НКЦК

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

CYBER DIGEST

Огляд подій в сфері кібербезпеки,
квітень 2023

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

Підготовлено за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»

Створення цієї публікації стало можливим завдяки підтримці американського народу, наданій через Агентство США з міжнародного розвитку (USAID). Погляди авторів, висловлені у цій публікації, не обов'язково відображають погляди USAID або Уряду США.

ЗМІСТ

ОСНОВНІ ТЕНДЕНЦІЇ

У квітні дослідники приділяли багато уваги атаці на ланцюжок постачання з боку північнокорейських хакерів проти компаній корпоративного телефонного зв'язку під назвою 3CX. Дослідники відзначали, що приватним компаніям вдалось зупинити цю атаку, що знаменує значний прогрес з часів атаки Solar Winds. Також, дослідники відзначали складність самої атаки, що являла собою каскад атак на ланцюжки постачань. Це був перший випадок такої атаки й це вказує на значне зростання можливостей північнокорейських хакерів. Одночасно жертвами того ж корейського угруповання стали декілька OKI в США та Європі.

ЄС продовжує заходи з реформи законодавчої основи власної кібербезпеки. Прийняття Закону про кіберсолідарність ЄС впровадить важливі додаткові елементи захисту інформаційних систем ЄС перед зростаючими ризиками за загрозами з боку іноземних суб'єктів, передусім – росії. Створення мережі SOC, створення кіберрезерву для швидкої мобілізації кваліфікованого людського ресурсу, а також впровадження інструментів фінансових компенсацій для учасників кіберпротистоянь – все це може допомогти ЄС створити більш адаптовану до поточних загроз модель безпеки.

Міжнародна співпраця стає все більш практично орієнтованою та охоплює не лише обмін технічною інформацією між відповідними підрозділами, але й оприлюднення спільних підходів до важливих проблем. Лише цього місяця відбулась презентація низки спільних документів: про безпеку розумних міст, принципів secure-by-design, дослідження кібератак російських APT угрупувань (на прикладі APT28), а Сінгапур та Франція розпочали співпрацю щодо використання AI у кібербезпеці. Розуміючи важливість цього напрямку США все частіше звертається до ідеї запровадження більш цілісної власної кампанії міжнародної кібердопомоги, в тому числі з акцентом на Тайвань.

Деструктивна кіберактивність пришвидшує темпи впровадження жорсткіших вимог кібербезпеки по всьому світу. CISA поширила оновлену модель зрілості для нульової довіри. Міністерство оборони США готується до впровадження жорсткіших вимог щодо виконання субпідрядниками CMMC. Великобританія вперше комплексно розповіла про власну модель активних (наступальних) дій в кіберпросторі проти зловмисних акторів.

Експерти попереджають, що все частіше зловмисні групи націлюються на мережеве обладнання ключових брендів (передусім – Cisco), сподіваючись таким чином закріпитись у мережах та здійснювати ефективніші шпигунські чи диверсійні операції. Також увага таких злочинців постійно прикута до ICS. Експерти вказують, що все частіше хакерам вдається реалізувати атаки проти таких систем (наприклад – проти ізраїльських іригаційних систем) або вони шукають таку можливість. Цьому сприяє той факт, що промислові системи не часто оновлюють підходи до безпеки, а замінити їх на більш безпечні буває складно.

Українська сторона продовжує нарощувати спроможності своїх фахівців у сфері кібербезпеки. Так, під егідою НКЦК проводяться тренінги для співробітників OKI по управлінню вразливостями (VDP), укладено меморандум про співпрацю Держспецзв'язку та CYBER RANGES для підвищення кваліфікації працівників у сфері кіберзахисту, проведено вже другі всеукраїнські змагання з кібербезпеки UA30CTF.

Продовжуються зміни в законодавчому полі. У квітні Україна затвердила спільний для всіх державних установ порядок реагування на кіберінциденти та кібератаки, прийнято рішення про створення Національного реєстру резервування державних інформаційних ресурсів, ухвалено постанову КМУ щодо використання Платформи для швидкого створення і керування державними реєстрами.

