США з питань політики та Міністерством оборони Великої Британії, і присвячений темі «Орієнтація на майбутнє конкуренції в інформаційному середовищі».

У своїй промові Н. Ткачук поділилася досвідом України щодо розбудови інформаційної стійкості в умовах війни. «Для нас важливо забезпечити реалізацію прав громадян на доступ до правдивої об'єктивної інформації, зокрема, на окупованих територіях. Держава вживає системних заходів не лише щодо протидії дезінформації та фейкам російської пропаганди, але й забезпечує стійкість технологічної компоненти інформаційної безпеки, функціонування зв'язку, об'єктів телекомунікацій та телерадіомовлення, зокрема, під час блекаутів та в умовах бойових дій», – зазначила вона.

Н.Ткачук наголосила, що українці відрізняються від росіян надзвичайно високим рівнем критичного мислення, та вже виробили певний імунітет від російської пропаганди. «Західний світ нарешті має усвідомити, що для країни-терориста права людини, загальносвітові та демократичні цінності не мають жодного значення, тож ми маємо бути готовими забезпечити протидію інформаційній війні в цих умовах».

ЗА ПЕРШИЙ МІСЯЦЬ РОБОТИ СИСТЕМИ PROTECTIVE DNS НА ПОНАД 30% ЗМЕНШИЛИСЬ ВТРАТИ УКРАЇНЦІВ ВІД ФІНАНСОВОГО ФІШИНГУ

На базі Національного координаційного центру кібербезпеки 14 березня 2023 року відбулася робоча зустріч щодо функціонування системи Protective DNS, призначеної для протидії фінансовому фішингу. Під час заходу розглядалися питання стосовно проміжних результатів та можливого вдосконалення роботи системи. В обговоренні взяли участь представники законодавчої та виконавчої гілок влади, банківського сектору, представники телеком-бізнесу та профільних асоціацій.

У лютому цього року в Україні було впроваджено систему Protective DNS. Вона забезпечує фільтрацію фішингових сайтів, таким чином перешкоджаючи діяльності кіберзлочинців, а українці отримали додатковий захист від шахраїв в Інтернеті. До системи вже приєдналися понад 320 українських провайдерів, які відповідально ставляться до безпеки своїх клієнтів. З-поміж них і найбільші гравці ринку – Kyivstar, lifecell, Vodafone, Укртелеком, Датагруп та Воля.

«За перший місяць роботи системи ми вже маємо суттєві результати – об'єм фішингового шахрайства в грошовому еквіваленті впав приблизно на 40–50%, а кількість звернень від ошуканих громадян – на 30–40%. Загалом це десятки або навіть сотні мільйонів гривень щомісяця, які українці не втратять завдяки роботі системи», – сказав керівник управління забезпечення діяльності НКЦК профільної служби Апарату РНБО України Сергій Прокопенко.

НКЦК РОЗПОЧАВ СПІВПРАЦЮ З МІЖНАРОДНОЮ КОМПАНІЄЮ «ІНТЕРНЕТ 2.0»

Національний координаційний центр кібербезпеки підписав меморандум про співпрацю з провідною організацією з кібербезпеки США та Австралії «Інтернет 2.0». Сторони домовилися про співробітництво у сфері кібербезпеки та проведення спільних навчальних тренінгів.

За сприяння Міністерства цифрової трансформації Україна стала першим у світі партнером «Інтернет 2.0» за межами країн розвідувального альянсу Five Eyes (FVEY), до якого входять Австралія, Канада, Нова Зеландія, Велика Британія та США. Компанія надаватиме свої технології та поділиться передовим досвідом для потреб кіберзахисту України. Також «Інтернет 2.0» відкрила офіс в Україні.

СБУ ВИКРИЛА СПРОБИ РОСІЙСЬКИХ СПЕЦСЛУЖБ ЗБИРАТИ РОЗВІДДАНІ В УКРАЇНІ «ВІД ІМЕНІ» ЗАКОРДОННИХ ЗМІ

Кіберфахівці Служби безпеки фіксують численні спроби спецслужб рф отримати розвідувальну інформацію в Україні під виглядом діяльності представників іноземних медіа. Для збору закритих відомостей ворог використовує спеціалізовані інтернет-платформи та професійні онлайн-форуми українських журналістів. На цих ресурсах окупанти розміщують інформаційні запити нібито від працівників відомих закордонних ЗМІ.

У своїх повідомленнях вони звертаються до медійників та інших учасників профільних груп щодо отримання матеріалів начебто для підготовки «сюжетів» або «документальних фільмів» про війну в Україні. Насамперед ворога цікавлять відомості про результати російських ракетних ударів по українських містах, у тому числі локації «прильотів» та їхні наслідки.

У разі надання відповідних медіафайлів або текстових повідомлень автори «оголошень» обіцяють «гонорар». Отримана таким чином інформація потрібна агресору для коригування повторних повітряних атак на українські об'єкти.

СБУ ВИКРИЛА ШАХРАЇВ, ЯКІ «ВІД ІМЕНІ» МІСЦЕВОЇ ВЛАДИ «ЗБИРАЛИ» ГРОШІ ДЛЯ ЗСУ

Кіберфахівці СБУ викрили злочинну організацію, яка займалася видурюванням грошей з українських бізнесменів. Шахраї представлялися чиновниками місцевої влади та просили в підприємців «допомоги для ЗСУ». За наявною інформацією, їм вдалося привласнити понад 3 млн грн.

Як встановило слідство, злочинну схему організував громадянин однієї з країн Центральної Азії, який наразі перебуває на тимчасово окупованій частині Луганщини. До протиправної діяльності він залучив ще дев'ятьох спільників зі столичного регіону і півдня України.

Через власні зв'язки вони підшукували представників компаній, які працюють в умовах воєнного стану, і встановлювали контактні дані їхніх керівників. Після цього розсилали їм фейкові листи від імені голів обласних, міських та районних військових адміністрацій. У них – просили перерахувати на ЗСУ від 20 до 100 тисяч грн. Сума залежала від оборотів підприємства.

ДЕРЖСПЕЦЗВ'ЯЗКУ ПРОВЕЛА ВОРКШОП ІЗ КУЛЬТУРИ КІБЕРБЕЗПЕКИ ДЛЯ ФАХІВЦІВ З УПРАВЛІННЯ ПЕРСОНАЛОМ У ДЕРЖАВНОМУ СЕКТОРІ

Для допомоги державному сектору України посилити кіберстійкість та сприяти розвитку обізнаності держслужбовців у питаннях кіберзахисту Держспецзв'язку за підтримки Національного агентства з питань державної служби, Вищої школи публічного управління та проєкту EU4PAR провела воркшоп із культури кібербезпеки для фахівців з управління персоналом на державній службі. У заході взяли участь близько 50 фахівців.

«Фахівці з людських ресурсів відіграють одну з ключових ролей у запровадженні культури кібербезпеки в установі водночас із фахівцями з інформаційної безпеки та комунікацій. Ці люди мають відповідні навички з поширення культури в установі, мають повноваження та інструменти, які допоможуть їм у цьому. Тому я закликаю всі установи – як державного сектору, критичної інфраструктури, так і всі інші компанії – залучати відповідних фахівців для того, щоб посилювати власний кіберзахист», – зазначив заступник голови Держспецзв'язку Олександр Потій.

