НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

CYBER DIGEST

Огляд подій в сфері кібербезпеки,
лютий 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

Країни світу продовжують модифікувати свої підходи до безпеки, спираючись на досвід російсько-української війни. ЄС активізував свої зусилля для запуску власної супутникової групи для безпеки свого урядового зв'язку, активніше працює над законопроєктом про кіберстійкість (Cyber Resilience Act) в частині вимог до критичного обладнання на ОКІ та проводить заходи із вдосконалення стандартів кібербезпеки. Зважаючи на нові додаткові зусилля Німеччини зменшити свою залежність від китайського обладнання, а також більшу увагу до захисту європейського кіберпростору від сторонніх виробників, можна констатувати тренд до політики більшої «суверенізації» європейського кіберпростору.

Україна продовжує виявляти факти спрямованих кібератак на державний сектор. За даними ДССЗЗІ протягом 2022 року було зареєстровано у 2,8 раза більше кіберінцидентів, ніж у 2021 році. А кількість подій інформаційної безпеки в категоріях «Шкідливий програмний код» та «Збір інформації зловмисником» зросла у 18,3 та 2,2 раза відповідно. Для того, щоб краще протидіяти цьому зростаючому потоку, впроваджуються нові практики спільної боротьби із загрозами у кіберпросторі (наприклад, проєкт із протидії кібершахрайству у фінансовому секторі), а також залучаються ресурси міжнародної допомоги та відомих міжнародних компаній (Recorded Future).

Основні суб'єкти забезпечення кібербезпеки в Україні продовжують розвивати міжвідомчу та міжнародну співпрацю, щоб бути готовим до нової хвилі кіберпротистояння з рф. Для цього у 2023 році планується проведення командно-штабних навчань (ТТХ) та з питань стратегічних комунікацій, а також щонайменше двох галузевих ТТХ з питань кібербезпеки. Для підвищення рівня кадрового потенціалу у сфері кібербезпеки проведено змагання UA30CTF для студентів (156 учасників). Також у міжнародному вимірі Україна посилює свою співпрацю із НАТО (участь українського представника в роботі CCDCOE), а також розвиток державно-приватного партнерства (наприклад представниками кіберспільноти з приватного сектору Франції).

Ще одним напрямком на якому зосередились кібербезпекові органи – навчання фахівців OSINT-технікам. За підтримки міжнародних партнерів було проведено низку тренінгів для представників державного сектору. Один з них охопив понад дві тисячі учасників з усіх регіонів України, а ще два – спеціалізовані для фахівців Сил оборони України.

Активізується міжнародна співпраця щодо спільних політик цифрового розвитку та кібербезпеки. Лінії цієї співпраці все частіше пов'язані із тіснішими взаємозв'язками між західними країнами та Азійсько-Тихоокеанським регіоном: нові угоди про співпрацю між ЄС та Сінгапуром, активізація діяльності альянсу Quad, нарощування співробітництва в межах проєкту #StopRansomware.

Зловмисна кіберактивність у лютому 2023 року продовжує тренди минулого року. Ransomware залишається головною проблемою для більшості урядів та приватних компаній. Зловмисники розширюють сферу застосування свого шкідливого ПЗ, створюючи нові версії для платформи Linux. Спроби урядових кібербезпекових структур запобігти загрозам та створити інструменти розблокування ресурсів є лише частково успішними – зловмисники модифікують своє ПЗ швидше. Лідерами кібератак залишаються ті самі великі угрупування, що й у попередні періоди (наприклад LockBit, Lazarus тощо). Продовжує зростати політично вмотивована хакерська активність – злам пошти британського парламентаря, атака на ізраїльський університет та низка інших інцидентів. Увагу привертає проблема атак на ланцюжки постачання з використанням платформ для коду з відкритим доступом.

Важливою темою лютого стало обговорення можливостей використання штучного інтелекту (ШІ) у зловмисних цілях. За оцінками спеціалістів такі системи як ChatGPT вже можливо використовуються державами в кібердіяльності. На думку фахівців з DARPA атаки проти ШІ можуть стати однією з ключових загроз безпеці людей вже у найближчому майбутньому, адже залежність суспільства від цієї технології лише зростає.

Також важливий тренд кібербезпеки – більша увага до безпеки IoT/IIoT. Ці системи все частіше використовуються в промисловості та повсякденному житті і потребують більшої безпеки. На фоні того, що загрози цьому сектору визначено одним з важливих безпекових трендів 2023 року, NIST запропонував алгоритми «полегшеної криптографії» для захисту таких малих пристроїв. Це може торкнутись як індустріальних систем, так і більш традиційних, таких як автотранспорт, медичне обслуговування тощо.

Промисловий сектор все більше занепокоєний можливістю масової ескалації ransomware проти ICS/OT систем. Вже відзначається на 87% зростання кількості атак на промислові компанії у 2022 році і питання коли це перекинеться на їх ОТ системи є питанням часу. Виробники ОТ обладнання докладають чималих зусиль для того, аби розробити патчі безпеки для такого обладнання. Але проблемою залишається те, що багато систем вже не піддаються модернізації та впровадженню кращих практик кібербезпеки. Також частиною проблеми є брак самої культури кібербезпеки для такого обладнання на підприємствах.

Протягом лютого 2023 року кібербезпекові компанії виявили низку нових APT груп або нові кампанії відомих APT груп. Ці кампанії так само орієнтовані на кібершпигунські операції на державні установи, дослідницькі організації, а також низку традиційних секторів: енергетика, фінанси, медицина, транспорт (в т.ч. судноплавство). Державні агенції (такі як ENISA) намагаються краще зрозуміти, які APT групи становлять найбільшу загрозу для їх країн, та пропонують шляхи покращеної взаємодії, аби мінімізувати загрози (наприклад, спільні підходи до створення програм відповідального розкриття вразливостей).

Світ підбиває підсумки першого року кібервійни. Загалом висновки можуть бути розділені на три категорії: оцінка дій України та її готовність до війни, основні риси кіберсуперництва протягом цього року та наслідки та перспективи на 2023 рік.

Оцінюючи Україну та вжиті нею заходи, експерти вказують на те, що Україні вдалось уникнути найважчих наслідків та не допустити масштабних кібератак. Завдяки тому, що українські кіберспеціалісти виявились ефективнішими ніж російські, Україні вдається ефективно відстежувати нові загрози. Також важливу роль зіграло те, що більшість важливих українських ресурсів перенесені у хмару. Підкреслюється, що український телеком-сектор показав свою стійкість перед обличчям фізичних та кіберзагроз.

Характеризуючи саме кіберсуперництво, звертають увагу на те, що попри докладання значних зусиль російськими хакерами для здобуття переваги в кіберпросторі, результати їхніх дій неоднозначні. Хоча росія активно поєднує кібер та інформаційну складову у проведенні своїх ІПСО, ці зусилля також не ефективні. Наявні занепокоєння, що кіберактивність обох сторін може «виплеснутись» на інші країни та їх цифрові інфраструктури справдились лише частково – стало більше атак на країни-партнери України, але вони так само не досягають руйнівних наслідків. Також експерти зазначають, що хоча кібератаки не грали помітну роль у війні, вони допомогли кожній стороні збирати велику кількість розвідувальних даних, які вони змогли використати на інших полях протиборства.

Щодо довгострокових наслідків та перспектив, то вже зараз очевидні помітні зміни в східноєвропейській кіберзлочинній екосистемі, а активність російськомовних хакерських спільнот частково знизилась. Також спостерігається «відтік мізків» з-поміж російських кіберфахівців. Новий розквіт хактивізму (крауд хактивізм) набув помітного поштовху. Найбільш важливий висновок у цій сфері – не варто недооцінювати спроможності росії у проведенні руйнівних кібератак – російські хакерські групи використовували цей час для навчання та можливо кращого обмірковування небезпечних атак. Відтак небезпека більш серйозних кібератак у 2023 році залишається і навіть зростає.

15.На мапі хакерських угруповань заявилась нова група, яка називає себе Anonymous Sudan. Вона влаштовує атаки проти європейських країн нібито протестуючи проти антиісламських дій. Разом з тим, дослідники підозрюють, що її учасники не є суданцями, а саме угрупування було створено в рамках російської інформаційної операції, спрямованої на ускладнення вступу Швеції до НАТО.

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

ЯПОНІЯ МОДЕРНІЗУЄ СВОЮ КІБЕРБЕЗПЕКОВУ ПОЛІТИКУ

У статті Stimson Center від 2 лютого йдеться про те, що під впливом російської агресії проти України Японія внесла до своєї Стратегії національної безпеки зміни, які стосуються кібербезпеки та інформаційної війни.

«Японія запровадить активний кіберзахист для завчасного усунення ймовірності серйозних кібератак», – йдеться у Стратегії. Для реалізації активного кіберзахисту Національний центр готовності до інцидентів та кібербезпекової стратегії (NISC) буде реструктуровано, і в ньому створять нову організацію з кібербезпеки, яка координуватиме політику у сфері кібербезпеки та керуватиме кіберпідрозділами сил самозахисту (JSDF) та поліції. Для впровадження активного кіберзахисту також будуть внесені зміни до законодавства.

В уряді для боротьби з інформаційною війною буде створено нову структуру «для агрегування та аналізу ситуації щодо дезінформації, яка походить з-за кордону». Міністерство закордонних справ планує використовувати штучний інтелект для посилення моніторингу інформаційного простору та посилення аналізу розвідувальних даних. Міністерство оборони також планує запровадити автоматичну систему збору та аналізу інформації за допомогою технології ШІ, щоб зрозуміти ситуацію інформаційної війни.

УРЯД ВЕЛИКОБРИТАНІЇ ІНІЦІЮЄ ПЕРЕГЛЯД ЗАКОНУ ПРО ЗЛОВЖИВАННЯ КОМП'ЮТЕРОМ 1990 РОКУ

7 лютого уряд Великобританії започаткував відкриті консультації з питань внесення змін до Computer Misuse Act 1990, або Закону про зловживання комп'ютером. Цей закон є основним законом Британії, спрямованим на захист від хакерів, і не зазнавав системних оновлень від часу свого прийняття. Британський уряд пропонує розширити свої правозастосовні повноваження проти хакерів.

На обговорення винесено такі питання:
- Вилучення IP-адрес: чи повинні правоохоронні органи мати повноваження вилучати домени та IP-адреси, коли вони використовуються злочинцями, наприклад, для злому чи шахрайства?
- Збереження даних: чи повинні правоохоронні органи мати можливість вимагати збереження комп'ютерних даних у випадку, якщо під час розслідування виявиться, що вони потрібні?
- Злочини, пов'язані з даними: чи слід криміналізувати володіння або використання викрадених даних, у тому числі ідентифікаційної інформації, отриманої від когось іншого, хто сам порушив Закон про неправомірне використання комп'ютерів?

У запиті на коментарі від 7 лютого уряд стверджує, що особливо зацікавлений в отриманні відгуків щодо своїх пропозицій від правоохоронних органів, реєстраторів і реєстрів доменних імен та хостинг-провайдерів.

Критики ініціативи стверджують, що пропоновані зміни недостатньо захищають дослідників у галузі кібербезпеки від переслідування. Консультації триватимуть до 6 квітня 2023 року.

ЄВРОСОЮЗ ПРОДОВЖУЄ РОБОТУ НАД ЗАКОНОПРОЄКТОМ ПРО КІБЕРСТІЙКІСТЬ (CYBER RESILIENCE ACT)

В ЄС тривають дискусії щодо норм та положень майбутнього Закону про кіберстійкість. 10 лютого Швеція запропонувала низку компромісних формулювань щодо продуктів, які будуть визначені як «критичні» чи «надзвичайно критичні» і щодо яких буде застосовуватись зовнішній аудит безпеки.

Нові пропозиції стосуються критеріїв віднесення до категорій критичності. Таким чином «критичними» будуть ті, які виконують ключову функцію безпеки (наприклад, автентифікацію, запобігання вторгненню або захист мережі) або відіграють центральну роль в управлінні ширшою системою / можуть пошкодити кілька інших продуктів (наприклад, керування мережею та контроль конфігурації). Надзвичайно критичними будуть ті, які відповідають обом критеріям одночасно.

УРЯД ТАЙВАНЮ ВІДКРИВ НОВИЙ ІНСТИТУТ, ЯКИЙ ЗАЙМАТИМЕТЬСЯ КІБЕРБЕЗПЕКОЮ

10 лютого Президентка Цай Ін Вень відвідала церемонію відкриття Національного інституту кібербезпеки Тайваню (NICS), підкресливши увагу уряду до цього питання. Новий інститут проводитиме дослідження та даватиме рекомендації, щодо політики держави у галузі кібербезпеки та безпеки даних. Також він допомагатиме як приватному, так і державному секторам під час великих кіберінцидентів. У своїй промові Цай сказала, що «кібербезпека — це національна безпека», і що інститут допоможе зібрати найкращі таланти у технологічному секторі для сприяння безпеці Тайваню.

ЄС ПЛАНУЄ З 2024 РОКУ ЗАПУСТИТИ ВЛАСНУ СУПУТНИКОВУ ГРУПУ АБИ ЗАБЕЗПЕЧИТИ БЕЗПЕКУ УРЯДОВОГО ЗВ'ЯЗКУ ПЕРЕД ОБЛИЧЧЯМ НОВИХ КІБЕРЗАГРОЗ

14 лютого Європарламент погодив запуск супутникової інфраструктури IRIS². Це перше в Європі багатоорбітальне угруповання супутників. Вони забезпечуватимуть безпечну комунікаційну інфраструктуру для урядових органів та агенцій ЄС, екстрених служб і європейських делегацій по всьому світу. Проєкт має забезпечити стратегічну автономію ЄС у сфері безпечного урядового зв'язку. Бюджет проєкту – 2,4 мільярда євро.

НОВА СТРАТЕГІЯ МІНОБОРОНИ США ЩОДО ЛЮДСЬКИХ РЕСУРСІВ В КІБЕРСФЕРІ ПЕРЕДБАЧАЄ СТВОРЕННЯ НОВИХ ПОСАД, ПОВ'ЯЗАНИХ ЗІ ШІ ТА ОБРОБКОЮ ДАНИХ

Хоча документ ще офіційно не опублікований, про його зміст можна судити зі слайдів, розміщених на сайті конференції AFCEA WEST 2023, повідомило видання Breakingdefense 14 лютого.

Стратегія побудована навколо чотирьох широких цілей:
- виконання процесів оцінки можливостей і аналізу, щоб випереджати потреби сил;
- створення програми управління талантами для всього підприємства;
- сприяння культурним змінам у відділі;
- розвиток партнерства «для покращення розвитку можливостей, ефективності роботи та розширення кар'єрного росту».