У фокусі уваги українських посадовців – пошук рішення щодо визначення поняття «кібервійна». На думку представників державних структур це дозволить притягнути до відповідальності тих, хто чинить воєнні злочини проти України. Ця ідея дискутується як на загальноукраїнському, так і міжнародному рівні (в межах серії конференцій, у яких взяли участь українські спеціалісти).

Міжнародні кібербезпекові організації продовжують викриття російської зловмисної кіберактивності та її джерел. У квітні оприлюднено декілька досліджень щодо підрядників фсб та гру, які створюють для цих організацій інструменти атак на критичну інфраструктуру демократичних країн чи проведення дезінформаційних кампаній для їх населення. Викрито декілька підтримуваних кремлем хакерів, що ведуть шпигунську кампанію проти дипломатичних служб країн ЄС і НАТО.

російська кіберактивність продовжує зростати. В той час як такі угрупування як KillNet своїми DDoS-атаками не можуть серйозно порушити роботу важливих систем, інші групи шукають можливостей проведення складніших та комплексних операцій. Наприклад, це спроби атак на мережеву інфраструктуру, використання вразливостей в обладнанні Cisco, створення нових ransomware, атаки на енергокомпанії, кампанії проти дипломатичних представництв. Швидше за все цих спроб буде ставати все більше, а російська кіберактивність буде лише зростати.

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

CISA ПРОВЕЛА ШОСТИЙ НАЦІОНАЛЬНИЙ МІСЯЦЬ ДОБРОЧЕСНОСТІ ЛАНЦЮЖКА ПОСТАЧАННЯ

6 квітня CISA запустила проведення 6-го Національного місячника доброчесності ланцюга постачання – серії освітніх заходів для різних стейкхолдерів, щоб привернути увагу до проблеми безпеки ланцюгів постачання та надати їм інструменти щодо зменшення загроз від такого типу атак. Хоча програма орієнтована на широке коло стейкхолдерів, але основні цільові групи – малий і середній бізнес.

МІНІСТЕРСТВО ОБОРОНИ США ПЛАНУЄ ПЕРЕВІРЯТИ ВСІХ СУБКОНТРАКТОРІВ НА ДОТРИМАННЯ CMMC

6 квітня стало відомо, що Міністерство оборони США готується до модифікації стандартного контракту в частині стандартної норми DFARS 7021, яка вимагає у підрядників дотримання вимог моделі кіберзрілості CMMC. До останнього часу для низки підрядників була доступна схема самооцінки та добровільного підтвердження відповідності. Відтепер, Міністерство оборони буде проводити незалежне власне підтвердження такої відповідності. Все це буде вимагати від субпідрядників більш виважено та відповідального поставитись до власної кібербезпеки.

США РОЗГЛЯДАЮТЬ МОЖЛИВІСТЬ ВВЕДЕННЯ ЖОРСТКІШИХ ОБМЕЖЕНЬ ПРОТИ KASPERSKY LAB

7 квітня стало відомо, що Міністерство торгівлі США розглядає можливість додаткових обмежень щодо російської компанії Kaspersky Lab на додачу до вже введених обмежень щодо використання цих продуктів у федеральних відомствах.

ANSSI ОПУБЛІКУВАЛА ЗВІТ ПРО СВОЮ ДІЯЛЬНІСТЬ 2022 РОЦІ

У квітні 2023 року французька ANSSI опублікувала звіт про свою діяльність у 2022 році. Серед ключових здобутків які відзначені у звіті:

- запуск регіональної інкубаційної програми CSIRT;
- публікація Панорами кіберзагроз 2021 р.;
- ухвалення директиви NIS2;
- перші національні TTX REMPAR22 та запуск MonServiceSécurisé.

ЕНН КІСТ-БАТЛЕР СТАНЕ НОВИМ ДИРЕКТОРОМ GCHQ

11 квітня було повідомлено, що чинного керівника британської служби GCHQ Джеремі Флемінга у травні 2023 року замінить Енн Кіст-Батлер. Вона стане першою жінкою на цій посаді та сімнадцятим керівником агентства. Зараз вона працює заступницею генерального директора MI5 і відповідає за оперативну, розслідувальну та захисну роботу MI5. Досвід роботи в системі MI5 становить понад 30 років.