RUSSIA'S CYBER TACTICS: LESSONS LEARNED 2022 – АНАЛІТИЧНИЙ ЗВІТ ДЕРЖСПЕЦЗВ'ЯЗКУ ПРО РІК ПОВНОМАСШТАБНОЇ КІБЕРВІЙНИ РОСІЇ ПРОТИ УКРАЇНИ

Держспецзв'язку підготувала аналітичний звіт про кіберагресію росії проти України у 2022 році russia's Cyber Tactics: Lessons Learned 2022. У звіті досліджено основні угрупування, їхню мотивацію, методи та інструменти атак. Ці знання допоможуть у побудові ефективних систем захисту як в українських установах, так і в організаціях по всьому світу.

Цей звіт орієнтований на всіх, чия діяльність так чи інакше пов'язана з кібербезпекою:

- топменеджерів органів влади України;
- спеціалістів з інформаційної безпеки операторів критичної та критичної інформаційної інфраструктури та компаній, які надають послуги їм;
- вендорів, що створюють продукти з кібербезпеки;
- партнерів України по всьому світу.

На основі проведеного дослідження можна говорити про основні тенденції російської кіберзагрози.

ДЕРЖСПЕЦЗВ'ЯЗКУ ПОСИЛЮЄ СПІВПРАЦЮ З ВИЩИМИ НАВЧАЛЬНИМИ ЗАКЛАДАМИ УКРАЇНИ

Державна служба спеціального зв'язку та захисту інформації України підписала меморандуми про співпрацю із Західноукраїнським національним університетом та з Тернопільським національним технічним університетом імені Івана Пулюя. Меморандуми передбачають залучення фахівців Служби до проведення лекцій, кібернавчань, тренінгів та інших заходів для студентів та викладачів ВНЗ, взаємодію у сфері захисту інформації та кіберзахисту тощо.

«Україна дедалі потребуватиме все більше висококваліфікованих фахівців у сферах інформаційної та кібербезпеки, здатних ефективно та швидко реагувати на кіберзагрози та протистояти їм, зміцнювати кіберстійкість державних органів, об'єктів критичної інфраструктури та інших установ. Тож посилення кадрового потенціалу у сфері кібербезпеки – один із пріоритетів Держспецзв'язку. Надзвичайно важливо, щоб студенти вже під час навчання здобували необхідні та актуальні для майбутньої роботи знання та набували відповідних навичок», – зазначає заступник голови Держспецзв'язку Олександр Потій.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ УКРАЇНЦІВ ЗАЛИШАЄТЬСЯ ОДНИМ ІЗ НАЙБІЛЬШИХ ВИКЛИКІВ У КІБЕРВІЙНІ РОСІЇ ПРОТИ УКРАЇНИ

Під час війни проти нашої країни російські хакери намагаються викрасти будь-яку інформацію щодо осіб, які служили або служать в установах сектору безпеки та оборони України. Про це йдеться у звіті Держспецзв'язку Russia's Cyber Tactics: Lessons Learned 2022. Зловмисники полювали на інформацію про мобілізаційні плани, ротації, підвищення по службі тощо. Ці дані могли бути використані російськими спецслужбами на тимчасово окупованих територіях для репресивних дій проти українців, які там перебувають.

Таким прикладом є угрупування Armageddon / Gamaredon (відстежується CERT-UA за ідентифікатором за UAC-0010), хакери якого полюють за привілейованим / необмеженим доступом до баз даних / каталогів / соціальних реєстрів Національної поліції, оскільки поліція зберігає та обробляє інформацію про автомобілі, рух, камери, дорожні ситуації, арешти тощо. Ці дані можуть бути використані спецслужбами рф також для полювання на конкретних осіб, провокацій та диверсій.

У 2022 РОЦІ GAMAREDON ЗДІЙСНИВ 74 КІБЕРАТАКИ НА УКРАЇНУ

До Gamaredon належать хакери ялтинського підрозділу фсб – колишні співробітники СБУ, які зрадили свою Батьківщину та перейшли на бік ворога. Минулого року не було жодного тижня, коли б CERT-UA не реєстрував діяльності цього угруповання. Основною метою Gamaredon є шпигунство. Відмінною рисою фішингових розсилань угруповання є високий рівень їхньої підготовки: знання українського контексту та розуміння специфіки роботи тих чи інших організацій.

Це угруповання атакує державний сектор, державні підприємства та сектор безпеки й оборони. Однією з головних цілей у секторі безпеки та оборони є Нацполіція. Хакери Gamaredon намагаються дістати доступ до всіх можливих баз даних і видобути максимум інформації про машини, їх пересування, камери спостереження, ситуацію на дорогах, арешт тощо.

Крім того, основними цілями Gamaredon у другому півріччі 2022 були:

- Облікові дані співробітників Служби безпеки України в месенджері Signal з метою отримання доступу до акаунтів для викрадання даних та деанонімізація користувачів.
- Атаки на систему зв'язку Державної прикордонної служби України та систему «Шлях», за допомогою якої прикордонники перевіряють осіб, які перетинають державний кордон України.
- Фішинг на Міністерство оборони України.
- Оборонні підрядники та виробники.

Gamaredon активно використовує для атак інфраструктуру кримського телеком-хостингу провайдера CrymCom.

РОСІЙСЬКІ ХАКЕРИ РОЗПОВСЮДЖУЮТЬ ЗАРАЖЕНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЧЕРЕЗ ТОРЕНТИ

Держспецзв'язку попереджає: завантаження зламаного програмного забезпечення – небезпечне. Зазвичай таке ПЗ розповсюджується за допомогою торент-трекерів, чим активно користуються зловмисники, в тому числі російські спецслужби, які додають до зламаного ПЗ шкідливий код.

Хакери троянізують ISO та установчі файли й розміщують їх у безплатному доступі на торент-трекерах. Якщо жертва завантажує та встановлює такі файли на свій комп'ютер, хакери дістають доступ до його вмісту і можуть протягом тривалого часу залишатися непомітними.

У багатьох постраждянських країнах системні адміністратори й досі використовують неліцензійне програмне забезпечення (в тому числі операційні системи) в установах та компаніях різних форм власності, що розповсюджується за допомогою торент-трекерів. Встановлюючи зламане ПЗ із торентів, вони фактично надають доступ російським спецслужбам до вмісту робочих машин. Особливо небезпечним є використання зламаної операційної системи, адже в такому випадку зловмисники мають повний адміністративний доступ до комп'ютера, на якому її встановлено.

Пересічні українські користувачі також перебувають у зоні ризику, встановлюючи неліцензійне програмне забезпечення з неофіційних джерел, торентів зокрема.

ЦИФРОВА ТРАНСФОРМАЦІЯ ТА КІБЕРБЕЗПЕКА: ЄВРОПЕЙСЬКІ ПАРТНЕРИ ПІДТРИМУЮТЬ УКРАЇНУ

Команда естонської Академії електронного управління, Представництво ЄС в Україні, представники Мінцифри та Держспецзв'язку взяли участь у заході «Збережемо цифрову Україну», який відбувся 16 березня у Києві.