Стратегія включає 39 оновлених посад, які включають хмару та DevSecOps, нову «унікальну посаду» систем керування та 71 посаду, яка включає функції штучного інтелекту, обробки даних та програмного забезпечення, йдеться на слайдах.

NCSC UK ЗАПРОПОНУВАВ ПРОСТИЙ АЛГОРИТМ МАПУВАННЯ ЛАНЦЮЖКІВ ПОСТАЧАННЯ

16 лютого британський Національний координаційний центр кібербезпеки (NCSC) оприлюднив керівництво щодо мапування ланцюжків постачання (supply chain). Це керівництво призначено для середніх і великих організацій, які хочуть поліпшити свою кібербезпеку через краще розуміння вразливостей, пов'язаних із роботою з постачальниками. Закладний алгоритм складається з простих восьми кроків та спирається на наявні кібербезпекові документи, поширені NCSC раніше.

NSA ОПУБЛІКУВАЛО НАСТАНОВИ ДЛЯ ДОМАШНІХ КОРИСТУВАЧІВ ЩОДО КРАЩОГО ЗАХИСТУ ЇХНІХ МЕРЕЖ

22 лютого NSA опублікувало настанови «Найкращі методи захисту вашої домашньої мережі», аби допомогти дистанційним працівникам захистити свої домашні мережі від зловмисників. Посібник містить рекомендації щодо захисту пристроїв маршрутизації, сегментів бездротової мережі, забезпечення конфіденційності під час дистанційної роботи тощо.

НАПЕРЕДОДНІ 24 ЛЮТОГО CISA ЗАКЛИКАЛА ДО БІЛЬШОЇ ПИЛЬНОСТІ УЧАСНИКІВ РИНКУ ДО ВЛАСНОЇ КІБЕРБЕЗПЕКИ

23 лютого CISA попередила всі організації та приватних осіб про можливість зростання російської кіберактивності напередодні річниці російського вторгнення в Україну. Попередження супроводжувалось посиланням на матеріали сайту Shields Up – вебсторінку CISA, яка надає ресурси для підвищення організаційної пильності та інформує громадськість про поточні загрози у кіберпросторі.

ANSSI РОЗБУДОВУЄ МЕРЕЖУ СВОГО ЛОКАЛЬНОГО ПРЕДСТАВНИЦТВА

У лютому 2023 року ANSSI оприлюднив результати своєї діяльності з розширення свого представництва на локальному рівні. Починаючи з 2015 року ця урядова агенція розпочала програму збільшення своєї присутності на регіональному рівні і наразі має представництво в усіх основних регіонах. Її місцеві представники тісно взаємодіють з органами влади та бізнесом (особливо малим та середнім) аби зменшити кіберзагрози на місцевому рівні. На цю програму виділено 176 мільйонів євро.

НІМЕЧЧИНА ГОТУЄТЬСЯ ЗМЕНШИТИ СВОЮ ЗАЛЕЖНІСТЬ ВІД ОБЛАДНАННЯ HUAWEI І ZTE У СВОЇХ 5G МЕРЕЖАХ

Уряд Німеччини готується до зменшення залежності своєї інформаційної інфраструктури від китайських виробників Huawei і ZTE. Це стало наслідком публікації у грудні 2022 року дослідження Strand Consult, яке показало, що Німеччина є одним з лідерів серед європейських країн щодо використання китайських технологій – близько 59 відсотків інфраструктури 5G пов'язано із китайськими виробниками. Наразі точно не відомо, який саме шлях зменшення залежності буде обрано. Найбільш ймовірний – обмеження операторів критичної інфраструктури використовувати технології не європейських виробників у забезпеченні основних функцій.

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

СПІЛЬНА ЗАЯВА QUAD ПРО СПІВПРАЦЮ ДЛЯ ПРОСУВАННЯ ВІДПОВІДАЛЬНИХ КІБЕРЗВИЧОК

7 лютого партнери альянсу Quad з Австралії, Індії, Японії та Сполучених Штатів запустили публічну кампанію з покращення кібербезпеки у своїх країнах – Quad Cyber Challenge. Вони закликали користувачів інтернету в Індо-Тихоокеанському регіоні та за його межами приєднатися до ініціативи.

ПІД ЕГІДОЮ ENISA ВІДБУЛАСЬ ВЕЛИКА ДИСКУСІЯ ЩОДО МАЙБУТНЬОГО ЄВРОПЕЙСЬКОЇ СТАНДАРТИЗАЦІЇ У СФЕРІ КІБЕРБЕЗПЕКИ

7 лютого ENISA спільно з європейськими організаціями зі стандартизації організувала конференцію високого рівня за участі 1600 спеціалістів аби обговорити поточні виклики у сфері стандартизації. Також обговорено питання як стандарти кібербезпеки підтримують впровадження європейського кібербезпекового законодавства. Дискусія стосувалась зв'язку між стандартами кібербезпеки та впровадженням нових законів ухвалених ЄС, впливу стандартів на електронну ідентифікацію та довірчі послуги, а також можливі погляди на стандарти з огляду на регіональні та міжнародні підходи.

США ПОСИЛЮЄ МІЖНАРОДНЕ СПІВРОБІТНИЦТВО В МЕЖАХ ІНІЦІАТИВИ #STOPRANSOMWARE

9 лютого NSA спільно з низкою інших безпекових державних органів США, а також Агентством оборонної безпеки (DSA) Республіки Корея випустили спільний звіт про кіберзагрози з боку Північної Кореї критичній інфраструктурі. Звіт поширює інформацію про тактики, методи та процедури (TTP), які використовують кібератори КНДР під час атак програм-вимагачів проти систем охорони здоров'я США та Південної Кореї, а також на іншу критичну інфраструктуру.

США ТА БРИТАНІЯ ВВОДЯТЬ САНКЦІЇ ПРОТИ ЧЛЕНІВ РОСІЙСЬКОЇ ХАКЕРСЬКОЇ ГРУПИ TRICKBOT

10 лютого США та Великобританія оголосили про введення санкції проти семи членів російської хакерської групи Trickbot. Угрупування було відповідальне за хвилю атак ransomware під час пандемії COVID-19 проти численних лікарень та медичних закладів. Останній рік активність групи знизилась і фахівці вважають, що її члени приєднались до групи Conti. Санкції мають здебільшого символічний характер, цей крок ускладнить хакерам відмивання грошей. Міністр закордонних справ Великої Британії Джеймс Клеверлі заявив, що «накладаючи санкції на цих кіберзлочинців, ми посилаємо їм та іншим особам, причетним до ренсомвер, чіткий сигнал, що вони будуть притягнуті до відповідальності».

СІНГАПУР ТА ЄС ПІДПИСАЛИ «ЦИФРОВИЙ ПАКТ»

У лютому 2023 року Сінгапур та Європейський Союз підписали угоду про партнерство для розвитку співпраці в низці сфер цифрової економіки. До них належать цифрові платежі, довірені потоки даних, 5G, штучний інтелект та цифрові ідентифікатори. Угода також охоплюватиме зусилля щодо стимулювання цифрового підвищення кваліфікації працівників, а також цифрової трансформації бізнесу та державних послуг. Ця угода охопить й більшу кооперацію у сфері кібербезпеки.

ВІДБУЛИСЬ КІБЕРНАВЧАННЯ DEFENSE CYBER MARVEL 2 (DCM2)

У лютому 2023 року відбулись семиденні кібернавчання під егідою британських Збройних Сил Defense Cyber Marvel 2. В них взяли участь 34 команди з 11 країн (включно з Україною). Команди відпрацьовували реагування на складні кіберсценарії, включаючи атаки на мережі та промислові системи управління (ICS). Сценарії опрацьовувались на кіберполігоні НАТО CR154.

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

ЗЛОВМИСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ HEADCRAB СКОМПРОМЕТУВАЛО ПОНАД 1200 СЕРВЕРІВ REDIS

З початку вересня 2021 року щонайменше 1200 серверів баз даних Redis по всьому світу були об'єднані в ботнет за допомогою «невловимої та серйозної загрози», яка отримала назву HeadCrab.

«Для зламу великої кількості серверів Redis цей прогресивний агент загроз використовує сучасне, спеціально створене шкідливе програмне забезпечення, яке неможливо виявити безагентними та традиційними антивірусними рішеннями», – заявив експерт Aqua Асаф Ейтані у звіті, опублікованому 1 лютого.

Значна концентрація заражень на сьогодні зафіксована в Китаї, Малайзії, Індії, Німеччині, Великобританії та США. Походження загрозливого актора наразі невідоме.

КОМПАНІЯ ION GROUP ЗАЗНАЛА АТАКИ RANSOMWARE LOCKBIT

2 лютого журналісти повідомили, що дублінська компанія-виробник програмного забезпечення Ion Group, яка допомагає фінансовим установам автоматизувати важливі бізнес-процеси, постраждала від атаки рансомвер, яка змусила кілька європейських і американських банків повернутися до роботи вручну. Пізніше було підтверджено, що атаку здійснило російське угруповання LockBit, яке минулого місяця також атакувало Британську Royal Mail. Зловмисники вимагали сплатити викуп наступного дня.

Агентство кіберрозвідки Канади стверджує, що LockBit має зв'язки з росією та спричинила 22% інцидентів програм-вимагачів у Канаді у 2022 році та становитиме «постійну загрозу» для канадських організацій у 2023. І хоча угрупування позиціонується як мотиване суто фінансовою вигодою, воно, швидше за все, діє за підтримки російського уряду.

Їх стосунки з урядом рф не до кінця зрозумілі. Le Monde Informatique, наприклад, стверджує, що не лише російські, а й північнокорейські та китайські служби використовують програми-вимагачі як прикриття для кібершпигунства.

ІТАЛІЯ ПОПЕРЕДЖАЄ: КАМПАНІЯ ІЗ ЗАСТОСУВАННЯМ RANSOMWARE НАЦІЛЕНА НА ЄВРОПУ ТА ПІВНІЧНУ АМЕРИКУ

Національне агентство з кібербезпеки Італії (ACN) 5 лютого попередило про масштабну кампанію з поширення програм-вимагачів на тисячах комп'ютерних серверів у Європі та Північній Америці. Атака спрямована на вразливості в технології VMware ESXi, які були виявлені раніше, але все ще залишають багато організацій уразливими до вторгнення з боку хакерів.

Про цю вразливість та нову хвилю атак, які її експлуатують, раніше попереджали експерти з кібербезпеки. Попередження про небезпеку та заклики закрити уразливість, про яку відомо вже півтора року, поширили й інші європейські державні кібербезпекові структури.

КИТАЙСЬКА «АРМІЯ БОТІВ» АТАКУЄ FACEBOOK-СТОРІНКИ ПРЕЗИДЕНТКИ ТА КОЛИШНЬОГО ПРЕМ'ЄР-МІНІСТРА ТАЙВАНЮ

Джерела, знайомі зі справами національної безпеки Тайваню, заявили, що Комуністична партія Китаю (КПК) використовує платних онлайн-коментаторів (ботів) для нападу на Facebook-акаунти президентки Тайваню Цай Ін Вень і колишнього прем'єр-міністра Су Цзен Чана. КПК найняла маркетингові компанії для участі в кібератаках – було виявлено щонайменше 825 підозрілих облікових записів. Ці записи використовуються для розповсюдження дезінформації та коментування у соцмережах з метою чинити вплив на вибори.

РОСІЙСЬКІ ХАКЕРИ ОТРИМАЛИ ДОСТУП ДО ЛИСТУВАННЯ БРИТАНСЬКОГО ПАРЛАМЕНТАРЯ СТЮАРТА МАКДОНАЛЬДА

8 лютого британський парламентар Стюарт Макдональд повідомив, що злочинцям вдалось отримати доступ до його електронної пошти і є вірогідність, що її вміст буде опубліковано як частина операції впливу. Він пов'язує цей злам зі своєю професійною діяльністю, в тому числі щодо підтримки України у боротьбі з російською агресією. Він занепокоєний, що його листування буде модифіковане дезінформаційними повідомленнями аби справити більший вплив на громадську думку. NCSC вважає, що за атакою стоїть угрупування Seaborgium.

ПІВНІЧНОКОРЕЙСЬКІ ХАКЕРИ АТАКУЮТЬ ЗАКЛАДИ ОХОРОНИ ЗДОРОВ'Я ЗА ДОПОМОГОЮ RANSOMWARE, ЩОБ ФІНАНСУВАТИ СВОЮ ДІЯЛЬНІСТЬ

Підтримувані державою хакери з Північної Кореї здійснюють атаки програм-вимагачів на заклади охорони здоров'я та критично важливу інфраструктуру, щоб фінансувати незаконну діяльність, попередили служби кібербезпеки та розвідки США та Південної Кореї у спільному повідомленні.

Нападники вимагають виплати у криптовалюті та, серед іншого, атакують такі об'єкти, як Департамент оборонних інформаційних мереж і мережі учасників оборонно-промислової бази в США та Південній Кореї.

ПІСЛЯ ТОГО, ЯК CISA ВИПУСТИЛА ІНСТРУМЕНТ ДЕШИФРУВАННЯ, З'ЯВИВСЯ НОВИЙ ВАРІАНТ RANSOMWARE ESXIARGS

Після того, як CISA випустила дешифратор для відновлення постраждалих від атак програм-вимагачів ESXiArgs, зловмисники поновили атаки з використанням оновленої версії, яка шифрує ще більше даних.

Про появу нового варіанту повідомив системний адміністратор на онлайн-форумі, де інший учасник заявив, що у файлах розміром понад 128 МБ 50 відсотків даних перебувають у зашифрованому вигляді, що ускладнює процес відновлення. Ще однією помітною зміною є видалення адреси біткоїн із тексту вимоги сплатити викуп, причому тепер зловмисники закликають жертв зв'язатися з ними на Tox, щоб отримати інформацію про гаманець.

Статистика, опублікована краудсорсинговою платформою Ransomwhere, показує, що станом на 9 лютого 2023 року новою версією ESXiArgs було заражено 1252 сервери, з яких 1168 – повторне зараження.

ПОЛІТИЧНО ВМОТИВОВАНА КІБЕРАТАКА НА УНІВЕРСИТЕТ ТЕХНІОН

Як повідомила 12 лютого Jerusalem Post, нова, ймовірно політично вмотивована хакерська група під назвою DarkBit, вразила відомий ізраїльський університет за допомогою програми-вимагача. Університет Техніон є найкращим навчальним закладом Ізраїлю, де викладають технології, та центром освіти з кібербезпеки. Університет був змушений відкласти проведення екзаменів.