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ І КОНГРЕС ПРАЦЮЮТЬ НАД ОФІЦІЙНОЮ ПРОГРАМОЮ КІБЕРДОПОМОГИ США

Як 12 квітня повідомив посол з особливих доручень Бюро кіберпростору та цифрової політики Державного департаменту США Натаніель Фік, Держдеп у співпраці з Конгресом працюють над створенням механізмів для надання допомоги іншим країнам для запобігання та відновлення після кібератак. Фік повідомив, що йдеться про цілісний підхід: «Це кошти. Це програмне забезпечення. Це підвищення потенціалу, навчання людей. Але це також … концептуальна допомога. Це організаційна допомога. Це культурна допомога». Разом з тим, сума, яку буде виділено на такі потреби, залишається невизначеною. США балансуватимуть свої пріоритети та свої можливості.

ЄС ЗРОБИВ ЩЕ ОДИН КРОК У ПРИЙНЯТТІ ЗАКОНУ ПРО КІБЕРСОЛІДАРНІСТЬ

18 квітня Європейська комісія прийняла пропозицію щодо Закону про кіберсолідарність ЄС. Закон передбачатиме створення Європейського кіберщита, який має стати загальноєвропейською інфраструктурою, що складається з національних і транскордонних центрів безпеки (SOC) по всьому ЄС. Також документ передбачає:

- тестування суб'єктів у найбільш критичних секторах (охорона здоров'я, транспорт, енергетика тощо) щодо їх потенційних вразливостей;
- створення кіберрезерву ЄС, який складається зі служб реагування на інциденти від надійних провайдерів послуг, які на основі завчасно укладеного договору готові втрутитися на запит держави-члена або установ Союзу, органів і агенцій у разі значного чи масштабного інциденту кібербезпеки;
- надання фінансової підтримки для тих випадків, коли держава-член може запропонувати підтримку іншій державі-члену.

СЕНАТ США ПЛАНУЄ РОЗГЛЯНУТИ ЗАКОН ПРО КІБЕРБЕЗПЕКОВУ СТІЙКІСТЬ ТАЙВАНЮ

20 квітня двопартійна ініціативна група представила проєкт Закону про кібербезпекову стійкість Тайваню. Він має зобов'язати Пентагон посилити свою кіберактивність та співпрацю з Тайванем з метою убезпечення його від китайської кіберактивності. Як описав мету закону один з його ініціаторів – «закон має озброїти Тайвань до зубів у сфері кібербезпеки».

Пентагон вже запланував низку проєктів для кібербезпекової допомоги Тайваню, на які поки не отримано бюджетного фінансування: 184 мільйони доларів США на розвиток наступального кіберпотенціалу, 90 мільйонів доларів США на кібербезпеку мереж та 39 мільйонів доларів США створення партнерського середовища для проведення спільних місій.

НІМЕЧЧИНА ПЕРЕВІРЯЄ ЙМОВІРНІСТЬ ВИКОРИСТАННЯ ОБЛАДНАННЯ HUAWEI ДЛЯ ВИМКНЕННЯ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ НІМЕЧЧИНИ

21 квітня було повідомлено, що Німеччина розпочала розслідування ймовірності використання технологій регулювання споживання електроенергії виробництва Huawei для вимкнення телекомунікаційних мереж Німеччини. Розслідування розпочалось ще у березні 2023 року через занепокоєння представників безпекових органів, що деякі компоненти виробництва Huawei можуть бути використані проти телекоммереж. Через це Міністерство внутрішніх справ Німеччини попросило мережевих операторів надати список усіх китайських компонентів, «значущих для безпеки». Очікується, що перевірки завершаться в найближчі місяці.