Під час зустрічі презентували масштабну європейську програму DT4UA, серед завдань якої – розвиток в Україні електронних публічних послуг, вдосконалення обміну даними між реєстрами та держустановами тощо. А також зосередили увагу на питаннях підтримки Європейського Союзу у зміцненні кібербезпеки в Україні.

Заступник голови Держспецзв'язку Олександр Потій під час заходу наголосив на важливості співпраці міжнародною спільнотою, зокрема для посилення захисту від кіберзагроз, та подякував європейським партнерам за допомогу.

КІБЕРБЕЗПЕКА ТА ЦИФРОВІ ВАЛЮТИ – НОВІ ТРЕНДИ У СФЕРІ GOVTECH

Kreston Ukraine за підтримки Міністерства цифрової трансформації України, Міністерства економіки України, Офісу реформ Кабінету Міністрів України та ISE Corporate Accelerator представили результати дослідження The global market of Govtech solutions станом на лютий 2023 року.

Дослідження містить загальну інформацію про Govtech індустрію, ключові компанії, інвесторів, регіональні особливості індустрії та здобутки України.

Головні тренди в Govtech станом 2023 за результатами дослідження:

- Гіперавтоматизація. За даними Gartner, протягом наступних трьох років 75% урядів матимуть щонайменше три ініціативи з упровадження гіперавтоматизації.
- Модернізація державної IT-інфраструктури для підвищення ефективності роботи.
- Кібербезпека. Державні установи повинні підтримувати безпеку та довіру громадян у цифровому просторі.
- Цифрові валюти. Використання криптовалют підвищить операційну ефективність та допоможе боротися з корупцією.
- Цифрова ідентифікація. Деякі країни вже мають простий процес ідентифікації та запровадили цифрові посвідчення особи, які іноді містять біометричну верифікацію.
- Технології штучного інтелекту для взаємодії з громадянами. Уряди все частіше використовуватимуть застосунки на основі штучного інтелекту для автоматизації державних послуг.

Більше про результати дослідження The global market of Govtech solutions — Govtech 20230224.pdf

КІБЕРПОЛІЦІЯ СТАЛА ПАРТНЕРОМ ПРОЄКТУ З ВИЯВЛЕННЯ КРИПТОГАМАНЦІВ, ПОВ'ЯЗАНИХ ІЗ ТЕРОРИСТИЧНОЮ ТА ПІДСАНКЦІЙНОЮ ДІЯЛЬНІСТЮ

В рамках ініціативи Scamfari кіберполіція буде виявляти та блокувати віртуальні активи зловмисників. Співпраця відбуватиметься в рамках підписаного меморандуму.

Проєкт передбачає спільну роботу над встановленням адрес криптогаманців, на які збирають «донати» для підтримки військової агресії рф проти України, й подальшим блокуванням таких активів.

Крім цього, Scamfari пропонує фінансову винагороду користувачам, які нададуть адресу криптогаманця та докази причетності його власників до протиправної діяльності. Дізнатися більше про проєкт можна за посиланням: https://osint.scamfari.com/

КІБЕРПОЛІЦІЯ ВИКРИЛА ЖИТЕЛЯ ХМЕЛЬНИЧЧИНИ У СТВОРЕННІ «ВІРУСУ» ДЛЯ ВИКРАДЕННЯ ДАНИХ КОРИСТУВАЧІВ

25-річного правопорушника викрили співробітники відділу протидії кіберзлочинам Хмельниччини спільно зі слідчим управлінням обласної поліції та обласним управлінням СБУ.

Чоловік розробив вірусне програмне забезпечення, яке позиціонував як додатки до комп'ютерних ігор. Потрапивши на пристрої користувачів, програма давала можливість завантажувати та відвантажувати файли, встановлювати й видаляти програми, робити скриншоти з віддаленого екрана, перехоплювати звук з мікрофона і відео з вбудованих або зовнішніх камер. Зібравши певні дані, зловмисник опрацьовував їх для подальшого викрадення облікових записів або виведення електронних коштів, які містилися на балансі таких акаунтів.

Встановлено, що зловмисник отримав доступ до більш як 10 тисяч комп'ютерів.
На момент проведення обшуку «під контролем» фігуранта перебувало майже 600 заражених комп'ютерів, до яких він міг приєднатися в реальному часі.

Відкрито кримінальне провадження за ч. 5 ст. 361 (Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж) Кримінального кодексу України. Санкція статті передбачає від десяти до п'ятнадцяти років позбавлення волі. Слідчі дії тривають.

КІБЕРПОЛІЦЕЙСЬКІ ПОКРАЩИЛИ НАВИЧКИ З ВИЯВЛЕННЯ ЗЛОЧИНІВ, ВЧИНЕНИХ З ВИКОРИСТАННЯМ ВІРТУАЛЬНИХ АКТИВІВ

Навчальний онлайн-семінар для українських правоохоронців організували представники світової блокчейн-екосистеми та постачальника криптовалютної інфраструктури Binance. Ініціатива спрямована на боротьбу з відмиванням злочинних доходів та фінансуванням тероризму.

Програма навчання включала матеріали правового та нормативного середовища, а також детальну інформацію про політику Binance щодо боротьби з відмиванням грошей та методи розслідування, розроблені компанією для виявлення та запобігання потенційним шахрайствам. Кіберполіцейські поглибили свої знання з питань блокчейн-технологій, криптовалют і методів боротьби з фінансовими та кіберзлочинами.

КІБЕРПОЛІЦІЯ ВИКРИЛА УЧАСНИКА ХАКЕРСЬКОЇ ГРУПИ, ПРИЧЕТНОЇ ДО АТАК ВІРУСОМ-ВИМАГАЧЕМ І ЗАВДАННЯ ЄВРОПЕЙСЬКИМ КОМПАНІЯМ 40 МЛН ЄВРО ЗБИТКІВ

Учасника угруповання встановили співробітники київського управління протидії кіберзлочинам спільно з Головним слідчим управлінням Нацполіції, працівниками Офісу Генерального прокурора та у співпраці з правоохоронцями Німеччини, Нідерландів, Федерального бюро розслідувань та за підтримки Європолу.

39-річний громадянин України, який наразі мешкає у Німеччині, причетний до масштабних кібератак з використанням програми-вимагача DoppelPaymer. Атаки цим «вірусом» стали можливими завдяки поширеному шкідливому програмному забезпеченню EMOTET. Програму-вимагач розповсюджували різними каналами, зокрема через фішингові та спам-розсилки з прикріпленими документами, що містили шкідливий код - JavaScript або VBScript. Потрапивши на техніку, шкідлива програма криптувала дані, а за відновлення доступу зловмисники вимагали викуп.

Серед потерпілих - майже чотири десятки європейських компаній, об'єктів критичної інфраструктури і промисловості. Загальна сума збитків сягає 40 мільйонів євро.