У Ізраїльському національному кіберуправлінні (INCD) заявили, що «встановлюють зв'язок із Technion, щоб отримати повну картину ситуації, допомогти з інцидентом і вивчити його наслідки».

Разом з тим, ЗМІ відзначають, що атаки на ВНЗ стали більш частим явищем, але на сьогодні INCD за законом може лише рекомендувати університетам дотримуватися певних стандартів кібербезпеки, але не має повноважень, щоб контролювати дотримання. Такі повноваження кіберуправління має лише щодо критичної інфраструктури.

APT SIDEWINDER 2021 АТАКУЄ ПОНАД 60 КОМПАНІЙ В АЗІАТСЬКО-ТИХООКЕАНСЬКОМУ РЕГІОНІ

15 лютого Group-IB опублікувала звіт, у якому детально описується діяльність державної групи загроз під назвою SideWinder. SideWinder APT, також відомий під іменами Rattlesnake, Hardcore Nationalist (HN2) та T-APT4. З 2012 року вона була помічена в кібершпигунстві проти урядів в Азійсько-Тихоокеанському регіоні. Вважається, що її штаб-квартира знаходиться в Індії.

У червні минулого року Group-IB виявила інструмент групи SideWinder.AntiBot.Script, який використовувався проти пакистанських компаній. Дослідники змогли скласти список потенційних цілей для групи, який містив 61 «урядову, військову, фінансову, правоохоронну, політичну, телекомунікаційну та медійну організацію в Афганістані, Бутані, М'янмі, Непалі та Шрі-Ланці». Дослідники також помітили значні збіги між серверами та ресурсами, якими користуються SideWinder і група BabyElephant APT, що може означати, що це одна й та сама група.

ФБР СТВЕРДЖУЄ, ЩО «СТРИМАЛО» КІБЕРІНЦИДЕНТ У СВОЇЙ КОМП'ЮТЕРНІЙ МЕРЕЖІ

17 лютого ФБР повідомило, що розслідує кібератаку на свої мережі. У короткій заяві про нещодавній кіберінцидент, який стався в одному з його найвідоміших польових офісів в Нью-Йорку, йшлося, що станом на час публікації повідомлення ситуація була під контролем. Поінформовані джерела повідомили CNN, що зловмисний інцидент вплинув на частину мережі, яка використовується для розслідування зображень сексуальної експлуатації дітей. ФБР не надала інформації щодо виду атаки та її походження.

ГРУПА LAZARUS, ЙМОВІРНО, ВИКОРИСТОВУЄ НОВИЙ БЕКДОР WINORDLL64 ДЛЯ ДОСТУПУ ДО КОНФІДЕНЦІЙНИХ ДАНИХ

23 лютого видання The Hacker News повідомило, що було виявлено новий бекдор, пов'язаний із завантажувачем шкідливого програмного забезпечення під назвою Wslink. Згідно з новими даними, цей інструмент, ймовірно, використовувався відомою Північнокорейською групою Lazarus. Він може вилучати, перезаписувати та видаляти файли, а також виконувати команди PowerShell та отримати повну інформацію про базову машину.

ПОВ'ЯЗАНІ З РОСІЄЮ ХАКЕРИ ОПРИЛЮДНИЛИ ВКРАДЕНІ У ROYAL MAIL ДАНІ У ДАРКВЕБ

24 лютого 44 гігабайти інформації, викрадені угрупованням LockBit у Королівської пошти Великобританії під час атаки ренсомвер 10 січня, були оприлюднені в дарквеб. Наскільки відомо, Royal Mail відмовилась платити викуп, а 23 лютого заявила, що їй вдалось відновити міжнародні пересилки після 6-тижневої перерви.

Компанія стверджує, що дані, які потрапили в мережу, не є дуже важливими, принаймні з точки зору бізнесу. Інші дослідники знайшли серед злитої інформації медичні дані працівників та дисциплінарні стягнення щодо тих, хто працював раніше. Швидше за все, компанія вирішила, що викрадені дані не складають такої великої цінності, щоб платити викуп та заохочувати подальшу кримінальну поведінку хакерів.

ХАКЕРИ ВИКОРИСТОВУЮТЬ ФІШИНГОВІ ВЕБСАЙТИ CHATGPT, ЩОБ ЗАРАЗИТИ КОРИСТУВАЧІВ ШКІДЛИВИМ ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ

Згідно зі звітом, який був опублікований Cyble 22 лютого, CRIL виявив кілька фішингових вебсайтів, які рекламують себе через шахрайську сторінку OpenAI у соціальних мережах для поширення різних типів зловмисного програмного забезпечення. Крім того, кілька фішингових сайтів видають себе за ChatGPT, щоб викрасти дані кредитної картки.

Скориставшись широким інтересом до ChatGPT, різні сімейства зловмисного програмного забезпечення Android використовують піктограму та назву ChatGPT, щоб ввести в оману користувачів, переконавши їх, що програми є справжніми. Це зрештою призводить до викрадення конфіденційної інформації з пристроїв Android.

ЗЛОЧИНЦІ ВИКРАЛИ МЕДИЧНІ ДАНІ БЛИЗЬКО ТРЬОХ МІЛЬЙОНІВ АМЕРИКАНЦІВ

На початку лютого 2023 року низка організацій охорони здоров'я Південної Каліфорнії надіслали листи із повідомленнями про порушення безпеки до понад трьох мільйонів пацієнтів, попереджаючи їх про те, що шахраї могли вкрасти конфіденційну інформацію про їх здоров'я та особисту інформацію. Це стало наслідком атаки ransomware у грудні 2022 року. Атаковані заклади закликали пацієнтів зареєструвати попередження про шахрайство в різних бюро кредитних історій і уважно стежити за виписками зі своїх рахунків.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

СТРАТЕГІЧНИЙ ТЕХНОЛОГІЧНИЙ ЛАНДШАФТ 2023: РИЗИКИ, МОЖЛИВОСТІ ТА НЕПЕРЕДБАЧУВАНІ ЯВИЩА

Dentons Global Advisors-Albright Stonebridge Group (ASG) опублікувала перший звіт «Стратегічний технологічний ландшафт», у якому за допомогою експертів було визначено ключові тенденції у сфері політики та полісі, які формуватимуть технологічний сектор у 2023 році.

«У 2023 році уряди продовжуватимуть стверджувати, що певні технології та їхні ланцюги постачання мають стратегічне та важливе значення для національної безпеки. Інтернет-платформи, компанії, що займаються апаратним забезпеченням, і виробники програмного забезпечення будуть боротися з новими правилами та нормами щодо таких питань, як онлайн-контент, штучний інтелект, захист даних і конкуренція. Напівпровідникова промисловість увійде на незвідану територію, оскільки уряди витрачатимуть гроші платників податків на усунення ризиків у ланцюзі постачання і запровадять новий експортний контроль», – йдеться у вступі до звіту. Сам звіт деталізує ці тенденції.

DARPA ЗАНЕПОКОЄНА МОЖЛИВОСТЯМИ АТАК НА ШІ

У редакційній статті ZDnet від 1 лютого підіймається питання про захищеність ШІ від сторонніх впливів (в т.ч. кібератак), які можуть змінити його поведінку, алгоритми дій та висновки, до яких він приходить. Зважаючи на все більшу залежність нашого життя від цих технологій, це становить стратегічну проблему. Для пошуку довгострокового рішення DARPA запустила проєкт «Гарантування стійкості штучного інтелекту проти обману» (GARD), який спрямований на те, щоб ШІ та алгоритми розроблялися таким чином, щоб вони були захищені від спроб маніпуляцій, втручання, обману чи будь-яких інших форм атак.

IT ФАХІВЦІ: CHATGPT ВІРОГІДНО ВЖЕ ВИКОРИСТОВУЄТЬСЯ ДЕРЖАВАМИ ДЛЯ КІБЕРАТАК

Згідно з результатами опитування, оприлюдненого BlackBerry 2 лютого, 74% опитаних IT-фахівців вважають, що ChatGPT становить загрозу кібербезпеці, хоча погляди на те, якою саме може бути така небезпека, різняться. 71% вважають, що державні суб'єкти вже використовують ChatGPT для здійснення кібератак.

Здатність ChatGPT допомагати хакерам створювати більш правдоподібні та легітимні фішингові електронні листи була визначена основною загрозою найбільшої кількісті опитаних (53%). До таких загроз належить і те, що ChatGPT дозволяє менш досвідченим хакерам вдосконалювати свої технічні знання і розвивати більш спеціалізовані навички (49%) і його можна використовувати для поширення дезінформації (49%).

Більшість респондентів вважають, що ChatGPT все ж таки має більше потенціалу для добра, ніж для зла, хоча 95% з них вважають, що держави мають регулювати такі типи просунутих інструментів ШІ.

В опитуванні взяли участь 1500 осіб, які приймають рішення в IT-сфері у Північній Америці, Великобританії та Австралії.

РОЗРОБЛЕНО БАЗОВУ МЕТОДИКУ ОЦІНКИ ЖИТТЄВОГО ЦИКЛУ ВИТРАТ НА ПРИДБАННЯ КІБЕРОЗБРОЄНЬ ДЛЯ МОРСЬКОЇ ПІХОТИ США – RAND CORP

У лютому 2023 року RAND Corp оприлюднило результати дослідження, яке було проведено на замовлення командування Корпусу морської піхоти США щодо оцінки життєвого циклу при придбанні кіберозброєнь (cyber weapon) та допомогти визначити шляхи підвищення прозорості прийняття відповідних рішень. Оцінка проводилась на базі дослідження тривалості життя 133 вразливостей.

Результати показали, що середня тривалість життя вразливості може бути досить короткою (від трьох до п'яти місяців відповідно) у ситуаціях, коли потенційні супротивники мають високий рівень захисту (тобто здатність швидко визначати та виправляти вразливі місця).

ВМС США ПЛАНУЄ ПЕРЕГЛЯНУТИ СВІЙ ПІДХІД ДО КІБЕРБЕЗПЕКИ ПРОДУКТІВ, ЯКІ ВПРОВАДЖУЮТЬСЯ ВІДОМСТВОМ

15 лютого головний інформаційний офіцер ВМФ США Аарон Вайс оголосив про перегляд наявної стратегії забезпечення кібербезпеки тих продуктів та IT-послуг, які надаються ВМФ. Базуючись на стратегії інформаційної переваги від 2020 року, буде запущено програму Cyber Ready яка має посилити кіберзахист шістьма способами: використання хмарних платформ і сервісів, впровадження системи безпеки з нульовою довірою, створення даних готових до використання для аналітики та підтримка прийняття рішень, щоденний моніторинг кібербезпеки та консолідація резервних IT-систем і програм.

NIST ОБРАВ АЛГОРИТМИ «ПОЛЕГШЕНОЇ КРИПТОГРАФІЇ» ДЛЯ ЗАХИСТУ МАЛИХ ПРИСТРОЇВ

7 лютого NIST оприлюднив своє рішення щодо алгоритму «полегшеної криптографії» для захисту інформації, яка передається за допомогою Інтернету речей та малої електроніки. Переможцем стала група криптоалгоритмів Ascon. Вибрані алгоритми розроблені для захисту інформації, створеної та переданої Інтернетом речей (IoT), включаючи датчики, а також для інших мініатюрних технологій: імплантовані медичні пристрої, детектори стресу всередині доріг і мостів, брелоки для доступу в транспортні засоби тощо.

ХАКЕРИ ПРОДАЮТЬ ПОСЛУГИ, ЯКІ ОБХОДЯТЬ ОБМЕЖЕННЯ CHATGPT ЩОДО ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Хакери винайшли спосіб обійти обмеження ChatGPT і використовують його для продажу послуг, які дозволяють людям створювати шкідливі програми та фішингові електронні листи, повідомили 8 лютого дослідники фірми Check Point Research.

НІДЕРЛАНДСЬКА ПОЛІЦІЯ ЗААРЕШТУВАЛА ТРЬОХ ОСІБ ЗА ЙМОВІРНУ ПРИЧЕТНІСТЬ ДО RANSOMWARE ГРУПИ. ОДИН З НИХ – ЕТИЧНИЙ ХАКЕР

25 лютого нідерландська поліція повідомила про арешт трьох осіб (двоє 21-річних та одного 18-річного) за ймовірну причетність до однієї з ransomware груп. Повідомляється, що один із заарештованих працює «етичним хакером» у голландській організації безпеки DIVD (Голландському інституті розкриття вразливостей) – Асоціації дослідників безпеки, яка отримує державне фінансування. Завдяки цьому злочинець мав доступ до будь-якої конфіденційної інформації, оскільки працював над конфіденційними розслідуваннями кіберзлочинів як дослідник DIVD.

ПРИБУТОК ДАРКНЕТ РІЗКО ВПАВ ПІСЛЯ ЗАКРИТТЯ РОСІЙСЬКОМОВНОГО РИНКУ «ГІДРА»

Згідно зі звітом Chainalysis, оприлюдненим 9 лютого, закриття російськомовного Hydra Market у квітні призвело до занепаду у світі російськомовних даркнет-ринків, в результаті чого загальний дохід продавців вдвічі зменшився. Компанія, яка займається аналізом блокчейну, каже, що активність блокчейну показує, що наприкінці 2022 року дохід від ринків даркнет склав 1,3 мільярда доларів США, що є суттєвим зниженням порівняно з 2,6 мільярда доларів доходу, отриманого у попередньому році.

За оцінками Міністерства юстиції США, у 2021 році на Hydra припадало майже 80% усіх криптовалютних транзакцій, пов'язаних із даркнетом.

INSIGHT PAPER ЩОДО WEB3

В рамках Digital Regulation Cooperation Forum (DRCF), група британських регуляторів Information Commissioner's Office (ICO), the Competition and Markets Authority (CMA), the Office of Communications (Ofcom) and the Financial Conduct Authority (FCA) випустили документ, у якому виклала свої погляди на здатність Web3 децентралізувати та демонополізувати надання послуг онлайн платформами.

Він базується на огляді літератури та дискусіях представників наукових кіл, промисловості, уряду та регуляторів на симпозіумі Web 3.0, організованому DRCF у жовтні 2022 року. Його мета – зрозуміти, як розвиваються технології, пов'язані з Web3, і визначити регуляторні можливості та проблеми, з якими стикаються як компанії, так і органи державної влади. Документ не є пропозицією регулювання, а заохоченням зацікавлених сторін до дискусії.