CISA ТА CNMF РОЗПОВІЛИ ПОДРОБИЦІ ПРО ПРОВЕДЕННЯ СПІЛЬНИХ МІСІЙ

25 квітня під час щорічної конференції RSA представники CISA та CNMF розповіли деталі своєї співпраці та обміну інформації. На прикладі декількох відомих випадків (SolarWinds, китайський злам Microsoft Exchange) вони показали як обмін інформацією між відомствами сприяє ефективнішому реагуванню. Так, CNMF ділиться інформацією з CISA щодо іноземних операцій аби посилити можливості останньої у протидії такій ворожій активності в США. Своєю чергою CISA ділиться інформацією про внутрішні кіберінциденти, щоб операції CNMF проти іноземних акторів були ефективніші. Сторони підкреслили, що така співпраця особливо активізувалась останніми роками

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

ОДНА З НАЙБІЛЬШИХ У СВІТІ ПЛАТФОРМ ДЛЯ КІБЕРШАХРАЙСТВА GENESIS MARKET БУЛА ЗНИЩЕНА ПРАВООХОРОННИМИ ОРГАНАМИ

Genesis Market було захоплено 4 квітня під час операції під керівництвом ФБР, в якій брали участь понад десяток міжнародних партнерів. Genesis, який функціонував як універсальний центр для злочинців, продаючи як викрадені облікові дані, так і інструменти для використання цих даних, був пов'язаний з мільйонами фінансово мотивованих кіберінцидентів у всьому світі, від шахрайства до атак програм-вимагачів.

На відміну від своїх конкурентів, Genesis Market надавав злочинцям доступ до «відбитків пальців браузера», які дозволяли їм видавати себе за веббраузери жертв, включаючи IP-адреси, сеансові файли cookie, інформацію про операційну систему та плагіни. Ці «відбитки пальців» дозволяли злочинцям отримати доступ до платформ передплати, таких як Netflix і Amazon, а також до онлайн-банківських послуг, не запускаючи попереджень системи безпеки.

ФБР ОТРИМАЛО ДОСТУП ДО ВНУТРІШНІХ СЕРВЕРІВ GENESIS MARKET

Високопоставлені чиновники ФБР і Міністерства юстиції заявили 5 квітня, що слідчим вдалося знищити кіберзлочинну платформу Genesis Market після ідентифікації та визначення місцеперебування її серверів. Майже 120 людей було заарештовано у всьому світі лише за 24 години після її ліквідації. Сторінки входу всіх трьох чистих вебдоменів Genesis Market були включені до санкційного списку Міністерства фінансів США, у якому було визначено, що Genesis Market знаходиться в росії, разом із вебсайтом .onion, який також використовувала злочинна платформа.

Американські правоохоронці заявили, що операція була безпрецедентною. Разом з тим, попри оголошення, сторінку входу на вебсайт в дарк веб ще не замінили заставкою ФБР, що спонукало дослідників кібербезпеки запитати про природу операції правоохоронних органів і про те, чи бекенд Genesis Market продовжує працювати.

СІМ КРАЇН ОДНОЧАСНО ПОШИРИЛИ НАСТАНОВИ ЩОДО SECURE-BY-DESIGN

13 квітня урядові структури США, Австралії, Канади, Великобританії, Німеччини, Нідерландів і Нової Зеландії опублікували настанову «Зміщення балансу ризиків кібербезпеки: принципи та підходи до Security-by-Design та Default». Настанова закликає виробників програмного забезпечення вжити заходів, необхідних для надання клієнтам лише secure-by-design продуктів та secure-by-default. Крім конкретних технічних рекомендацій, у настанові викладено основні принципи, якими мають керуватись виробники програмного забезпечення при впровадженні безпеки програмного забезпечення в процеси проєктування перед розробкою.

NCSC-UK ТА NSA ОПРИЛЮДНИЛИ ОГЛЯД ОСНОВНИХ ПРАКТИК APT28 ЩОДО ВИКОРИСТАННЯ МАРШРУТИЗАТОРІВ CISCO

18 квітня NCSC-UK та NSA із залученням інформації ФБР та CISA, опублікували спільний звіт про кібербезпеку, в якому висвітлюються тактика, прийоми та процедури (TTP), пов'язані з використанням групою APT28 (в/ч 26165 Головного розвідувального управління Генштабу російської федерації) маршрутизаторів Cisco. Цей кібератор продовжує використовувати відому вразливість маршрутизатора Cisco, щоб здійснювати проведення розвідки та розгортання зловмисного програмного забезпечення для неавтентифікованого доступу.