КОМАНДА КІБЕРПОЛІЦІЇ УВІЙШЛА В П'ЯТІРКУ ЛІДЕРІВ НА NATO TIDE HACKATHON 2023

Журі відзначило рішення українських поліцейських щодо розробки концепції візуальної навігації малого безпілотного літального апарату як одне з кращих. Серед запропонованих для вирішення тем кіберполіцейські обрали «Створення концепту та інструменту для вивчення дезінформації» та «Розробка концепції візуальної навігації малого безпілотного літального апарату».

За результатами розв'язання завдань правоохоронці розробили два концептуальних описи рішень та один робочий прототип програмного забезпечення. Досягнення команди кіберполіції були представлені журі та увійшли в п'ятірку кращих рішень за напрямом розробки концепції візуальної навігації малого безпілотного літального апарату.

Під час участі у заході кіберполіцейські удосконалили знання та навички, отриманий досвід буде корисним для побудови нових програмних рішень, зокрема для протидії дезінформації та розслідування кіберзлочинів.

КІБЕРПОЛІЦІЯ ВИКРИЛА ЗЛОЧИННУ ГРУПУ, ЯКА ОФОРМЛЮВАЛА КРЕДИТИ НА ЗНИКЛИХ БЕЗВІСТИ І ПОЛОНЕНИХ ВІЙСЬКОВОСЛУЖБОВЦІВ

Для реалізації злочинної схеми зловмисники здійснювали перевипуск SIM-карт та отримували доступ до онлайн-банкінгу. Далі оформлювали кредитні картки та привласнювали позики. Загальна сума збитків становить понад 2 мільйони гривень.

Організовану злочинну групу викрили співробітники Департаменту кіберполіції спільно зі слідчим управлінням поліції Київщини, СБУ, працівниками служб безпеки Приватбанку, Монобанку, Сенсбанку та за процесуального керівництва обласної прокуратури.

Встановлено, що троє осіб отримували дані про мобільні номери військовослужбовців, із якими втратили зв'язок рідні або тих, хто наразі перебуває у полоні. Зловмисники здійснювали перевипуск SIM-карт і перевіряли, чи є перевипущені номери фінансовими. Далі отримували доступ до онлайн-банкінгу. З рахунків захисників перераховували залишок грошей, а також випускали кредитні карти й привласнювали суми позики.

За попередніми даними, угрупованню вдалося отримати доступ до мобільних номерів понад 20 військовослужбовців, які знаходяться в полоні або зникли безвісти. Загальна сума збитків становить понад 2 мільйони гривень.

У НКЦК ВІДБУЛОСЯ НАВЧАННЯ З КІБЕРБЕЗПЕКИ ТА КІБЕРРОЗВІДКИ ДЛЯ ФАХІВЦІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ

Національний координаційний центр кібербезпеки при РНБО України та Міністерство цифрової трансформації України за підтримки Фонду цивільних досліджень та розвитку США (CRDF Global) та Державного департаменту США організував дводенний тренінг з кібербезпеки та кіберрозвідки для фахівців сектору безпеки і оборони на тему «Кібербезпека, управління кіберінцидентами/кіберзагрозами та кіберрозвідка».

Навчання у рамках підписаного меморандуму про співпрацю між НКЦК та міжнародною компанією з кібербезпеки США та Австралії «Інтернет 2.0» провели представники цієї провідної організації у сфері кібербезпеки. У тренінгу взяли участь понад 40 представників сектору безпеки і оборони.

З-поміж основних тем, які опановували учасники тренінгу: новітні методи та технології у сфері кібербезпеки, включаючи виявлення та реагування на загрози, захист даних та управління інцидентами, збір розвідданих та аналіз документів. Також учасники заходу мали змогу на практиці відпрацювати отримані навички.

НКЦК ПРАЦЮЄ НАД УДОСКОНАЛЕННЯМ НОРМАТИВНО-ПРАВОВОЇ БАЗИ У СФЕРІ КІБЕРБЕЗПЕКИ

Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України спільно з Національною Академією Служби безпеки України та Інститутом інформації, безпеки і права Національної академії правових наук України за сприяння Верховної Ради України та Інституту дослідження кібервійни провели науково-практичний семінар на тему: «Організаційно-правові засади розвитку системи забезпечення кібербезпеки України».

У заході також взяли участь представники Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України, Національної поліції України та Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

«За останні роки в Україні вперше було створено мінімально необхідну нормативно-правову базу з кібербезпеки. Ухвалено другу редакцію Стратегії кібербезпеки України та відповідні положення, які закріплені в указах Президента, постановах уряду та ухвалених законах. Зроблено перші кроки, і ми маємо і надалі системно підходити до питання удосконалення нормативно-правової бази з урахуванням набутого досвіду в першій у світі кібервійні», – сказав заступник Секретаря РНБО України Сергій Демедюк.

Керівник служби з питань інформаційної безпеки та кібербезпеки Апарату Ради національної безпеки і оборони України, секретар НКЦК Наталія Ткачук зазначила, що зараз вперше НКЦК, основні суб'єкти національної системи кібербезпеки, Верховна Рада України, наукові інституції та приватний сектор працюють єдиним фронтом. «Сьогодні не лише ми вивчаємо міжнародний досвід щодо нормотворення, але й наші міжнародні партнери прагнуть вивчати досвід України. І основна тема, до якої зараз прикута увага – це законодавче унормування створення в Україні кібервійськ, що є для нас надпріоритетним завданням», – сказала керівник служби.

Учасники заходу обговорили проблемні питання правового регулювання кібербезпеки України. Напрацьовані пропозиції будуть використані під час нормотворчої роботи, яка здійснюється Комітетом Верховної Ради України з питань національної безпеки, оборони та розвідки, до компетенції якого належать питання кібербезпеки.

УКРАЇНА ПРАЦЮЄ НАД ТЕХНОЛОГІЧНИМИ РІШЕННЯМИ РАЗОМ З ЄВРОПЕЙСЬКИМИ ПАРТНЕРАМИ

Заступник голови Держспецзв'язку Віктор Жора та заступник міністра з питань євроінтеграції Міністерства цифрової трансформації України Валерія Іонан зустрілися з Полом Хофхайнзом (Paul Hofheinz), президентом і співзасновником Лісабонської ради – відомого аналітичного центру та політичної мережі, яка об'єднує експертів, громадських діячів з усієї Європи.

Під час зустрічі обговорили перспективні напрями подальшої співпраці. Окрім того, Віктор Жора розповів про перебіг першої у світі кібервійни, яку веде росія. Особливу увагу заступник очільника Держспецзв'язку звернув на здобутки Служби у протистоянні загрозам з боку російських хакерів та обмін інформацією між Україною та іншими державами щодо відбиття кібератак. Він підкреслив, що український досвід протистояння російській кіберагресії є важливим для країн-партнерів.

Також Віктор Жора наголосив на необхідності посилення спільної міжнародної роботи з метою формування нових, більш ефективних підходів до протидії кіберзлочинності та захисту інформаційних систем.

КМУ УХВАЛИВ ПОСТАНОВУ, ЯКА УНОРМОВУЄ ВПРОВАДЖЕННЯ НЕЗАЛЕЖНОГО АУДИТУ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Уряд ухвалив постанову «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури» та затвердив Порядок проведення такого аудиту.