5. КРИТИЧНА ІНФРАСТРУКТУРА

ЗАГРОЗИ ДЛЯ ICS/OT СТАЮТЬ РЕАЛЬНИМИ ЯК НІКОЛИ – CYBER INSIGHTS 2023

Першого лютого було оприлюднено звіт Cyber Insights 2023 для технологій ICS та OT. Відповідно до його висновків, масштабні кіберзагрози для цих технологій стануть реальною загрозою вже цього року. Цьому сприяє:
- конвергенція IT та OT;
- геополітичні чинники (в т.ч. російсько-українська війна);
- ширше впровадження IoT/IIoT в промисловому сектору;
- розширення платформ де застосовуються ransomware.

Такі атаки можуть призвести до людських жертв та забруднення навколишнього середовища.

КРИТИЧНА ІНФРАСТРУКТУРА ПІД ЗАГРОЗОЮ ЧЕРЕЗ НОВІ ВРАЗЛИВОСТІ, ВИЯВЛЕНІ В БЕЗДРОТОВИХ ПРИСТРОЯХ IIOT

Кібербезпекова компанія Otorio 9 лютого повідомила, що у бездротових пристроях промислового Інтернету речей (IIoT) від чотирьох різних постачальників було виявлено 38 вразливостей, які можуть створити значну поверхню для атак загрозливими суб'єктами, які прагнуть використовувати середовища операційних технологій (OT). Ці вразливості можуть бути використані для того, щоб обійти рівні безпеки та проникнути у цільові мережі, поставивши під загрозу критичну інфраструктуру або перериваючи виробництво.

МІСТО ОКЛЕНД ПОСТРАЖДАЛО ВІД АТАКИ RANSOMWARE

10 лютого міська влада Окленда підтвердила повідомлення про те, що її мережі були вражені програмами-вимагачами, оприлюднивши заяву про те, що атака почалася в ніч 8 лютого. У початковому повідомленні йшлося про те, що відділ інформаційних технологій координує роботу з правоохоронними органами та активно вивчає масштаби та серйозність проблеми.

«Ми продовжуємо виконувати наші основні функції. 911, фінансові дані та ресурси з надання допомоги у надзвичайних ситуаціях не постраждали», – йдеться у заяві.

15 лютого міська влада оголосила режим надзвичайної ситуації у зв'язку з кібератакою. В.о. голови адміністрації міста Г. Гарольд Даффі заявив, що «багато систем залишаються несправними» після того, як «мережа» міста була виведена з ладу, щоб стримати атаку. Міська влада не коментує, які державні департаменти особливо постраждали. Режим надзвичайної ситуації дозволяє швидше реагування з боку влади.

HONEYPOT-FACTORY: ВИКОРИСТАННЯ ОБМАНУ В СЕРЕДОВИЩАХ ICS/OT

Аналітик Orange Cyberdefense Томас Жан опублікував статтю на The Hacker News, у якій детально описує прогрес та виклики, пов'язані з переходом технологій обману, використовуваного для захисних цілей, від традиційних IT до безпеки ICS. Він наголошує, що нещодавно опублікований звіт Orange Cyberdefense Security Navigator демонструє, що за останні кілька років спостерігається швидке зростання кількості атак на промислові системи управління (ICS), а, також, на тому факті, що такі атаки можуть найближчим часом стати привабливішими для хакерів.

На його думку, обман є ефективним способом покращення виявлення загроз і можливостей реагування. Однак безпека ICS відрізняється від традиційної IT-безпеки кількома параметрами. Хоча технологія обману для захисного використання, як honeypots, досягла більшого рівня розвитку, все ще існують проблеми через фундаментальні відмінності між системами, як використовувані протоколи. Статтю присвячено висвітленню цієї проблеми.

ПРОТИДІЯ АТАКАМ НА ГІПЕРВІЗОРИ ESXI VMWARE

Оскільки організації продовжують віртуалізувати свою критично важливу інфраструктуру та бізнес-системи, зловмисники, які встановлюють програми-вимагачі, відповідають тим же. Про це йдеться у звіті Insikt Group®, оприлюдненому 13 лютого.

Згідно з даними компанії, у 2022 році програми-вимагачі здійснили втричі більше атак на гіпервізори ESXi VMware, ніж у 2021 році. Появі звіту передувала масована кампанія з використання програм-вимагачів, у рамках яких було пошкоджено понад 3000 підключених до Інтернету серверів VMware. У 2020 році Recorded Future задокументував лише дві атаки на гіпервізори ESXi, що свідчить про те, що нещодавня всесвітня кампанія програм-вимагачів є лише однією з ознак ширшої тенденції.

У своєму звіті Recorded Future пропонує кілька способів пом'якшення ризиків, щоб допомогти захисникам протистояти тенденції, яка збережеться у 2023 році. Серед них використання двофакторної автентифікації, сегментації мережі та дозволені списки.

СКАНДИНАВСЬКІ АВІАЛІНІЇ ПОСТРАЖДАЛИ ВІД КІБЕРАТАКИ, «АНОНІМНИЙ СУДАН» ВЗЯВ НА СЕБЕ ВІДПОВІДАЛЬНІСТЬ

14 лютого кібератака на Scandinavian Airlines (SAS) вивела з ладу її вебсайт і розкрила деякі дані клієнтів. Компанія запевнила, що паспортні дані залишились у безпеці.

Це був важкий вівторок для Швеції загалом. Через кібератаку національний суспільний телевізійний мовник SVT тимчасово не працював, а низка компаній, університетів і операторів зв'язку також зазнали кібератак.

Група, яка називає себе «Анонімний Судан», взяла на себе відповідальність за обидва напади, і у заяві, опублікованій на своєму вебсайті, причиною назвала спалення Корану під час січневих протестів у Стокгольмі. Зловмисники погрожують подальшими атаками, якщо уряд Швеції офіційно не перепросить за спалення Корану.

Дослідники шведської фірми TrueSec вважають, що «Анонімний Судан» насправді не є суданцями через їхні зв'язки з російськими групами хактивістів. Його, швидше за все, було створено в рамках російської інформаційної операції з метою нашкодити та ускладнити вступ Швеції до НАТО.

КІЛЬКІСТЬ АТАК ПРОГРАМ-ВИМАГАЧІВ НА ПРОМИСЛОВІ КОМПАНІЇ ЗРОСЛИ НА 87% У 2022 РОЦІ

Згідно з опублікованим 15 лютого звітом «Огляд безпеки ICS/OT 2022 року» від компанії Dragos, кількість атак програм-вимагачів проти промислових організацій у 2022 році зросла на 87% порівняно з попереднім роком, причому більшість зловмисного програмного забезпечення спрямовано на виробничий сектор. Компанія також виявила, що у 2022 році атаки на організації ICS/OT здійснили на 35% більше ренсомвер груп, ніж у 2021 році.

НОВА ЗАГРОЗА WIP26 НАЦІЛЕНА НА ПОСТАЧАЛЬНИКІВ ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ НА БЛИЗЬКОМУ СХОДІ

Постачальники телекомунікаційних послуг на Близькому Сході стають мішенню раніше незадокументованого носія загрози, який підозрюють у зборі розвідувальної інформації, повідомило 16 лютого видання The Hacker News з посиланням на звіт компанії SentinelOne.

Дослідники назвали його WIP26 і стверджують, що він значною мірою покладається на загальнодоступну хмарну інфраструктуру, намагаючись уникнути виявлення, вдавши, що зловмисний трафік є легітимним.
В його арсеналі зловживання Microsoft 365 Mail, Azure, Google Firebase і Dropbox для доставлення зловмисного програмного забезпечення, викрадення даних і цілей командування та контролю.

СУДНОПЛАВНІ КОМПАНІЇ ТА МЕДИЧНІ ЛАБОРАТОРІЇ В АЗІЇ СТАЛИ ОБ'ЄКТОМ ШПИГУНСЬКОЇ КАМПАНІЇ – SYMANTEC

22 лютого спеціалісти компанії Symantec повідомили про виявлену кібершпигунську кампанію, спрямовану на кілька судноплавних компаній та медичних лабораторій в азійських країнах. За атакою стоїть нове хакерське угруповання, яке назвали Hydrochasma. Дослідники не знають, де базується Hydrochasma. Угрупування не використовує спеціального зловмисного програмного забезпечення, покладаючись виключно на загальнодоступні. У своєму звіті Symantec пояснила, що найімовірнішою мотивацією кампанії є збір і, можливо, викрадання розвідувальних даних.

ВИРОБНИК ПРОДУКТІВ ХАРЧУВАННЯ DOLE ЗАЗНАВ АТАКИ RANSOMWARE

23 лютого було повідомлено, що компанія Dole (виробник харчових продуктів) зазнала атаки ransomware, через що була змушена зупинити деякі виробничі потужності (попередньо кілька заводів компанії у Північній Америці). Наразі не відомо про реальні масштаби атаки та які заходи вживаються для відновлення функціональності. Представники компанії зазначають, що співпрацюють з правоохоронними органами для розслідування інциденту.

ЗАГРОЗИ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ЇЇ ОТ ІНФРАСТРУКТУРИ ЗРОСТАЮТЬ

Компанія з кібербезпеки Cyble виявила 8000 віртуальних обчислювальних мереж (VNC) доступ до яких відкритий з мережі Інтернеті. Більшість цих систем розташовано в США, Китаї та Швеції. Публічно доступні ОТ системи можуть наражати критичну інфраструктуру на атаки хакерів, і тим самим поставити під загрозу національну безпеку.

ОТ особливо вразливі через застарілість технології, обмежену кількість виправлень, слабкі паролі, обмежені ресурси безпеки та відкритий порт 5900. Щоб захистити OKI підприємства повинні тримати найбільш важливі IT/OT активи за брандмауерами, обмежити доступ до VNC через Інтернет, регулярно оновлювати пристрої, запровадити надійну політику паролів, визначити пріоритетність засобів контролю доступу.

6. АНАЛІТИЧНІ ОЦІНКИ

КЕРІВНИЦТВО CISA ЗАКЛИКАЄ БЕЗПЕКОВІ КОМПАНІЇ ДО БІЛЬШОЇ ВІДПОВІДАЛЬНОСТІ ЗА КІБЕРБЕЗПЕКУ ЇХНІХ ПРОДУКТІВ

У статті, опублікованій Foreign Affairs першого лютого, очільники CISA Джен Істерлі та Ерік Голдстайн стверджують, що Сполучені Штати стикаються не з проблемою кібербезпеки, а з ширшою проблемою технологій і культури. Вона полягає у тому, що технологічні компанії розробляють та продають продукти без належної уваги до безпеки користувачів. І ця проблема є найбільш болючою в технологічному секторі, адже його продукти є дуже широко розповсюдженими. В результаті, необхідність протистояти загрозам лягає на користувачів, які не мають, ані ресурсів, ані необхідних знань, щоб захистити себе.

«Американцям потрібна нова модель, якій можна довіряти, щоб гарантувати безпеку та цілісність технології, якою вони користуються щогодини та щодня. Проблеми слід вирішувати на ранній стадії – під час розробки технології, а не під час її використання», – стверджують автори статті та пропонують шляхи, як цього можна досягти у співпраці з користувачами.

APT34 ЗНОВУ АКТИВІЗУВАЛИСЬ ПРОТИ ДЕРЖАВ БЛИЗЬКОГО СХОДУ – TREND MICRO

Другого лютого кібербезпекова компанія Trend Micro заявила про виявлення нової кампанії, яку розпочала група APT34, пов'язана з іранським урядом. Головною метою є викрадення облікових даних користувачів. Найбільш бажані цілі для угрупування: організації фінансового сектору, державні установи, енергетична, хімічна та телекомунікаційна галузі. Основні країни, на які спрямовано атаки: Об'єднані Арабські Емірати, Китай, Йорданія та Саудівська Аравія.

ЗА КІБЕРАТАКОЮ НА ФРАНЦУЗЬКИЙ ЖУРНАЛ CHARLIE HEBDO СТОЯЛО ІРАНСЬКЕ ХАКЕРСЬКЕ УГРУПОВАННЯ – MICROSOFT

Третього лютого Центр аналізу цифрових загроз (DTAC) Microsoft оприлюднив результати свого розслідування атаки на французький сатиричний журнал Charlie Hebdo. За їх оцінками за атакою стояло іранське угрупування NEPTUNIUM. Хакери заявили, що внаслідок кібератаки у січні 2023 року отримали особисту інформацію понад 200000 клієнтів Charlie Hebdo: імена, номери телефонів, домашні та електронні адреси облікових записів. На думку правоохоронних органів це може поставити під загрозу життя цих людей.

ENISA ТА CERT-EU ВИПУСТИЛИ ЗВІТ ПРО НАЙНЕБЕЗПЕЧНІШІ ДЛЯ ЄС ХАКЕРСЬКІ ГРУПИ

15 лютого ENISA та CERT-EU оприлюднили спільний звіт, у якому розглядають діяльність низки хакерських угрупувань, які вважають постійною загрозою для держав-членів та їх організацій. До переліку цих груп включено: APT27, APT31, Ke3chang (APT15), Mustang Panda. Документ також охоплює TTPs цих угрупувань та рекомендації зі зменшення загроз.

ENISA ПУБЛІКУЄ ДОСЛІДЖЕННЯ ЩОДО МОЖЛИВИХ ШЛЯХІВ СТВОРЕННЯ НАЦІОНАЛЬНИХ ПРОГРАМ ВІДПОВІДАЛЬНОГО РОЗКРИТТЯ ВРАЗЛИВОСТЕЙ

16 лютого ENISA поділилась своїм поглядом на те, як держави-члени мають створювати свої програми щодо відповідального розкриття вразливостей. Створення таких політик (програм) є вимогою Директиви про заходи для високого спільного рівня кібербезпеки в ЄС (NIS2).

У звіті аналізуються пов'язані з цим юридичні, спільні та технічні проблеми, пов'язані з такими ініціативами. Також він включає резюме ключових очікувань галузі при розбудові таких програм:

- політики повинні враховувати чинні ініціативи та стандарти;
- має бути посилене співробітництво між гравцями галузі та державним сектором аби уникнути непорозумінь.

ПРОДОВЖУЄТЬСЯ СКООРДИНОВАНА КІБЕРШПИГУНСЬКА КАМПАНІЯ ПРОТИ ЯПОНІЇ – TREND MICRO

16 лютого компанія Trend Micro оприлюднила результати свого нового дослідження щодо зловмисної кампанії «Земля Яко» (Earth Yako), яка проводиться проти організацій в Японії. Це, переважно, кібершпигунська кампанія, яка розпочалась у 2021 році проти дослідницьких, економічних та енергетичних структур і триває досі. Наразі групи, які стоять за нею, почали використовувати нові TTPs та інфраструктуру для проведення атак. На думку дослідників, за кампанією може стояти одна з наступних груп: Darkhotel, APT10 або APT29.