США, ВЕЛИКА БРИТАНІЯ, АВСТРАЛІЯ, КАНАДА ТА НОВА ЗЕЛАНДІЯ ОПУБЛІКУВАЛИ НАЙКРАЩІ ПРАКТИКИ КІБЕРБЕЗПЕКИ ДЛЯ РОЗУМНИХ МІСТ

19 квітня урядові кібербезпекові структури США, Великої Британії, Австралії, Канади та Нової Зеландії випустили спільний посібник з найкращими практиками кібербезпеки для розумних міст. Посібник містить:

- огляд ризиків для розумних міст, включаючи розширені та взаємопов'язані поверхні атак;
- ризики ланцюга постачання (ІКТ);
- підвищення рівня автоматизації роботи інфраструктури.

Щоб захиститися від цих ризиків, партнери пропонують три основні рекомендації: безпечне планування та проєктування, проактивне управління ризиками в ланцюзі постачання і операційна стійкість.

РОСІЯ ТА КИТАЙ ПРОСУВАЮТЬ ІДЕЮ НОВОЇ МІЖНАРОДНОЇ КОНВЕНЦІЇ ПРО КІБЕРЗЛОЧИННІСТЬ

21 квітня у Відні на п'ятій сесії спеціального комітету з Конвенції ООН про кіберзлочинність росія та Китай спробували знову посунути питання прийняття Конвенції ООН про кіберзлочинність («Протидія використанню інформаційних та комунікаційних технологій з кримінальною метою»). росія просуває цю оновлену ідею з 2017 року (до того основний акцент робився на проєкт Конвенції про міжнародну інформаційну безпеку).

Формально документ спрямований на розв'язання проблем міжнародної взаємодії під час розслідування чи попередження кіберзлочинів. Однак дискусія, що триває між демократичними та авторитарними країнами, стосується включення або не включення в цей документ відсилок до поваги прав людини, права на честь та гідність, на справедливий суд та неможливість екстрадиції людей в ті країни, які можуть переслідувати їх не за кіберзлочини, а за політичні чи інші переконання.

СІНГАПУР ТА ФРАНЦІЯ БУДУТЬ СПІЛЬНО РОЗВИВАТИ МОЖЛИВОСТІ AI У КІБЕРЗАХИСТІ

24 квітня було оголошено про угоду між Міністерством оборони Сінгапуру (Mindef) і Міністерством збройних сил Франції (MOAF), яка передбачає співпрацю двох країн у потенційних дослідженнях щодо використання штучного інтелекту для геопросторового аналізу, обробки природної мови, аналізу комп'ютерних загроз тощо. Дослідження відбуватимуться в межах спільного дослідницького центру, який став першою лабораторією в Сінгапурі, яку Mindef створив разом з іншою країною.

НАТО ПРОВЕЛО В ЕСТОНІЇ НАЙБІЛЬШІ У СВІТІ НАВЧАННЯ З КІБЕРБЕЗПЕКИ

Об'єднаний центр передових технологій з кібероборони НАТО (CCDCOE), який знаходиться в Таллінні, 18-21 квітня провів найбільші у світі навчання з кіберзахисту Locked Shields 2023. У них взяли участь приблизно 3 000 осіб.

«Locked Shields» — це навчальні навчання «червона команда проти синьої команди», у яких «сині команди» складаються з країн-членів CCDCOE та їхніх країн-партнерів; «синя команда» має захищати критичну інфраструктуру від кібератак «червоної команди».