Порядок передбачає обов'язкове проведення аудиту інформаційної безпеки раз на два роки для об'єктів критичної інфраструктури I та II категорії критичності та раз на три роки для об'єктів III категорії критичності. При цьому, в разі настання кризової ситуації на об'єкті критичної інфраструктури, проведення аудиту проводять невідкладно.

Проведення аудиту забезпечують оператори критичної інфраструктури. При цьому вони зможуть самостійно обирати аудиторів, які узгоджуватимуть з операторами критерії оцінки захищеності інформації, програму, процедури та методики проведення незалежного аудиту.

За результатами проведення аудиту інформаційної безпеки аудитори у звітах надаватимуть рекомендації щодо усунення виявлених недоліків у системах інформаційної безпеки.

Держспецзв'язку забезпечить проведення аналізу звітів за результатами незалежного аудиту інформаційної безпеки та надання узагальненої інформації до РНБО України та КМУ.

КІБЕРАТАКИ НА УКРАЇНУ: ЗА ДОПОМОГОЮ ХАКЕРІВ РОСІЯ НАМАГАЄТЬСЯ ОТРИМАТИ БУДЬ-ЯКУ ІНФОРМАЦІЮ, ЯКА МОЖЕ ДАТИ ЇЙ ПЕРЕВАГУ В КОНВЕНЦІЙНІЙ ВІЙНІ

У січні–лютому 2023 року Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Держспецзв'язку, опрацювала понад 300 кіберінцидентів та кібератак. Це майже вдвічі менше, ніж у відповідний період торік, коли росія готувалася до повномасштабного вторгнення й активність хакерів була аномально високою.

Як зазначають фахівці, у січні 2023 року активність кіберзловмисників була дещо знижена. Це, ймовірно, може бути пов'язане з періодом новорічних свят у ворога. Проте у лютому хакери повернулись до звичного рівня активності.

Від початку цього року CERT-UA фіксує зростання кількості атак з метою шпигунства з акцентом на утриманні постійного доступу до організації. І навіть серед шкідливого програмного забезпечення, яке поширюють російські хакери, переважають програми для збору даних та віддаленого доступу до пристроїв користувачів. Це може бути однією з ознак того, що росія готується до тривалої війни. За допомогою хакерів вона намагається отримати будь-яку інформацію, яка може дати перевагу в конвенційній війні проти нашої країни: від даних щодо мобілізації – до розкриття секретів логістики західної зброї.

СБУ ВИКРИЛА НА ХМЕЛЬНИЧЧИНІ ВОРОЖУ БОТОФЕРМУ, ЧЕРЕЗ ЯКУ «РОЗГАНЯЛИ» ФЕЙКИ ПРО ВІЙНУ В УКРАЇНІ

Кіберфахівці Служби безпеки ліквідували прокремлівську ботоферму у Хмельницькій області. Понад дві тисячі ботів «розганяли» дезінформацію про ситуацію на фронті та закликали українців ухилятися від мобілізації. Також проросійський осередок займався дискредитацією військово-політичного керівництва та підрозділів Сил оборони нашої держави.

За оперативною інформацією, основними «замовниками послуг» ботоферми були представники спецслужб країни-агресора. Вони купували фальшиві акаунти і використовували їх в популярних соцмережах начебто від імені пересічних українців. Через проведення інформаційних диверсій агресор намагався розхитувати внутрішньополітичну обстановку у західних регіонах України.

Зловмиснику планується повідомити про підозру за ч. 5 ст. 361 Кримінального кодексу України (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку). Триває слідство для встановлення всіх обставин злочину і притягнення винних до відповідальності.

КІБЕРПОЛІЦІЯ ВИКРИЛА ЗЛОВМИСНИКІВ У ФІНАНСУВАННІ ОКУПАНТІВ

Фігуранти робили «донати» на потреби російських військових і незаконних збройних формувань так званих «лднр». Восьмеро жителів різних регіонів України переказували гроші на потреби окупаційних військ і представників псевдореспублік «лднр». Інформацію про збори вони отримували з пропагандистських Telegram-каналів. Загалом фігуранти переказали близько 200 тисяч гривень на криптогаманці, утворені росіянами.

В ході оперативних заходів кіберполіція заблокувала 8 криптовалютних гаманців, які використовувалися у злочинних цілях. Загальний баланс на рахунках становить близько двох мільйонів гривень.

Відкрито кримінальне провадження за ч. 1 ст. 258-5 (Фінансування тероризму) Кримінального кодексу України. Санкція статті передбачає від п'яти до восьми років позбавлення волі та з конфіскацією майна. Слідчі дії тривають.

НА ЛЬВІВЩИНІ СУДИТИМУТЬ УЧАСНИКІВ ЗЛОЧИННОЇ ОРГАНІЗАЦІЇ ЗА ШАХРАЙСТВО ПІД ВИГЛЯДОМ ДЕРЖАВНИХ ВИПЛАТ

Зловмисники отримували дані про банківські картки громадян за допомогою фішингових сайтів і надалі привласнювали з них гроші. Правоохоронці завершили досудове розслідування і скерували до суду обвинувальні акти.

Учасників угруповання викрили співробітники Управління протидії кіберзлочинам у Львівській області спільно зі слідчим управлінням поліції Львівщини в січні цього року.

Четверо підсудних створювали фішингові сайти, інтерфейс яких був подібним до сайтів для оформлення соціальних виплат, зокрема єПідтримки, допомоги від ЄС, різних програм благодійних фондів. Для поширення фішингових посилань зловмисники використовували онлайн-сервіси масової розсилки SMS. У такий спосіб фігуранти отримували дані банківських карт громадян і привласнювали гроші з їхніх рахунків. Шахрайські вебсайти працівники кіберполіції заблокували.

Підозрюваним загрожує до п'ятнадцяти років ув'язнення.

8. ПЕРША СВІТОВА КІБЕРВІЙНА

КОНСУЛЬСТВО США ЗЛАМАЛИ «ПРИХИЛЬНИКИ ПУТІНА»

28 лютого видання Newsweek повідомило, що група хакерів, що називає себе російськомовними українцями, захопила Twitter-акаунт Генерального консульства США в Мілані та поширила низку антиукраїнських повідомлень, у тому числі порівняння України з нацистською Німеччиною. Пост, який було видалено пізніше того ж ранку, переглянули щонайменше 149 000 разів.

ОГЛЯД ХАКТИВІСТІВ У ВІЙНІ РОСІЇ ПРОТИ УКРАЇНИ

GroupSense нараховує сорок два хактивісти, які працюють в інтересах України, на відміну від тридцяти шести, які діють від імені росії. Найвідомішими українськими групами були IT Army of Ukraine, AgainstTheWest/BlueHornet, Network Battalion '65, DoomSec і GhostSec.

Серед російських допоміжних виконавців варто відзначити Killnet, Zarya, NoName057(16), Beregini та Nemezida. XakNet представляє неоднозначність. Група заявляє, що є незалежною патріотичною хактивістською організацією, але більшість спостерігачів підозрюють, що насправді це підрозділ однієї з російських спецслужб. Найчастіше жертвами атак стають країни колишнього Варшавського договору.