APT ГРУПИ, ПІДТРИМУВАНІ ДЕРЖАВАМИ, НАЦІЛЕНІ НА ТРАНСПОРТ, СУДНОПЛАВСТВО ТА ЕНЕРГЕТИКУ – TRELLIX

22 лютого Trellix Advanced Research Center оприлюднив результати дослідження активності APT груп за лютий 2023 року. За їх висновками, найбільш активні APT групи були пов'язані із китайським урядом, а основні цілі (69% виявлених зловмисних дій) націлені на транспорт, судноплавство, енергетику (нафта та газ). Додатково підкреслено, що сфера фінансів та охорони здоров'я найбільше піддаються атакам з боку ransomware.

ДОСТУПНІСТЬ КІБЕРСТРАХУВАННЯ ДЛЯ ОКІ В ЄС – ЗВІТ ENISA

23 лютого ENISA поширила своє дослідження щодо тих проблем, з якими стикаються оператори основних послуг (OES), намагаючись отримати доступ до кіберстрахування. Згідно з зібраними даними, три з чотирьох європейських ОКІ зараз не мають кіберстрахового покриття. 77% респондентів мають формалізований процес виявлення кіберризиків. Водночас 64% опитаних організацій заявляють, що не вимірюють кіберризики.

Серед мотивів, через які ОКІ готові долучитись до кіберстрахування: покриття у разі збитку в результаті кіберінциденту (46%), вимоги законодавства (19%). 56% респондентів заявили, що вважають інші інструменти зниження ризиків ефективнішими, ніж кіберстрахування.

ІНІЦІАТИВИ З ПРОТИДІЇ АТАКАМ НА ЛАНЦЮЖКИ ПОСТАЧАНЬ ВСЕ ЩЕ НЕ ДОСТАТНЬО ЕФЕКТИВНІ – THE REGISTER

За словами автора статті, щонайменше 4 різних ініціативи, спрямовані на зниження ризику атак на ланцюги постачання, були започатковані у перший тиждень лютого. Така увага до питання є виправданою, адже загроза зростає. Компанія Gartner очікує, що до 2025 року 45% організацій у всьому світі зазнають атаки на ланцюг постачання програмного забезпечення, що в три рази більше, ніж у 2021 році.

Автор також наголошує, що зловмисники націлилися на такі сховища коду, як GitHub і PyPI, і такі компанії, як постачальник платформи CI/CD CircleCI. Це означає, що організаціям необхідно звертати увагу не лише на шкідливе програмне забезпечення, але і на компоненти, з якого побудовано їх софт. Адже організації використовують у середньому понад 40 000 пакетів програмного забезпечення з відкритим кодом, завантажених розробниками.

КІБЕРЗЛОЧИННІСТЬ НЕ ДЕМОНСТРУЄ ОЗНАК СПАДУ

Прогнози щодо кіберзагроз у матеріалі, опублікованому The Dark Reading 6 лютого базуються на ключових спостереженнях дослідницької групи Zscaler ThreatLabz, до якої входять понад 125 експертів із безпеки. На їх думку, зберігатимуться та зростатимуть такі тенденції:

- пропозиції CaaS (Злочин як послуга Crime-as-a-service) продовжать зростати, підвищуючи ефективність атак та знижуючи бар'єр для входження;
- ланцюги постачання перебуватимуть під прицілом більше, ніж будь-коли. Компрометація слабших постачальників об'єкта атаки є доступнішою та призводить до успішних атак. Тому ця тактика, ймовірно, буде використовуватися в майбутньому;
- час очікування – період між початковим зломом і кінцевою стадією атаки – зменшується. Для більшості організацій це також період часу, протягом якого атака може бути виявлена та зупинена, перш ніж вона завдасть шкоди;
- ребрендинг нападників – сімейства шкідливих програм, угруповання програм-вимагачів та інші асоціації кіберзлочинців часто будуть реорганізовуватися;
- захисту кінцевої точки буде недостатньо. Зловмисники частіше використовуватимуть тактики обходу антивірусних програм та інших рішень безпеки кінцевих точок;
- витік вихідного коду веде до розгалуження. Оновлені та розгалужені версії зловмисного програмного забезпечення та інших загроз ускладнюватимуть виявлення для захисників, оскільки існує дуже багато варіантів, які використовують спеціальні методи для розгортання однієї атаки. Такі варіанти розвиватимуться різними темпами.

США ПОЛІПШУЄ НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ МЕДИЧНИХ ПРИСТРОЇВ

У своїй статті для Lawfare blog від 8 лютого викладач Школи права Каліфорнійського університету в Берклі та старший політичний радник Стенфордського центру кіберполітики Джим Демпсі підтримує запровадження вимог щодо кібербезпеки медичних пристроїв, що приєднуються до Інтернету. Такі вимоги було запроваджено Законом про асигнування, який президент Байден підписав 29 грудня 2022 року.

Демпсі також підтримує надання повноважень відповідним державним органам щодо регулювання таких пристроїв. У своїй статті він аргументує необхідність надання подібних повноважень галузевим державним органам щодо критично важливих суспільних суб'єктів в їх юрисдикції та висловлює надію, що посилення ролі держави у галузі кібербезпеки стане одним з напрямів нової Стратегії кібербезпеки США, на появу якої очікують найближчим часом.

НАДТО БАГАТО ДАНИХ І НЕДОСТАТНЬО ЧАСУ ДЛЯ ОСМИСЛЕННЯ

Намагаючись захистити свої мережі від кіберзагроз, більшість керівників корпорацій не враховують, які хакери становлять найбільшу загрозу для їхньої організації. Це випливає з нового опитування, проведеного Mandiant.

Попри те, що переважна більшість із 1350 бізнесменів та IT-спеціалістів, з якими спілкувався Mandiant, заявили, що розуміють, що необхідно вивчати зловмисника, 79% респондентів сказали, що приймають «більшість» рішень щодо безпеки, не звертаючи уваги на зовнішній контекст. Одна з можливих причин полягає у надто великій кількості даних і сповіщень, що перевантажує захисників і залишає їм мало часу для визначення пріоритетів. Про це повідомили 84% респондентів.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

ПІД ГОЛОВУВАННЯМ СЕКРЕТАРЯ РНБО УКРАЇНИ ОЛЕКСІЯ ДАНІЛОВА ВІДБУЛОСЯ ЗАСІДАННЯ НАЦІОНАЛЬНОГО КООРДИНАЦІЙНОГО ЦЕНТРУ КІБЕРБЕЗПЕКИ

Під час засідання було розглянуто питання, зокрема, щодо можливої ескалації кіберагресії рф та першочергових заходів протидії в умовах воєнного стану, результатів проведення командно-штабних навчань «Національна кіберготовність - 2022»; про внесення змін до Загальних правил обміну інформацією про кіберінциденти (Протоколу TLP) тощо.

За словами Секретаря РНБО, предтечею і складовою нової хвилі масштабної агресії рашистів, як і рік тому, може стати наступ у кіберпросторі, і ми маємо бути готові до відсічі. Україна, сказав О. Данілов, зміцнила та розвинула національну систему кібербезпеки, значно підвищила рівень технічного оснащення українського війська і кібервоїнів. У цьому контексті він висловив вдячність усім суб'єктам забезпечення кібербезпеки, зокрема НКЦК, за злагоджену роботу із захисту кіберпростору, попередження кіберінцидентів і мінімізації їх наслідків.

О. Данілов також наголосив на тому, що Україна посилила свої позиції як повноправний партнер міжнародної взаємодії у сфері кібербезпеки. У цьому контексті він згадав про підписання Угоди між Україною та Об'єднаним центром передових технологій з кібербезпеки НАТО. Присутність України в цьому Центрі, сказав він, посилить обмін кібердосвідом між Україною та країнами-членами NATO CCDCOE. Крім того, це важливий крок на шляху вступу України до НАТО.

Секретар РНБО також звернув увагу на важливість підготовки фахівців у сфері кібербезпеки. Йшлося також про важливість удосконалення нормативно-правової бази задля посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам. Учасники засідання затвердили нову редакцію Загальних правил обміну інформацією про кіберінциденти (Протоколу TLP).

ПРЕДСТАВНИК УКРАЇНИ ВПЕРШЕ ДОЛУЧИТЬСЯ ДО РОБОТИ ОБ'ЄДНАНОГО ЦЕНТРУ ПЕРЕДОВИХ ТЕХНОЛОГІЙ З КІБЕРОБОРОНИ НАТО

На засіданні Кабінету Міністрів України 17 лютого 2023 року було підтримано пропозицію Державної служби спеціального зв'язку та захисту інформації України та ухвалено постанову «Про представника Державної служби спеціального зв'язку та захисту інформації в Об'єднаному центрі передових технологій з кібероборони НАТО» (CCDCOE). Завдяки спільній роботі Національного координаційного центру кібербезпеки при РНБО України та Держспецзв'язку наші фахівці вперше представлятимуть Україну в Об'єднаному центрі передових технологій з кібероборони НАТО.

Також у подальшому передбачається присутність на ротаційній основі в CCDCOE представників й інших основних суб'єктів національної системи кібербезпеки – Міністерства оборони України та Служби безпеки України.

Присутність представника України в CCDCOE сприятиме обміну інформацією та збільшенню ефективності протидії агресії у кіберпросторі. Українські фахівці матимуть доступ до величезної бази знань, зможуть брати участь у спільних кібернавчаннях та проводити разом із партнерами дослідження у сфері кібербезпеки, зокрема у сфері захисту критичної інфраструктури.

НКЦК ТА НБУ ЗАПУСТИЛИ ПРОЄКТ ІЗ ПРОТИДІЇ КІБЕРШАХРАЙСТВУ У ФІНАНСОВОМУ СЕКТОРІ

Головна мета проєкту – посилити захист громадян від кіберзлочинців, які суттєво активізували діяльність у період воєнного стану в Україні. Для крадіжки коштів зловмисники проводять фішингові кампанії, метою яких є виманювання даних для доступу до банківських рахунків. Обіцянки шахраїв варіюються в залежності від актуальних новин, особливо тих, що стосуються надання громадянам державної та міжнародної фінансової допомоги.

Завдання проєкту просте – зменшити переходи користувачів на шахрайські сайти шляхом перенаправлення їх на сторінку з попередженням, що сайт створений зловмисниками. Лише за перший місяць зафіксовано близько 120 тисяч унікальних переходів на цю сторінку. Іншими словами, десятки тисяч громадян України щомісяця будуть захищеними від потрапляння на «гачок» кібершахраїв і потенційної можливості бути ошуканими.

Восени минулого року НКЦК було створено робочу групу, до якої увійшли представники державних органів та провайдери з найбільшою інфраструктурою. Відбулося успішне тестування роботи системи захисту від фінансового фішингу. Першим з найбільших провайдерів, який долучився до проєкту, став Kyivstar. Крім того, до системи захисту вже долучились усі оператори, які дбають про кібербезпеку своїх клієнтів.

USAID ВИДІЛИТЬ 60 МЛН ДОЛАРІВ НА ПОСИЛЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Віцепрем'єр-міністр – Міністр цифрової трансформації Михайло Федоров зустрівся із заступницею голови USAID Ізобель Коулман. Під час зустрічі обговорили подальшу співпрацю України з Агенцією США з міжнародного розвитку. Зокрема, посилення кіберзахисту та підтримку цифрової трансформації.

USAID заявили, що виділять 60 млн доларів на зміцнення кібербезпеки України. Це допоможе уряду захистити об'єкти критичної інфраструктури від російських кібератак. Зокрема, енергетичну, телекомунікаційну та систем зберігання даних.

«USAID – надійний партнер України. Завдяки підтримці агенції ми запустили застосунок та портал Дія, а також десятки найпопулярніших послуг, які українці можуть отримати в декілька кліків. Команда Мінцифри активно співпрацює з USAID у сфері цифрової трансформації та кібербезпеки. За підтримки агенції ми створюємо найзручніші сервіси в Дії для українців і вже ділимося досвідом зі світом. Вдячні USAID за регулярну допомогу, підтримку наших діджитал-ініціатив та посилення кіберзахисту держави», – зазначив Михайло Федоров.

РОСІЯ ЗДІЙСНЮЄ ПОНАД 10 КІБЕРАТАК НА УКРАЇНУ ЗА ДЕНЬ. ВІД ПОЧАТКУ ВТОРГНЕННЯ ЇХ БУЛО 4500 – СБУ

Україна бореться зі збільшенням числа кібератак, причому росія здійснює щонайменше 10 атак на день, повідомив The Independent Голова Служби безпеки України Василь Малюк. За його словами, після вторгнення було зафіксовано понад 4500 кібератак.

«Наразі росія здійснює в середньому понад 10 кібератак на день... Їхні цілі різні: державні ресурси, об'єкти критичної інфраструктури тощо. Але ми успішно протистоїмо противнику і в кіберпросторі», – сказав він.

За словами Голови СБУ, у 2020 році відомство зафіксувало 800 кібератак, у 2021 році – близько 2000, а після вторгнення – понад 4500. Він додав, що йдеться про різні типи атак, іноді масові.

НА XVII ЗАСІДАННІ НАЦІОНАЛЬНОГО КЛАСТЕРА КІБЕРБЕЗПЕКИ ОБГОВОРЕНО ТЕНДЕНЦІЇ ТА НОВІ МОЖЛИВОСТІ У СФЕРІ КІБЕРБЕЗПЕКИ У 2023 РОЦІ

21 лютого 2023 року відбулося XVII засідання Національного кластера кібербезпеки на тему «Кібербезпека 2023: тенденції, нові можливості та перспективи». Захід організовано Національним координаційним центром кібербезпеки спільно з Фондом цивільних досліджень та розвитку США за підтримки Державного департаменту США.

Відкриваючи засідання, керівник управління забезпечення діяльності НКЦК профільної служби Апарату РНБО Сергій Прокопенко зазначив, що Національний кластер кібербербезпеки як координаційний захід показав свою ефективність. Завдяки йому державні установи та об'єкти критичної інфраструктури отримали необхідну підтримку, зокрема через грантові програми. І у 2023 році команда Кластера продовжуватиме цю роботу.