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

RILIDE: НОВЕ ШКІДЛИВЕ РОЗШИРЕННЯ ДЛЯ БРАУЗЕРА ДЛЯ КРАДІЖКИ КРИПТОВАЛЮТ

4 квітня компанія Trustwave SpiderLabs повідомила, що виявила новий штам зловмисного програмного забезпечення під назвою Rilide. Воно спрямоване на браузери на базі Chromium, такі як Google Chrome, Microsoft Edge, Brave та Opera.

Зловмисне програмне забезпечення Rilide маскується під легітимне розширення Google Drive і дозволяє зловмисникам здійснювати широкий спектр дій, включаючи моніторинг історії вебперегляду, створення скріншотів і впровадження шкідливих сценаріїв для виведення коштів з різних бірж криптовалют.

ЕКСПЕРТИ ПОПЕРЕДЖАЮТЬ ПРО RANSOMWARE «РОРШАХ» З УНІКАЛЬНО ШВИДКИМ ШИФРУВАННЯМ УРАЖЕНИХ СИСТЕМ

Дослідники ізраїльської фірми Check Point виявили нову програму-вимагач, яку назвали Rorschach. Їхня група реагування на інциденти виявила її під час розслідування атаки проти компанії, що базується у США. Сергій Шикевич, менеджер групи аналізу загроз у Check Point Research, сказав, що Rorschach є «найшвидшим і одним із найдосконаліших програм-вимагачів, які ми бачили досі».

У звіті, опублікованому 4 квітня, компанія заявила, що Rorschach виглядає унікальним, не має жодних збігів, які могли б легко віднести його до будь-якого відомого штаму програм-вимагачів, і не має бренду, типового для більшості груп програм-вимагачів.

ЗІРВАНА АТАКА ПІВНІЧНОЇ КОРЕЇ ДЕМОНСТРУЄ ШЛЯХ, ПРОЙДЕНИЙ З ЧАСІВ SOLARWINDS

Як 4 квітня повідомило видання Politico, спроба Пхеньяна проникнути в ланцюжок постачання програмного забезпечення відомої компанії корпоративного телефонного зв'язку під назвою 3CX не привернула особливої уваги, оскільки приватні кібербезпекові компанії переважно задушили її в зародку.

Видання описує як саму атаку, так і реакцію приватного сектора, відзначаючи з одного боку прогрес північнокорейських хакерів, а з іншого – те, наскільки виросла майстерність спільноти кіберзахисників.

СЛУЖБА КРИМІНАЛЬНИХ СПРАВ ВЕЛИКОБРИТАНІЇ ВИЗНАЄ, ЩО «ОБСЛУГОВУВАННЯ ВЕБСАЙТУ» БУЛО КІБЕРІНЦИДЕНТОМ

6 квітня служба кримінальної документації Великобританії ACRO (служба поліції, яка надає британцям довідки з детальною інформацією про судимості) визнала, що «необхідне технічне обслуговування вебсайту», про яке вона заявляла протягом понад двох тижнів, насправді було необхідним у відповідь на інцидент кібербезпеки. Характер інциденту поки не розголошується.

ХАКЕРІВ З ІРАНУ СПІЙМАЛИ НА ПРОВЕДЕННІ ДЕСТРУКТИВНИХ АТАК ПІД ПРИКРИТТЯМ ПРОГРАМ-ВИМАГАЧІВ – MICROSOFT

Як 7 квітня повідомила Microsoft Threat Intelligence, іранське державне угруповання, відоме як MuddyWater, було помічено за здійсненням деструктивних атак на гібридні середовища під виглядом операції з вимагання. Атаки здійснювалися як на локальну, так і на хмарну інфраструктуру у партнерстві з іншим кластером активності, що розвивається, під назвою DEV-1084.

«Хоча зловмисники намагалися замаскувати цю діяльність під звичайну кампанію програм-вимагачів, дії, які унеможливлюють відновлення, демонструють, що кінцевою метою операції є знищення та збій», – повідомив Microsoft.

MuddyWater – це ім'я, присвоєне актору з Ірану, якого уряд США публічно пов'язав із Міністерством розвідки та безпеки країни (MOIS). Відомо, що він активний принаймні з 2017 року.