РОСІЯ НАМАГАЄТЬСЯ ЗАБЛОКУВАТИ ВИКОРИСТАННЯ STARLINK ЧЕРЕЗ ПОСТАНОВКУ ПЕРЕШКОД ДЛЯ GPS – DEFENSE ONE

Першого березня вийшов матеріал, в якому описується поточна ситуація з використанням Starlink українськими військовими в зоні бойових дій. У статті вказується, що російські війська розуміючи не можливість заблокувати зв'язок із супутниковою групою напряму вдаються до інших методів протиборства. Зокрема, Starlink використовує невеликий GPS приймач, щоб допомогти вибрати, з яких супутників передавати його сигнали. Тому спостерігались спроби росії глушити сигнали GPS аби перервати роботу Starlink.

У РОСІЇ ЗАБОРОНИЛИ ІНОЗЕМНІ ЗАСТОСУНКИ ДЛЯ ОБМІНУ ПОВІДОМЛЕННЯМИ

Першого березня Роскомнагляд заборонив використовувати кілька іноземних застосунків для обміну повідомленнями в державних установах. Рішення було прийнято у зв'язку з вступом в силу ч. 8-10 ст. 10 закону «Про інформацію, інформаційні технології та про захист інформації». Під заборону підпадають застосунки, які дозволяють прямий обмін повідомленнями, не передбачають відкритого розміщення інформації в мережі, і які належать іноземним власникам. Серед них Discord, Microsoft Teams, Skype для бізнесу, Snapchat, Telegram, Threema, Viber, WhatsApp і WeChat.

Як зазначає Computing, інші іноземні програми (наприклад, Zoom) залишаються прийнятними. У заяві Роскомнагляду немає конкретних звинувачень у підривній діяльності чи прямій співучасті у діяльності антиросійських сил, як було під час заборони Facebook та Instagram.

РІК ВАЙПЕРІВ: ЯК ПІДТРИМАНИЙ КРЕМЛЕМ SANDWORM АТАКУВАВ УКРАЇНУ ПІД ЧАС ВІЙНИ

Першого березня видання The Record розмістило аналіз діяльності угрупування Sandworm, пов'язаного з російським ГРУ. На думку видання, найвидатнішим внеском Sandworm у кіберфазу війни росії проти України стало розгортання шкідливого програмного забезпечення Wiper, яке кинуло виклик українській обороні, але не виправдало очікувань.

Sandworm не здійснив очікуваних атак на інфраструктуру, зокрема енергомережу України. Група використовувала програмне забезпечення-вимагач проти цілей, які цікавлять росію, зокрема, для помсти проти організацій, які надавали матеріальну допомогу Україні.

«Хакери Sandworm також сприяють інформаційним операціям», – зазначається у звіті. Наприклад, вони поширюють змови про західні лабораторії біологічної зброї в Україні у своєму власному блозі Substack і через канал Telegram, контрольований ГРУ». Але очевидно, що тактична координація зі звичайними кінетичними військовими операціями може бути або поза компетенцією Sandworm, або поза її можливостями. «Це поки неясно, чи координують хакери Sandworm свої кібератаки з російськими військовими операціями».

15 березня видання Wired опублікувало портрет нового очільника Sandworm Євгенія Серебрякова.

ЗА СЛОВАМИ НАКАСОНЕ, РОСІЯ ЗАЛИШАЄТЬСЯ «ДУЖЕ ПОТУЖНИМ» КІБЕРСУПРОТИВНИКОМ

Як генерал Накасоне, який керує як CYBERCOM, так і Агентство національної безпеки США, заявили 7 березня під час слухань у Комітеті Сенату у справах збройних сил, що їх команди «дуже уважно» стежать за ситуацією в Україні, зазначивши, що росія залишається «дуже потужним супротивником». За словами Накасоне, рф може розв'язати шквал кібератак проти України та Заходу в рамках військового просування вглиб України під час весняного наступу або помсти за успішний український контрнаступ. Він наголосив, що війна в Україні ще далеко не скінчилася.

ПОВ'ЯЗАНА З РОСІЄЮ TA499 ЗДІЙСНЮЄ АТАКИ ЧЕРЕЗ ВІДЕОДЗВІНКИ

У звіті, опублікованому 7 березня, компанія Proofpoint описала діяльність російських пранкерів, відомих як Вован і Лексус. Згідно зі звітом компанії, загроза TA499 працює таким чином, що розсилає емейли західним політикам, які підтримують Україну, із запрошенням приєднатися до відеодзвінка від імені посольств України. Під час дзвінка використовують діпфейки довіреного співрозмовника, а жертву змушують сказати щось таке, що може поставити її у незручне становище. Розмови записуються для подальшого використання в цілях російської пропаганди. «TA499 є загрозою, до якої не можна ставитися легковажно через шкоду, яку така пропаганда може завдати бренду та суспільному сприйняттю тих, на кого вона спрямована», – зазначають у компанії.

В МОСКВІ ТА ІНШИХ РЕГІОНАХ РОСІЇ ЗНОВ ПРОЗВУЧАЛА ХИБНА ПОВІТРЯНА ТРИВОГА

9 березня в москві в результаті злому серверів радіостанцій та телеканалів в ефірі прозвучала неправдива інформація про повітряну тривогу, повідомило управління МНС рф у москві. Подібні інциденти сталися також у тульські та свердловській області, повідомили відповідні управління МНС. Такі ж явища вже спостерігалися на території рф, зокрема наприкінці лютого цього року.

РОСІЯ ГОТУЄТЬСЯ ДО НОВОЇ ФАЗИ КІБЕРВІЙНИ – MICROSOFT

15 березня корпорація Microsoft опублікувала звіт про перший рік російсько-української кібервійни, докладно проаналізувавши дії сторін, а також ті методи і засоби до яких вдавались російські зловмисники атакуючи Україну. На думку Microsoft наразі ми знаходимось у третій фазі протистояння, яка розпочалась у вересні 2022 року.

Прогнозна оцінка дій російських зловмисних акторів полягає у тому, що вони продовжують корегувати як цілі своїх атак, так і методи до яких вони вдаються. росія намагається розширити можливості доступу до розвідданих про Україну та підтримки, яка надається як цивільній, так і військовій складовій.

Ще один напрям дій – створення умов для руйнівних атак проти України та, можливо, за її межами. Для цього розробляються нові види ransomware, а також використання соціальних медіа для просування бекдорного піратського програмного забезпечення для української аудиторії.

ДОСЛІДНИКИ ПОПЕРЕДЖАЮТЬ, ЩО ПРОРОСІЙСЬКІ ХАКЕРИ ВСЕ ЧАСТІШЕ АТАКУЮТЬ ЛІКАРНІ

19 березня дослідники з кібербезпеки заявили, що відстежують, як проросійська хакерська група, відома як Killnet, з листопада все частіше вдається до DDoS атак на організації у сфері охорони здоров'я.

В останні місяці група зосередила свою увагу на вебсайтах організацій у сфері охорони здоров'я, розпочавши в лютому кампанію проти лікарень у більш ніж 25 штатах США. І хоча це угруповання переважно не завдає значної шкоди атакованим організаціям, більша частина атак досягають своєї мети тимчасово відключити вебсайти лікарень від мережі.