«У 2022 році завдяки злагодженій спільній роботі державного, приватного сектору та міжнародній підтримці Україна довела свою стійкість у кіберпросторі. Зараз ми спостерігаємо зменшення кількості кібератак порівняно з минулим роком, але рівень загроз при цьому не зменшився. Адже атаки ворога стали більш витонченими та складнішими, і несуть більші ризики. Тому питання кібербезпеки залишається з-поміж основних на порядку денному та у фокусі на всіх рівнях – від технічних фахівців до управлінців усіх суб'єктів кібербезпеки», – сказав С. Прокопенко. Також він презентував пріоритети, технологічні проєкти та плани проведення заходів Національним координаційним центром кібербезпеки у 2023 році.

До обговорення тенденцій та нових можливостей у сфері кібербезпеки у 2023 році долучилися понад 300 представників державного сектору, міжнародної та донорської спільноти, посольств та приватних установ. З-поміж ключових спікерів заходу – представники Мінцифри, Представництва НАТО в Україні, Центру інженерних досліджень і розробок армії США, австралійської компанії Internet 2.0 та інші.

У 2023 РОЦІ НКЦК ПРОВЕДЕ ГАЛУЗЕВІ КОМАНДНО-ШТАБНІ НАВЧАННЯ СТРАТЕГІЧНОГО РІВНЯ З ПИТАНЬ КІБЕРБЕЗПЕКИ ТА З ПИТАНЬ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ

Заступник Секретаря РНБО України Сергій Демедюк під час засідання НКЦК 9 лютого 2023 року підбив підсумки командно-штабних навчань з питань кібербезпеки стратегічного рівня «Національна кіберготовність 2022» (грудень 2022 року) за участю представників усіх державних органів, керівники яких є членами НКЦК, а також інших державних органів та об'єктів критичної інфраструктури.

Проведення таких навчань на постійній основі передбачено Планом реалізації Стратегії кібербезпеки України.

«Командно-штабні навчання дозволили скоординувати дії всіх залучених суб'єктів забезпечення кібербезпеки і відпрацювати алгоритм взаємодії на достатньому рівні. Водночас потрібно ухвалити невідкладні рішення щодо вдосконалення заходів з організації та проведення командно-штабних навчань стратегічного рівня, а також стосовно запровадження практики проведення галузевих командно-штабних навчань з питань кібербезпеки», – зазначив Сергій Демедюк.

НКЦК має протягом поточного року забезпечити проведення щорічних командно-штабних навчань стратегічного рівня з питань кібербезпеки та з питань стратегічних комунікацій і щонайменше двох галузевих командно-штабних навчань з питань кібербезпеки.

ПОНАД 2000 ДЕРЖСЛУЖБОВЦІВ З УСІЄЇ УКРАЇНИ НАВЧАЛИСЬ ВИКОРИСТОВУВАТИ ІНСТРУМЕНТИ OSINT

Національний координаційний центр кібербезпеки за підтримки Фонду цивільних досліджень та розвитку США (CRDF Global) та Державного департаменту США провели триденний онлайн-тренінг на тему: «OSINT – розвідка з використанням відкритих джерел». У ньому взяли участь понад 2000 представників державного сектору з усіх регіонів України.

Через велику кількість бажаючих навчання проходило онлайн в два етапи: 8-10 лютого та 22-24 лютого цього року. Разом з провідними дослідниками-практиками української компанії «Мольфар» учасники обговорюватимуть останні дослідження та виконуватимуть практичні завдання до таких тем: види пошуків за відкритими джерелами, пошук контактів та використання телеграм-ботів, ІПСО і її використання як одного з методів ведення інформаційної війни; аналіз зображень HUMINT або соціальна інженерія тощо.

Також відбулась лекція «GEOINT – Мистецтво геолокації» від представника французької компанії Predicta Lab.

ФАХІВЦІ НКЦК ПРОВЕЛИ РОБОЧУ ЗУСТРІЧ З ПРЕДСТАВНИКАМИ ФРАНЦУЗЬКИХ КОМПАНІЙ У СФЕРІ КІБЕРБЕЗПЕКИ

Керівник служби з питань інформаційної та кібербезпеки Апарату РНБО України, секретар НКЦК Наталія Ткачук та керівник управління забезпечення діяльності НКЦК профільної служби Апарату РНБО Сергій Прокопенко зустрілись з представниками кіберспільноти з приватного сектору Франції, з-поміж яких – керівництво Cyber Task Force, Gatewatcher та Predicta Lab. У заході також взяли участь представники посольства Франції в Україні та українського бізнесу.

«Одним з пріоритетів НКЦК є розвиток державно-приватного партнерства як в Україні, так і на міжнародній арені. Минулого року ми значно посилили позиціювання України як повноправного партнера міжнародної взаємодії у сфері кібербезпеки. Ми відчуваємо підтримку демократичних країн та зацікавлені у співпраці з французькою стороною у напрямку розвитку національної сфери кібербезпеки України», – зазначила Наталія Ткачук.

Під час зустрічі особливу увагу було приділено питанням співпраці у сфері кібербезпеки, можливості обміну досвідом та започаткування спільних освітніх проєктів тощо.

«УКРАЇНА Є ЩИТОМ ВІД КІБЕРАТАК ДЛЯ ВСЬОГО ЗАХІДНОГО СВІТУ» – ІЛЛЯ ВІТЮК

Абсолютна більшість кібератак рф наразі сфокусовані саме на нашій державі – у 2023 році кіберфахівці СБУ вже нейтралізували понад 550 таких загроз. Про це в ефірі національного телемарафону заявив начальник Департаменту кібербезпеки СБУ Ілля Вітюк.

Він зазначив, що західні партнери розуміють – якби український кіберзахист впав, то ворожий потенціал був би спрямований на них. «Якщо минулого року ми нейтралізували більше 4,5 тисяч кібератак та критичних кіберінцидентів, то за півтора місяці цього року вже маємо 550 таких атак. Тобто росія продовжує тримати темп і масованість. Але абсолютну більшість кібератак ми зупинили на початкових етапах», – підкреслив Ілля Вітюк.

За його словами, основними цілями ворожих кібернападів є об'єкти логістики і транспорту, енергетична галузь України, військові об'єкти, а також інформаційні ресурси і державні реєстри.

Як наголосив начальник Департаменту кібербезпеки СБУ, рф постійно атакує Україну з 2014 року. «Втім, наша спецслужба еволюціонувала значно більше за росіян. Сам факт, що більшість українських систем працює у штатному режимі – яскравий доказ тому, що ми успішно справляємося з викликами, навіть в надскладних психологічних умовах та дефіциту енергоресурсів. Підтримка міжнародних партнерів також допомагає Україні ефективно протистояти ворогу».

«У цій війні ми не тільки відбиваємо атаки російських окупантів, а й ефективно контратакуємо самі. Важлива мета: отримання розвідінформації для наших ЗСУ. Але іноді і просто «даємо їм по зубах», симетрично і навіть набагато потужніше відповідаємо на їх кіберагресію», – резюмував Ілля Вітюк.

ДЕРЖСПЕЦЗВ'ЯЗКУ ПРОВЕЛА ЗМАГАННЯ З КІБЕРБЕЗПЕКИ UA30CTF ДЛЯ СТУДЕНТІВ ЗА ПІДТРИМКИ ЄС

Держспецзв'язку за підтримки проєкту EU4DigitalUA, що фінансується ЄС, провела змагання з кібербезпеки UA30CTF. У змаганні взяли участь 156 студентів III-VI курсів із 22 закладів вищої освіти України.

Перше місце здобула команда 4n0M4lY (Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського»), друге та третє – Ghost of Sheva («Київський Національний університет ім. Тараса Шевченка») та Silent Sparrow («Київський національний економічний університет ім. Вадима Гетьмана», Університет «Україна», Національний технічний університет України «Київський політехнічний інститут ім. Ігоря Сікорського») відповідно.

Змагання проходили у форматі гри #Jeopardy CTF. Протягом шести годин команди вирішували 25 завдань як на логіку, так і на пошук та експлуатацію вразливостей, у поєднанні з вирішенням цікавих логічних завдань.

«Одним із пріоритетів Держспецзв'язку в напрямку реформування сфери кіберзахисту є розбудова кадрового потенціалу. Зокрема, підвищення рівня підготовки майбутніх фахівців. Задля цього Держспецзв'язку не тільки розпочала реформування формальної освіти, а й проводить практичні заходи на зразок цього, де студенти матимуть можливість використати свої знання у форматі змагань. Сподіваюсь, що в майбутньому в Україні буде ще більше таких заходів», – зазначив заступник голови Держспецзв'язку Віктор Жора.

ПРАВООХОРОНЦІ ОГОЛОСИЛИ ПІДОЗРУ РОСІЙСЬКОМУ БЛОГЕРУ-ПРОПАГАНДИСТУ

У своїх медіа-матеріалах фігурант виправдовує збройну агресію рф проти України, поширює фейки, дезінформацію та російську пропаганду. За українським законодавством зловмиснику загрожує до 5 років позбавлення волі.

Документування протиправної діяльності здійснювали співробітники Департаменту кіберполіції спільно з Головним слідчим управлінням Нацполіції та працівниками Офісу Генерального прокурора України. Кіберполіцейські опрацьовували інтернет-джерела для збору доказової бази протиправної діяльності чоловіка.

Російський відеоблогер для проєкту WarGonzo на YouTube та у проросійському Telegram-каналі створював пропагандистські матеріали. Зокрема, у них він виправдовував збройну агресію рф проти України, окупацію територій нашої держави, поширював фейки та дезінформацію. Загальна аудиторія пропагандистського проєкту на різних вебресурсах становить близько 3 мільйонів користувачів, а кількість переглядів матеріалів – більш як 500 мільйонів.

АВСТРАЛІЙСЬКІ ПАРТНЕРИ НАВЧАЛИ УКРАЇНСЬКИХ ВІЙСЬКОВИХ ОСОБЛИВОСТЕЙ ЗАСТОСУВАННЯ МЕТОДИКИ OSINT

В Києві відбувся тренінг для фахівців Сил оборони України, який провели співробітники австралійської кампанії Fivecast. На заході був присутній заступник Міністра оборони України з питань цифрового розвитку, цифрових трансформацій і цифровізації Олег Гайдук, який подякував нашим іноземним партнерам за підтримку та наголосив на важливості місії, яку ми спільно виконуємо, захищаючи весь світ від російської агресії. Захід відбувся за сприяння урядів Австралії та Великої Британії.

Під час практичного тренінгу присутнім було продемонстровано можливості сучасної методики пошуку в мережі Інтернет інформації різного характеру. Співробітники складових Сил оборони навчалися застосувати запропонований програмний продукт для відпрацювання пошукових запитів за різною тематикою.

У 2022 РОЦІ КІЛЬКІСТЬ ЗАРЕЄСТРОВАНИХ КІБЕРІНЦИДЕНТІВ ВИРОСЛА МАЙЖЕ ВТРИЧІ – ЗВІТ

Протягом 2022 року Державним центром кіберзахисту було зареєстровано в 2,8 разів більше кіберінцидентів, ніж в 2021 році. Кількість подій інформаційної безпеки в категоріях «Шкідливий програмний код» та «Збір інформації зловмисником» зросла у 18,3 та 2,2 рази відповідно.

Такі дані оприлюднені у річному звіті про роботу Системи виявлення вразливостей та реагування на кіберінциденти та кібератаки. Зокрема, за минулий рік Системою:

- опрацьовано близько 58 мільярдів подій, отриманих за допомогою засобів моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки;
- детектовано 181 мільйон підозрілих подій інформаційної безпеки (при первинному аналізі);
- опрацьовано 179 тисяч критичних подій інформаційної безпеки (потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу);
- зафіксовано та оброблено безпосередньо аналітиками безпеки 415 кіберінцидентів (критичних подій ІБ).

Згідно зі звітом загальна кількість критичних подій інформаційної безпеки, джерелом яких є IP-адреси росії, виросла на 26%, порівняно з 2021 роком. Кількість подій інформаційної безпеки в категоріях «Шкідливий програмний код» та «Збір інформації зловмисником» зросла у 18,3 та 2,2 рази відповідно.

ФАХІВЦІ ДЕРЖСПЕЦЗВ'ЯЗКУ ПРОДОВЖУЮТЬ ПРАЦЮВАТИ З НАЙКРАЩИМИ СВІТОВИМИ ІНСТРУМЕНТАМИ КІБЕРЗАХИСТУ

Фахівці Держспецзв'язку завдяки міжнародній допомозі дістали можливість ефективно використовувати в роботі з кіберзахисту України передові світові розробки. У 2022 році проєкт USAID «Кібербезпека критично важливої інфраструктури України» допоміг профінансувати ліцензію на 2023 рік для низки модулів Intelligence Cloud Platform від Recorded Future.

Recorded Future Intelligence Cloud – це продукт, який допомагає збирати дані, аналізувати поведінку і виявляти прийоми та інфраструктуру зловмисників та їхні цілі у кіберпросторі. Платформа використовується в тому числі й у функціонуванні Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки.

КІБЕРЗЛОВМИСНИКИ НАМАГАЛИСЯ ВИКРАДАТИ ДАНІ, МАСКУЮЧИСЬ ПІД УКРАЇНСЬКЕ МЗС

Урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA) виявила вебсторінку, яка імітує офіційний вебресурс Міністерства закордонних справ України. На цій сторінці відвідувачам пропонують завантажити програмне забезпечення для виявлення «заражених комп'ютерів». Насправді ж під посиланням приховується шкідливе програмне забезпечення.

У разі переходу за посиланням на комп'ютер завантажується BAT-файл «Protector.bat». Його відкриття призведе до завантаження та запуску на комп'ютері PowerShell-скриптів, які здійснюють пошук файлів із розширеннями: .edb, .ems, .eme, .emz, .key, .pem, .ovpn, .bat, .cer, .p12, .cfg, .log, .txt, .pdf, .doc, .docx, .xls, .xlsx, .rdg у каталозі робочого столу, створюють знімки екрану та передають дані на сервер зловмисників.

У межах співпраці з CERT Polska та CSIRT MON виявлені аналогічні фішингові ресурси, які імітують офіційні вебсторінки МЗС України, Служби безпеки України, а також Поліції Польщі. Слід зауважити, що в червні 2022 року подібна фішингова вебсторінка імітувала вебінтерфейс поштового серверу Міністерства оборони України. Згадана активність відстежується за ідентифікатором UAC-0114 (також відома як Winter Vivern).

ЯК ЗАХІДНИМ КРАЇНАМ ЗАХИСТИТИСЬ ВІД РОСІЙСЬКОЇ КІБЕРАГРЕСІЇ – КОЛОНКА ЮРІЯ ЩИГОЛЯ ДЛЯ ATLANTIC COUNCIL

російські кібератаки можуть призвести до підриву та блокування роботи державних органів і критичної інфраструктури, маніпулювання громадською думкою та розповсюдження шкідливого програмного забезпечення через зламані облікові записи електронної пошти. Про це розповів голова Держспецзв'язку Юрій Щиголь у колонці для Atlantic Council.