ЛАБОРАТОРІЯ КАСПЕРСЬКОГО ЗАЯВИЛА ПРО ПРО ВИЯВЛЕННЯ НА ДОНБАСІ ТА КРИМУ КІБЕРАТАК З ВИКОРИСТАННЯМ НОВОГО ВІРУСУ

Як 21 березня заявили в компанії «Лабораторія Касперського», з 2021 року на окупованих частинах Донбасу та в Криму реєструються масштабна кампанія з кібершпигунства, яка спрямована проти окупаційних адміністрацій, транспортних, логістичних та сільськогосподарських організацій. У компанії наголосили, що для проведення кібератак застосовується порівняно нове шкідливе програмне забезпечення, яке називається Common Magic.

КІБЕРБЕЗПЕКОВА ДОПОМОГА УКРАЇНІ ДАЛА КІБЕРБЕЗПЕКОВИМ КОМПАНІЯМ ВАЖЛИВИЙ ДОСВІД – CISCO TALOS

23 березня кібербезпекова компанія Cisco Talos поширила невеликий документальний фільм про свою діяльність в кібердопомозі Україні під час кібервійни. Один з висновків, до якого приходить компанія, – досвід швидкого збору численних фахівців в спеціальні Threats Hunting teams та встановлення робочих відносин з урядовими структурами для допомоги їм, стане прототипом для створення аналогічних груп у разі виникнення схожих конфліктів або реагування на масштабні кіберподії.

НОВА СТРАТЕГІЯ КІБЕРБЕЗПЕКИ США БАЗУЄТЬСЯ НА ДОСВІДІ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Стаття Colin Demarest опублікована 2 березня на ресурсі Defense One описує основні компоненти та підходи нової Стратегії кібербезпеки США, а також містить коментарі ключових офіційних осіб США, відповідальних за сферу кібербезпеки, стверджуючи, що багато в чому документ базовано на досвіді протистояння рф в рамках російської агресії проти України.

ЧОГО СЛУЖБИ БЕЗПЕКИ МОЖУТЬ НАВЧИТИСЯ ЗА РІК КІБЕРВІЙНИ?

Автори статті на Computer Weekly підбили підсумки року війни між рф та Україною у кіберпросторі. Серед висновків, які зробили експерти, процитовані у статті:

- невдачі рф були наслідком не стільки відсутності атак, або їх слабкості, скільки того, що за 10 років атак з боку рф Україна та її союзники, що прийшли на допомогу, навчилися відбивати їх.
- клієнти, які розпочали масштабний проєкт цифрової трансформації два-п'ять років тому, тепер усвідомлюють, що їм потрібно зупинитися та переоцінити, на які ризики їх наражає війна в Україні.
- керівники служби інформаційної безпеки та групи безпеки в організаціях, які більше ризикують стати об'єктом російського вторгнення, повинні звертати увагу на нові розвідувальні дані про загрози, коли вони з'являються. Адже додатковим ефектом конфлікту стало значне зрушення в природі фінансово мотивованої російської кіберзлочинної екосистеми.

РОСІЯ СПРОЩУЄ ПРОЦЕС ПРАЦЕВЛАШТУВАННЯ ТА ОТРИМАННЯ ВНЖ ДЛЯ ІНОЗЕМНИХ ІТ-ФАХІВЦІВ

Як повідомила 15 березня офіційна представниця МВС рф Ірина Волк, іноземні ІТ-фахівці можуть укладати трудовий договір або цивільно-правовий договір на виконання робіт з організаціями, які провадять діяльність у галузі ІТ, без оформлення дозволу на роботу чи патенту. При цьому роботодавці (акредитовані ІТ-компанії) залучають таких працівників без отримання дозволу на залучення та використання працівників.

РОСІЙСЬКІ ХАКЕРИ «WINTER VIVERN» ПОМІЧЕНІ В АТАКАХ НА УКРАЇНУ, ЄВРОПУ ТА ІНДІЮ

Нова шпигунська кампанія хакерської групи, підозрюваної у зв'язках з москвою, була націлена на урядові установи та операторів зв'язку в Україні, Індії та Європі, повідомили дослідники 16 березня.

Відповідно до аналізу компанії SentinelOne, група, відома як Winter Vivern, є «дуже креативною» та працює з обмеженими ресурсами, ретельно відбираючи цілі для атак. Схоже, що діяльність хакерів підтримує інтереси російського та білоруського урядів, особливо у зв'язку з триваючою війною в Україні. Серед тактик, застосованих угрупуванням:

- спроба інфікувати українські державні комп'ютерні системи шкідливим програмним забезпеченням, розміщеним на вебсайтах, які імітують законні державні служби.
- створення вебсторінки для фішингу облікових даних для цільових користувачів служби електронної пошти, яку використовує індійський уряд.
- маскування пакетних файлів Windows – часто використовуваних для автоматизації рутинних завдань або виконання серії команд – під антивірусні сканери та їх використання для завантаження зловмисного корисного навантаження на пристрої жертв.

LINUX ВІДМОВИВСЯ ПРИЙМАТИ ВИПРАВЛЕННЯ СВОГО ДРАЙВЕРА ВІД РОСІЙСЬКОЇ КОМПАНІЇ БАЙКАЛ ЕЛЕКТРОНІКС

Як повідомило російське видання Securitylab, мейнтейнер мережевої підсистеми ядра Linux Якуб Кічинський відмовився приймати виправлення для мережевого драйвера STMMAC від співробітника російської компанії Baikal Electronics Сергія Сьоміна. Відмова Кічинського супроводжувалася наступним повідомленням: «Нам некомфортно приймати патчі від вашої організації або пов'язані з виробленим їй обладнанням». Крім того, Сергію порекомендували утриматися від участі в розробці мережевої підсистеми ядра Linux до подальшого повідомлення.

ПІДТРИМУВАНИХ КРЕМЛЕМ ХАКЕРІВ ЗВИНУВАЧУЮТЬ В ОСТАННІХ СПРОБАХ ФІШИНГУ ПРОТИ АГЕНТСТВА ЄС

15 березня дослідники з кібербезпекової фірми BlackBerry повідомили, що за нещодавніми спробами кібератак на дипломатичні та урядові установи в Європейському Союзі стоїть російська державна хакерська група, відома як Nobelium. Наголос робився на організаціях, які «допомагають українським громадянам, які втікають з країни, і надають допомогу уряду України», – зазначили дослідники.
Зокрема, Nobelium, також широко відомий як APT29 або Cozy Bear, надсилав фішингові електронні листи з нібито розкладом для посла Польщі в США на 2023 рік. Вони містили зловмисне програмне забезпечення EnvyScout, яке дозволяє зловмисникам скидати шкідливі файли на комп'ютер, повідомляє BlackBerry.
«Загрозливі актори уважно стежать за геополітичними подіями та використовують їх, щоб підвищити ймовірність успішного зараження», – заявили дослідники.