«Тоді як більш традиційні акти агресії можуть спровокувати рішучу відповідь, кібератаки функціонують у «сірій зоні», що робить їх зручними для кремля, який намагається спричинити якомога більший хаос у Європі та Північній Америці та при цьому не нарватися на прямий воєнний удар у відповідь», – зазначає голова Держспецзв'язку.

На його думку, західні країни мають врахувати досвід України у протидії російській кіберагресії. Зокрема, для своєчасної протидії атакам надзвичайно важливо координувати зусилля із громадськістю та обмінюватися інформацією із широким колом зацікавлених сторін.

Однак для того, щоб зупинити кіберагресію в усьому світі, цього замало. Потрібні більш рішучі зміни. Кібератаки мають сприйматися так само, як звичайна воєнна агресія, і мають викликати таку саму безкомпромісну реакцію. Якщо цього не станеться, навіть якщо путін зазнає поразки в Україні, шляхом росії можуть піти інші авторитарні країни.

ТАРГЕТОВАНІ КІБЕРАТАКИ ЗАЛИШАЮТЬСЯ ОДНІЄЮ З ОСНОВНИХ КІБЕРЗАГРОЗ ВІД ХАКЕРІВ ІЗ ФСБ – ЗВІТ

Фахівці Державного центру кіберзахисту Держспецзв'язку проаналізували шкідливе програмне забезпечення (ШПЗ) GammaLoad та GammaSteel, яке використовує у своїх кампаніях група UAC-0010 (Gamaredon, Armageddon, Primitive Bear). GammaLoad та GammaSteel застосовуються зловмисниками для таргетованих атак на органи державної влади та об'єкти критичної інформаційної інфраструктури України.

Зловмисна активність, що відслідковується за ідентифікатором UAC-0010, здійснюється з колишніми співробітниками СБ України в АР Крим, зараз – співробітниками одного з підрозділів фсб рф в АР Крим. Для того, щоб лишатися непоміченими для засобів кіберзахисту, побудованих на сигнатурному аналізі, зловмисники постійно вдосконалюють свої тактики та модифікують різновиди шкідливого програмного забезпечення. Таким чином, таргетовані кібератаки залишаються однією з основних кіберзагроз в Україні.

Опублікована у звіті інформація ще раз підкреслює необхідність проактивного виявлення загроз, заснованого на поведінковому аналізі.

У 2022 РОЦІ В УКРАЇНІ ЗАРЕЄСТРУВАЛИ 2194 КІБЕРІНЦИДЕНТИ – ДЕРЖСПЕЦЗВ'ЯЗКУ

Протягом 2022 року фахівці Держспецзв'язку зареєстрували в Україні понад дві тисячі кіберінцидентів та ще більшу кількість кібератак. Про це у коментарі Суспільному повідомив Віктор Жора, заступник голови державної служби спеціального зв'язку та захисту інформації України з питань цифрового розвитку, цифрової трансформації та цифровізації.

«Кібератаки стаються, тому що у нас йде повноцінна кібервійна. Перша у світі кібервійна. Почалась вона 9 років тому, фактично зразу після анексії Криму та окупації східної частини Донбасу. Зараз триває активна фаза. Фактично з 14 січня 2022 року ми зазнаємо постійних кібератак і достатньо ефективно протидіємо», — розповів посадовець.

За його словами, запобігти кібератакам можна завдяки комплексу заходів. «Це і спеціальні комплекси кіберзахисту, це взаємодія між основними суб'єктами забезпечення кібербезпеки, це своєчасне реагування на кіберінциденти і дотримання правил кібергігієни і тих рекомендацій, які надаються експертами з кібербезпеки», — пояснив чиновник.

КІБЕРЗЛОВМИСНИКИ НАЧЕБТО ВІД ІМЕНІ УКРТЕЛЕКОМУ НАМАГАЛИСЯ ШПИГУВАТИ ЗА КОМП'ЮТЕРАМИ ЖЕРТВ

Урядова команда реагування на комп'ютерні надзвичайні події України (CERT-UA) зафіксувала масове розповсюдження електронних листів начебто від імені АТ «Укртелеком». Метою такого розсилання, спрямованого переважно на органи державної влади, ймовірно, є шпигунство.

Виявлена активність відстежується за ідентифікатором UAC-0050 щонайменше від 2020 року. Попередні кібератаки згаданої групи здійснювалися із застосуванням програми для віддаленого адміністрування RemoteUtilities. Фахівці CERT-UA, виходячи з функціоналу програм і з того, що об'єктами кібератак зазвичай (але не винятково) є органи державної влади України, вважають, що така активність здійснюється з метою шпигунства.

ПРЕДСТАВНИК НАЦІОНАЛЬНОЇ АКАДЕМІЇ СБУ ВЗЯВ УЧАСТЬ У ТРЕНІНГУ DOE ТА CISA США З КІБЕРБЕЗПЕКИ В ЕНЕРГЕТИЧНОМУ СЕКТОРІ

Міжнародний тренінг з кібербезпеки автоматизованих систем управління технологічними процесами в енергетичному секторі «Introduction to Control Systems Cybersecurity Training» організували Національний науково-дослідний інститут Польщі (NASK) разом з кібербезпековим підрозділом (CESER) Міністерства енергетики США (DOE) та Агентством США з питань кібербезпеки та захисту інфраструктури CISA (Cybersecurity and Infrastructure Security Agency).

Навчальні матеріали, що надавалися учасникам тренінгу, розроблено співробітниками Idaho National Laboratory (INL) Міністерства енергетики США (DOE). Робота з практичними кейсами здійснювалася з використанням модифікованого віртуального забезпечення, а сам тренінг проводився топовими міжнародними спеціалістами з кіберзахисту.

ЗА СПРИЯННЯ НКЦК ВІДБУВСЯ ТРЕНІНГ ЩОДО ВИКОРИСТАННЯ ІНСТРУМЕНТІВ OSINT ДЛЯ ПРЕДСТАВНИКІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ

10 лютого 2023 року відбувся тренінг для представників сектору безпеки і оборони щодо використання інструментів OSINT в інтересах правоохоронної діяльності, національної безпеки та оборони.

У заході, який відбувся за сприяння Національного координаційного центру кібербезпеки та Національної академії Служби безпеки України, взяли участь співробітники Національної поліції України, Служби безпеки України, а також курсанти Національної академії Служби безпеки України.

Навчальний курс для органів сектору безпеки і оборони з імплементації інструментарію Open Source Intelligence (OSINT) у державний сектор, організовано Інститутом постінформаційного суспільства наприкінці минулого року за сприяння НКЦК та Національної академії Служби безпеки України.
«Взаємодія з приватним сектором та провідними навчальними інституціями України є одним з пріоритетів НКЦК у сфері розбудови потенціалу національної системи кібербезпеки держави. Ми постійно проводимо навчальні курси для підвищення кваліфікації працівників державного сектору та вдячні усім, хто допомагає нам у цьому», – зазначила керівник служби з питань інформаційної та кібербезпеки Апарату РНБО України, секретар НКЦК Наталія Ткачук.

КІБЕРПОЛІЦІЯ СПІВПРАЦЮВАТИМЕ З «УКРАЇНСЬКИМ НАЦІОНАЛЬНИМ ОФІСОМ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ТА ІННОВАЦІЙ»

У рамках партнерства передбачається проведення тренінгів, семінарів і навчань для ефективнішої протидії злочинам у сфері авторського права.

Начальник Департаменту кіберполіції Юрій Виходець провів робочу зустріч із представниками Державної організації «Український національний офіс інтелектуальної власності та інновацій». Сторони обговорили проблемні питання, зокрема щодо боротьби з інтернет-піратством, незаконними ретрансляціями телеканалів, поширенням протиправного контенту в мережі.

Юрій Виходець зазначив, що кіберполіція співпрацює з найбільшими медіа-корпораціями країни, налагоджує державно-приватне партнерство, оскільки захист прав інтелектуальної власності – складне питання, яке потребує комплексного підходу.

8. ПЕРША СВІТОВА КІБЕРВІЙНА

ВИЯВЛЕНО КІБЕРАТАКУ НА НИЗКУ УКРАЇНСЬКИХ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

23 лютого було виявлено атаку на низку вебресурсів українських державних та місцевих органів влади, внаслідок якої було модифіковано вміст кількох сторінок на цих ресурсах.

В рамках Об'єднаної групи з реагування при НКЦК, фахівці Держспецзв'язку, СБУ та Департаменту Кіберполіції спільно працювали над локалізацією та дослідженням обставин кіберінциденту.

Наразі можна стверджувати, що інцидент не призвів до суттєвого порушення працездатності систем та не вплинув на виконання державними органами своїх функцій. Роботу більшості інформаційних ресурсів було відновлено і вони працювали в штатному режимі.

Як бачимо, напередодні річниці повномасштабного вторгнення росія продовжувала нагадувати про себе в кіберпросторі, де вона давно поводиться як держава-терорист, атакуючи цивільні цілі.

KILLNET АТАКУЄ ЛІКАРНІ В КРАЇНАХ, ЯКІ ДОПОМАГАЮТЬ УКРАЇНІ У ВІЙНІ

Видання Becker's Hospital Review повідомило 2 лютого, що російська хактивістська мережа KillNet продовжує атакувати лікарні в країнах, які вважаються ворожими до росії. Нападники здебільшого за допомогою DDoS атак вразили медичні установи у Великобританії, Нідерландах, США, Німеччині, Польщі та скандинавських країнах. Зазвичай, їхні атаки не завдають значної шкоди.

Також повідомляється, що в США угрупування атакувало щонайменше 17 медичних установ. У коментарі виданню MedCityNews, головний технологічний директор зі стратегії безпеки в кібербезпековій компанії Akamai Патрік Салліван сказав, що медичні заклади зазвичай вибудовують захист від ренсомер та фішингу, але DDoS атаки стають дедалі більшою загрозою. Він рекомендував лікарням відпрацювати механізми реагування шляхом проведення навчань.

TELEGRAM ВРАЗЛИВИЙ ДО КОНТРОЛЮ З БОКУ РОСІЙСЬКИХ СПЕЦСЛУЖБ – WIRED

Другого лютого видання Wired оприлюднило статтю, в якій стверджує, що месенджер Telegram, який багато хто вважає безпечним через анонімність користувачів, швидше за все зазнав втручання російських спецслужб. російські дисиденти ставали предметом уваги поліції, за умов, які, здається, можна пояснити лише співпрацею Telegram з російською владою.

ЗВІТ ПРО ДІЯЛЬНІСТЬ APT ЗА ЧОТИРИ ОСТАННІ МІСЯЦІ 2022 РОКУ

Звіт компанії ESET містить інформацію про акторів, пов'язаних з Китаєм, Іраном, Північною Кореєю та рф. У частині щодо росії йдеться про те, що «пов'язані з нею групи APT продовжували брати активну участь в операціях, спрямованих проти України, розгортаючи деструктивні програми-вимагачі та вайпери. Серед багатьох інших випадків ми виявили сумнозвісну групу Sandworm, яка використовувала раніше невідомий вайпер проти енергетичної компанії в Україні. Групи APT зазвичай керуються державою або спонсорованими нею акторами. Описана атака сталася у жовтні, в той самий період, коли російські війська почали завдавати ракетних ударів по енергетичній інфраструктурі України. І хоча ми не можемо продемонструвати, що ці події були скоординовані, це свідчить, що Sandworm і військові сили росії мають схожі цілі».

У звіті описано невідомий раніше NikoWiper, який було використано для атаки на енергетичну компанію в Україні.

БІЛОРУСЬКЕ ХАКЕРСЬКЕ УГРУПОВАННЯ ОПРИЛЮДНИЛО ЧИСЛЕННІ ДАНІ РОСКОМНАГЛЯДУ

Дамп розміром 335 ГБ, опублікований вночі 15 лютого групою, яка називає себе Білоруськими кіберпартизанами, містить файли та електронні листи відділу головного радіочастотного центру роскомнагляду.

За повідомленням угрупування, роскомнагляд збирав інформацію щодо протестів в Україні та Казахстані. Матеріали на цю тему можна знайти у Телеграм-каналі угрупування. Раніше агентство Рейтерс повідомило, що роскомнагляд запустив інструмент Oculus, який дозволить йому моніторити інтернет для виявлення ознак небажаних повідомлень та організації протестів.

GOOGLE ДАЄ ОЦІНКУ ПЕРШОМУ РОКУ КІБЕРВІЙНИ

16 лютого кібербезпекові підрозділи Google (Threat Analysis Group, Mandiant та Google Trust & Safety) оприлюднили свої висновки щодо основних тенденцій року протистояння. Серед них:

- підтримувані російським урядом зловмисники доклали значних зусиль, щоб отримати перевагу в кіберпросторі, але результати часто неоднозначні;
- росія активно поєднує кібер та інформаційну складову у проведенні своїх ІПСО;
- війна спричинила помітні зміни в східноєвропейській кіберзлочинній екосистемі (наприклад розділилися через політичну прихильність і геополітику), що матиме довгострокові наслідки.

ЗБОЇ В РОБОТІ ВЕБСАЙТІВ КІЛЬКОХ НІМЕЦЬКИХ АЕРОПОРТІВ

Робота вебсайтів щонайменше трьох німецьких аеропортів була порушена 16 лютого, через день після того, як серйозний збій в IT системі Lufthansa затримав тисячі пасажирів в аеропорту Франкфурта. Серед постраждалих аеропорти Дюссельдорфа, Нюрнберга та Дортмунда. Є підозри, що збій був наслідком DDoS атаки.

15 лютого проросійське хакерське угруповання Killnet повідомило російським ЗМІ, що несе відповідальність за збій у Lufthansa. Очільник угруповання KillMilk заявив, що атаку було здійснено у відповідь на рішення канцлера Німеччини Олафа Шольца передати України танки «Леопард».

Lufthansa, однак, звинуватила в збої пошкоджені широкосмугові кабелі, помилково перерізані на залізничній лінії під час будівельних робіт. Це не перший випадок, коли Killnet приписує собі успіхи на тлі системних збоїв і кібератак, які, ймовірно, не відбулися або були невдалими.

Тим часом угруповання під назвою «Анонімний Судан» взяло на себе відповідальність за кібератаки на німецькі аеропорти. «У Німеччині знову нельотна погода», – повідомили хакери в Telegram, розмістивши список своїх ймовірних жертв.

ХАКЕРИ ЗЛАМАЛИ ДЕЯКІ СИСТЕМИ ОПОВІЩЕННЯ В РОСІЇ ТА ПОШИРИЛИ ІНФОРМАЦІЮ ПРО ФАЛЬШИВУ ЗАГРОЗУ

23 лютого невстановлені хакери зламали системи низки радіостанцій в росії (включаючи Relax FM, Avatoradio, Yumor FM і Comedy Radio), а також систему розсилки SMS-повідомлень та поширили через них сигнали про загрозу повітряного удару. Повідомлення поширилось на низку російських міст: П'ятигорськ, Тюмень, Воронеж, Казан, Нижній Новгород, Магнітогорськ, Старий Оскол, Уфа та Новоуральськ.

TRUSTWAVE ПІДБИВАЄ ПІДСУМКИ ПЕРШОГО РОКУ КІБЕРВІЙНИ

24 лютого кібербезпекова компанія Trustwave оприлюднила свої висновки з першого року кібервійни. На думку її спеціалістів, кіберкомпонента не була наскільки помітною, як цього очікували. Крім того, існувало помітне занепокоєння, що кіберактивність обох сторін може «виплеснутись» на інші країни та їх цифрові інфраструктури. Водночас поки що ці загрози реалізовані лише частково. Основний висновок полягає в тому, що кібератаки не грали помітну роль у війні, але допомогли кожній стороні збирати велику кількість розвідувальних даних.

Експерти компанії закликають не недооцінювати кіберможливості росії – хоча їй і не вдалось організувати помітних кібератак із впливом на фізичний простір, однак вони теж навчаються у цій війні та можуть атакувати з використанням нових TTPs. Також Trustwave повертається до ідеї запровадження певних правил для кіберпротистоянь, в тому числі на базі «Талліннського посібника» (Tallin Manual).

УКРАЇНСЬКИЙ ДОСВІД ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ МАЄ БУТИ ВИКОРИСТАНИЙ США ДЛЯ ПОЛІПШЕННЯ ВЛАСНОЇ КІБЕРБЕЗПЕКИ – CSIS

24 лютого експерти CSIS оприлюднили своє бачення щодо стратегічних напрямків поліпшення кіберстійкості критичної інфраструктури та органів державної влади в США. Вони особливо звертають увагу на необхідність врахування досвіду України у цьому питанні, а також на більш ефективне управління ризиками, наголошуючи на тому, що «кібербезпека це управління ризиками, а не спроба їх усунення».

Також серед важливих елементів стійкості вони визначають: обмін інформацією, інвестиції в інфраструктуру, впровадження архітектури нульової довіри, державно-приватне партнерство, проведення кібернавчань (ТТХ), більше уваги до фахівців з кібербезпеки.

ВІЙНА РОСІЇ ПРОТИ УКРАЇНИ РУЙНУЄ ЕКОСИСТЕМУ КІБЕРЗЛОЧИНЦІВ

Відповідно до звіту Insikt Group, опублікованому 24 лютого, у східноєвропейській кіберзлочинній спільноті такі групи, як Conti, розпалися. Частина її членів висловили підтримку, а частина розкритикували вторгнення москви в Україну. росія також постраждала від «кібервитоку мізків», оскільки деякі з найбільш частих користувачів даркнет в росії були мобілізовані до армії, що призвело до зниження активності в російськомовному даркнеті.

Recorded Future також оцінює, що краудсорсингова активність, ймовірно, зіграє певну роль у подальшій війні між рф та Україною, що може мати економічні наслідки. За оцінками дослідників, кіберзлочинність, як у СНД, так і в усьому світі, вступає в нову еру нестабільності внаслідок війни росії проти України.

ВИДАННЯ SECURITYWEEK ОПРИЛЮДНИЛА СВОЇ ОЦІНКИ ПЕРШОГО РОКУ КІБЕРВІЙНИ

Журналісти видання, на базі власних оцінок та компіляції інших схожих звітів у своїй статті від 24 лютого, роблять висновок, що хоча росія системно посилювала свою кіберактивність, але їй не вдалось досягнути помітних результатів в цих зусиллях. Україна ж навпаки продовжує нарощувати свій кіберзахист.

Також серед висновків:
- російська кіберактивність проти України була значною і не зменшується;
- активність російськомовних хакерських спільнот знизилась;
- спостерігається «відтік мізків» з-поміж російських кіберфахівців (якісь можуть бути мобілізовані, але частина виїхала з країни);
- хактивізм (крауд хактивізм) набув нового поштовху через діяльність таких груп як KillNet;
- український телекомсектор показав свою стійкість перед обличчям фізичних та кіберзагроз;
- Україна ефективно моніторить нові загрози;
- важливі системи перенесені у хмару;
- українські кіберспеціалісти виявились ефективнішими ніж російські.

DDOS-АТАКИ ЗАЛИШАЮТЬСЯ НАЙБІЛЬШ ПОШИРЕНИМ ІНСТРУМЕНТОМ У ПЕРШІЙ СВІТОВІЙ КІБЕРВІЙНІ – ДОСЛІДЖЕННЯ CYBERPEACE INSTITUTE

24 лютого CyberPeace Institute оприлюднив результати свого дослідження щодо розгортання кіберскладової російсько-української війни. Відповідно до їх даних, з 1100 проаналізованих кібератак майже 80% припали на DDoS-атаки. Фахівці організації також підкреслюють, що досить складно зрозуміти справжні масштаби впливу кібероперацій на життя людей і чи є цей вплив помітним.

У 2023 РОЦІ РОСІЙСЬКІ КІБЕРВІЙСЬКА МОЖУТЬ ВДАТИСЬ ДО БІЛЬШ СЕРЙОЗНИХ АТАК – POLITICO

У своїй статті від 25 лютого видання Politico узагальнює наявні оцінки першого року кібервійни (на базі оприлюднених звітів дослідницьких компаній) і робить висновки про можливі тенденції наступного року. Зокрема – небезпека більш серйозних кібератак:

«російські зловмисні актори мали так само мало часу на планування своїх наступальних дій, як і інші суб'єкти у лютому 2022 року. Адже вони так само не були обізнані із реальними планами свого керівництва», – вважає Марк Монтгомері, старший науковий співробітник відділу кібернетичних і технологічних інновацій Фонду захисту демократій.

ТЕМНА УГОДА 2.0: КІБЕРЗЛОЧИННІСТЬ, РОСІЯ ТА ВІЙНА В УКРАЇНІ

INSIKT GROUP опублікувала другий звіт, в якому розглянуто негласні зв'язки між російською федерацією, кіберзлочинцями та самоназваними хактивістами в росії та Східній Європі в контексті російської війни в Україні. Він є продовженням попереднього звіту, за вересень 2021 року «Темна угода: зв'язки між російською державою та злочинними діячами».

Серед висновків звіту:
- залишається дуже ймовірним, що російська розвідка, військові та правоохоронні служби мають давнє негласне взаєморозуміння з кіберзлочинцями, які створюють загрози.

У деяких випадках ці агентства підтримують налагоджені та систематичні відносини з кіберзлочинцями, використовуючи погрози, непряму співпрацю або через вербування.
- цілком ймовірно, що кіберзлочинці діють заодно з росією, координуючи чи посилюючи російські наступальні кібер-інформаційні операції.
- декілька сфер кіберзлочинності зазнали трансформацій у результаті російської війни в Україні. До них належать зміни в ландшафтах загроз шкідливого програмного забезпечення як послуги (MaaS) і програм-вимагачів як послуги (RaaS), зростання шахрайства з платіжними картками з боку росії, зміни в націлюванні на кіберзлочинців та в інфраструктурі чи хостингу тощо.

КІБЕРВІЙНА РОСІЇ ПРОТИ УКРАЇНИ ДАЄ ЖИТТЄВО ВАЖЛИВІ УРОКИ ДЛЯ ЗАХОДУ

Голова ДССЗЗІ України Юрій Щиголь опублікував статтю на Atlantic Council, в якій підсумував деякі уроки, які Україна винесла з досвіду російської кібервійни:

- наслідки кібератак може бути важко утримати в певних рамках. Ті, хто обирає цілі, можуть вважати кібератаки зональною зброєю, на відміну від високоточної зброї;
- кібератаки продовжують знаходитися у «сірій зоні». Їх можна використовувати з меншою кількістю обмежень, ніж кінетичні удари. Їх легше заперечити, і їх важче стримати;
- кібероперації є економними з точки зору робочої сили;
- допоміжні підрозділи можуть зробити важливий внесок у наступальні кібероперації;
- кібероперації важко здійснити, щоб їх підготувати та провести необхідні як час, так і навички.

ВЛАСНИКИ БОТНЕТУ PASSION ПРОПОНУЮТЬ ЙОГО ПОСЛУГИ ПРОРОСІЙСЬКИМ ХАКЕРСЬКИМ ГРУПАМ

Група Passion, пов'язана з Killnet і Anonymous russia, нещодавно почала пропонувати DDoS як послугу проросійським хакерам. Ботнет Passion був використаний під час атак 27 січня, спрямованих проти медичних установ в США, Португалії, Іспанії, Німеччині, Польщі, Фінляндії, Норвегії, Нідерландах і Великобританії як помста за відправлення танків на підтримку України.

У своєму каналі в Telegram група стверджує, що не контролюється і не фінансується російським урядом, і просить своїх підписників пожертвувати «на реалізацію спільної місії». Нову групу описано у Radware Cybersecurity Advisory.

ЗЛОВМИСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ПОВ'ЯЗАНЕ З РОСІЄЮ, МАЛО НЕ ВИВЕЛО З ЛАДУ ЕЛЕКТРИЧНІ ТА ГАЗОВІ ОБ'ЄКТИ США МИНУЛОГО РОКУ

Як розповів журналістам Роберт М. Лі, який є засновником і генеральним директором компанії Dragos, що допомагає компаніям реагувати на кібератаки, хакери з групи, яку Dragos називає «Chernovite», використовували шкідливе програмне забезпечення в перші тижні війни в Україні, щоб спробувати знищити «близько дюжини підприємств з виробництва електроенергії та рідкого природного газу в США».

Лі підкреслив, що через цю атаку інфраструктура США була ближче до відключення, ніж коли-небудь до того. Лі описав зловмисне програмне забезпечення як «інструмент рівня держави для воєнного часу». Він не сказав, чи насправді під час атаки зловмисне програмне забезпечення було встановлено в цільових мережах, чи хакери були лише близькі до проникнення в системи.

Політика Dragos полягає у тому, щоб не пов'язувати хакерські угруповання з державами, але інші дослідники згадане вище шкідливе програмне забезпечення швидше за все пов'язано з рф.

ДАТСЬКІ ЛІКАРНІ ПОСТРАЖДАЛИ ВІД КІБЕРАТАКИ «АНОНІМНОГО СУДАНУ»

Вебсайти дев'яти лікарень Данії перестали працювати ввечері 27 лютого після DDoS-атак з боку групи, яка називає себе Anonymous Sudan. Влада Данії повідомила, що хоча сайти й не працювали, надання медичних послуг перервано не було. Через кілька годин було оголошено, що роботу сайтів було відновлено.

Угруповання Anonymous Sudan заявило у Telegram, що атаки відбулися «через спалення Корану», маючи на увазі інцидент у Стокгольмі, під час якого громадянин Данії та Швеції Расмус Палудан, описаний Guardian як «ультраправий політик і антиісламський провокатор» підпалив священну книгу перед посольством Туреччини.

9. РІЗНЕ

ДОСЛІДНИК СПРОБУВАВ КУПИТИ ДАНІ ПРО ПСИХІЧНЕ ЗДОРОВ'Я. ЦЕ ВИЯВИЛОСЯ НАПРОЧУД ЛЕГКО

Відповідно до дослідження Стенфордської Школи державної політики Університету Дьюка, опублікованого 13 лютого, конфіденційні дані про психічне здоров'я продаються маловідомими брокерами за кілька сотень доларів і без особливих намагань приховати особисту інформацію, таку як імена та адреси.

Деякі з брокерів обходилися з конфіденційними даними особливо безцеремонно. Один не висував жодних вимог щодо використання інформації, яку він продавав, і пропонував продати імена та адреси людей з «депресією, біполярним розладом, проблемами тривоги, панічним розладом, раком, посттравматичним стресовим розладом, обсесивно-компульсивним розладом і розладом особистості, а також осіб, які перенесли інсульт, і дані про їхню расову та етнічну приналежність», – йдеться у звіті.

Брокери даних розвинулися у значну, але приховану індустрію, яка не регулюється державою, і громадяни не мають жодної можливості зробити так, щоб інформація про них не потрапляла до рук брокерів.

ЦИВІЛЬНІ ХАКЕРИ МОЖУТЬ СТАТИ ВІЙСЬКОВИМИ ЦІЛЯМИ, ПОПЕРЕДЖАЄ ЧЕРВОНИЙ ХРЕСТ

Цивільні особи, які йдуть у кіберпростір для участі у військових діях між росією та Україною, можуть бути законно піддані військовим діям у відповідь, попередив високопосадовець Міжнародного комітету Червоного Хреста (МКЧХ) Мауро Віньяті.

Сьогодні «будь-хто, хто має смартфон», може брати участь у кібервійні, сказав Віньяті. «Цифровізація також змінила концепцію віддаленості», – додав він, тобто «хоча люди можуть бути фізично видалені з театру бойових дій, вони знаходяться лише в одному кліку від цифрового поля бою». Це створює ребус у розмежуванні, хто є цивільним, а хто є активним учасником війни.

«Заохочення участі цивільного населення в кібердіяльності під час збройного конфлікту може підірвати захист цивільного населення, яке має бути звільнене від наслідків збройного конфлікту. Ось чому МКЧХ наполегливо рекомендує державам змінити тенденцію до цивілізації цифрового поля битви», – сказав Віньяті під час виступу на Мюнхенській конференції з безпеки.

ПЕРВИННІ МІРКУВАННЯ ЩОДО РЕГУЛЮВАННЯ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ, ТАКОГО ЯК CHATGPT

Автори аналітичної записки розглядають ризики, які може нести в собі використання генеративного штучного інтелекту в різних галузях.
Перша категорія ризиків походить від того, що компанії бажають інтегрувати можливості генеративного ШІ до комерційних продуктів. Але у такому випадку, ані самі компанії, ані розробники не контролюють, ані процес генерації, ані помилки, які можуть статися в процесі.

Друга категорія ризиків походить від зловмисного використання ШІ з боку державних та недержавних акторів. Автори пропонують можливі способи пом'якшення таких ризиків.