РОСІЙСЬКИЙ РОСТЕХ НІБИТО МОЖЕ ДЕАНОНІМІЗУВАТИ КОРИСТУВАЧІВ TELEGRAM

Як 25 березня повідомило видання Bleeping Computer з посиланням на російські ЗМІ The Bell і Медуза, російський ростех купив платформу, яка дозволяє йому розкривати особи анонімних користувачів Telegram. Особливий інтерес для корпорації, яка активно залучена до моніторингу обігу інформації всередині країни, становлять адміністратори Телеграм каналів. Можливості їх ідентифікації, ймовірно, будуть використані для придушення несприятливих новин з країни.

ЕКСПЕРТИ ПРОАНАЛІЗУВАЛИ ВИСВІТЛЕННЯ ВІЙНИ В УКРАЇНІ В ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ

Враховуючи той факт, що інформаційне середовище переважно складають приватні компанії, Atlantic Council зібрала групу експертів, щоб пояснити війну, яка ведеться через українське інформаційне середовище, і винести уроки для Сполучених Штатів та їхніх союзників на майбутнє. 22 березня, Атлантична рада представила звіт з аналізом від експертів.

9. РІЗНЕ

АВСТРАЛІЙСЬКИЙ ІНСТИТУТ СТРАТЕГІЧНОЇ ПОЛІТИКИ СТВОРИВ ТРЕКЕР КРИТИЧНИХ ТЕХНОЛОГІЙ

ASPI Трекер критичних технологій – це великий проєкт, який включає звіт і вебсайт, на якому відображено результати моніторингу конкуренції між Китаєм та західними країнами у сфері критичних технологій.

TIKTOK, BYTEDANCE ТА ЇХНІ ЗВ'ЯЗКИ З КОМУНІСТИЧНОЮ ПАРТІЄЮ КИТАЮ

Подання спеціальному комітету Сенату Австралії щодо іноземного втручання через соціальні мережі від 14 березня 2023 року. Його автори стверджують «Наше дослідження поза будь-яким правдоподібним сумнівом підтверджує, що TikTok належить ByteDance, а ByteDance є компанією КНР, яка підпорядковується впливу, настановам та фактичному контролю Комуністичної партії Китаю».

«Ми показуємо, як державні агенції КПК і КНР (разом партія-держава) розширили свої зв'язки з ByteDance до такої міри, що компанію більше не можна описувати як приватне підприємство».

У дослідженні йдеться про те, що TikTok надає Пекіну приховану можливість використовувати платформу як зброю, шляхом придушення, посилення та іншого калібрування наративів таким чином, щоб таргетувати політичні групи за кордоном.

ТАЙВАНЬ ПІДОЗРЮЄ, ЩО КИТАЙСЬКІ КОРАБЛІ ПЕРЕРІЗАЛИ ІНТЕРНЕТ-КАБЕЛІ, ЩО ВЕДУТЬ ДО ЙОГО ОСТРОВІВ

Для підключення до зовнішнього світу 14 000 жителів острова Мацу покладаються на два підводні інтернет-кабелі, що ведуть до головного острова Тайваню. Національна комісія зв'язку, посилаючись на телекомунікаційну службу острова, звинуватила два китайських судна в перерізанні кабелів. Уряд Тайваню не назвав це навмисним актом з боку Пекіна, і не було прямих доказів того, що китайські кораблі несуть відповідальність.

Перерізання кабелів має не лише негативний економічний вплив, адже відсутність інтернету може відвернути туристів, а має і значні наслідки для національної безпеки.

ВІЙНА РОСІЇ ПРОТИ УКРАЇНИ КАТАЛІЗУЄ ФРАГМЕНТАЦІЮ ІНТЕРНЕТУ

Автори тексту, Професор Крістоф Майнель та Доктор Девід Хагебьоллінг з Потсдамського університету, підкреслюють, що заборони, які рф запроваджує в інтернеті, а також, листи, які надіслала Україна на адресу ICANN з проханням відкликати російські IP-адреси, є намаганням держав втручатися у технічний бік функціонування інтернету. Це пришвидшує рух до фрагментації Інтернету. На їх думку, інтернет має зберігатися, як глобальне суспільне благо і закликають держави світу подвоїти свої зусилля у цьому напрямку, працюючи над Глобальним цифровим договором, робота над яким відбувається за сприяння Технічного посланника Генерального секретаря ООН і який буде погоджено у вересні 2024 року, в результаті чого мають бути розроблені спільні принципи для цифрового простору.

ХВОРА НА РАК ПОДАЛА ДО СУДУ НА ЛІКАРНЮ ПІСЛЯ ТОГО, ЯК БАНДА ВИМАГАЧІВ ОПРИЛЮДНИЛА ЇЇ МЕДИЧНІ ФОТОГРАФІЇ В ОГОЛЕНОМУ ВИГЛЯДІ

Як 15 березня повідомило видання The Register, пацієнтка подала до суду на Lehigh Valley Health Network (LVHN) за те, що лікарня допустила «запобіжний» та «серйозно шкідливий» витік. Конфіденційні фотографії та особисті дані пацієнтки з'явилися в Інтернеті після атаки програм-вимагачів. У позові стверджується, що LVHN проявив недбалість, не захистивши «дуже конфіденційну та конфіденційну особисту інформацію (PII)» пацієнтів, і вимагає статусу групового позову для інших осіб, які постраждали від порушення.
Фахівці з кібербезпеки рекомендують надавачам медичних та інших послуг, надання яких передбачає збір та зберігання конфіденційної інформації клієнтів, збільшити увагу до процедур, які забезпечують безпеку даних.

КРЕМНІЄВА ДОЛИНА ТА КАПІТОЛІЙСЬКИЙ ПАГОРБ СТВОРЮЮТЬ АНТИКИТАЙСЬКИЙ АЛЬЯНС

Як пише 17 березня Wall Street Journal, група керівників з Кремнієвої долини, включаючи інвестора Пітера Тіля, і вашингтонські законодавці мобілізуються проти участі Китаю в технологічній індустрії США. Газета повідомляє про зростання анти-TikTok настроїв у США та країнах-союзниках.

Адміністрація Байдена зажадала, щоб китайські власники TikTok продали свої частки в застосунку або вони зіткнуться з можливою забороною США через побоювання, що додаток передає дані громадян США китайському уряду. TikTok відкидає звинувачення та заявляє, що уряд Китаю ніколи не просив компанію передавати дані громадян США, а якби таке прохання і прозвучало, то компанія цього б не робила.

Ініціатором зусиль зі створення двопартійного, двостороннього альянсу китайських яструбів є Джейкоб Хелберг, колишній політичний радник Google, який є новим членом Комісії з огляду економіки та безпеки США та Китаю.

ЗАКОНОДАВЦІ США СКАЗАЛИ ГЕНЕРАЛЬНОМУ ДИРЕКТОРУ TIKTOK, ЩО ДОДАТОК «СЛІД ЗАБОРОНИТИ»

23 березня відбулися слухання у Комітеті з енергетики та торгівлі Палати представників США, під час яких виконавчий директор TikTok Шоу Чу намагався переконати американських законодавців, що TikTok не становить загрози національній безпеці та приватності громадян США. Адже він є приватною компанією, яка не має жодного стосунку до уряду Китаю.

Як повідомляє The Record, його спроба була невдалою і майбутнє TikTok в США залишається під великим питанням, адже дві основні партії США підтримують заборону застосунку.