ПІВНІЧНОКОРЕЙСЬКІ ХАКЕРИ ПОВ'ЯЗАНІ З АТАКОЮ НА ЛАНЦЮЖОК ПОСТАЧАННЯ 3CX – MANDIANT

Як 11 квітня повідомила компанія Mandiant, ґрунтуючись на своєму розслідуванні про вторгнення 3CX і атаку на ланцюг постачання, ця активність належить кластеру під назвою UNC4736. Mandiant з високою впевненістю оцінює, що UNC4736 пов'язана з Північною Кореєю.

ЗЛОВМИСНИКАМ З LOCKBIT МАЙЖЕ ВДАЛОСЬ СТВОРИТИ RANSOMWARE ДЛЯ MAC

17 квітня одразу декілька кібербезпекових організацій та експертів заявили про те, що ними було виявлено працюючий варіант програми ransomware для комп'ютерів Mac з процесором Arm. За розробкою стоїть пов'язане з росією злочинне угрупування LockBit. Водночас наразі цей вірус має обмежені можливості для поширення та реалізації. Він використовує недійсний цифровий підпис, а це означає, що його нелегко запустити в настільній операційній системі Apple.

ПІВНІЧНОКОРЕЙСЬКІ ХАКЕРИ ЗАСТОСУВАЛИ ПОДІБНУ ДО МАТРЬОШКИ КАСКАДНУ АТАКУ НА ЛАНЦЮГ ПОСТАЧАННЯ ПРОТИ 3CX

20 квітня компанія Mandiant опублікувала додаткове розслідування. «Це перший випадок, коли ми спостерігали численні атаки на ланцюг постачання програмного забезпечення», – сказав журналістам головний технічний директор компанії Чарльз Кармайкл на брифінгу перед публікацією звіту. «Це просто демонструє підвищений рівень кібернаступальних можливостей північнокорейських загроз».

У звіті йдеться про те, що компанії вдалося ідентифікувати початковий вектор атаки. Проте розслідування атаки ще триває.

FIN7 СТВОРИЛО НОВЕ СІМЕЙСТВО ЗЛОВМИСНИХ ПРОГРАМ MINODO, ЯКИМ КОРИСТУЮТЬСЯ ЕКСЧЛЕНИ CONTI

27 квітня, IBM Security X-Force повідомило про виявлення нового сімейства зловмисних програм Minodo. На думку дослідників його створено розробниками, які тісно пов'язані з групою кіберзлочинців FIN7. Колишні члени синдикату Trickbot/Conti активно використовують Minodo принаймні з кінця лютого 2023 року, щоб розмістити в уражених системах або викрадач інформації Project Nemesis, або інші ефективніші бекдори, такі як Cobalt Strike. Дослідження показує не лише детальний аналіз шкідливого ПЗ, але і складні зв'язки, які виникають між кіберзлочинними групами в процесі реалізації їх задумів.

РОЗРОБНИК ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ 3CX БУВ СКОМПРОМЕТОВАНИЙ В РЕЗУЛЬТАТІ ПЕРШОЇ У СВОЄМУ РОДІ АТАКИ НА ЛАНЦЮЖОК ПОСТАЧАНЬ

Відома журналістка, яка пише на теми технологій та кібербезпеки, Кім Зеттер розкриває деталі атаки на 3CX для осіб без технічного бекграунду. Якщо коротко, хакери спочатку скомпрометували іншого виробника програмного забезпечення та вбудували зловмисне програмне забезпечення в одну з його програм. 3CX було зламано, коли працівник компанії завантажив цю програму на свій комп'ютер. Невідомо, що спонукало працівника завантажити заражене ПЗ.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

CISA ОПРИЛЮДНИЛА ОНОВЛЕНУ МОДЕЛЬ ЗРІЛОСТІ НУЛЬОВОЇ ДОВІРИ

11 квітня CISA поширила другу версію моделі зрілості нульової довіри, яка базується на зауваженнях та пропозиціях (понад 300 пропозицій), які були надані до першої версії (оприлюднена у 2021 році). Оновлена модель зрілості базується на п'яти основних напрямках (стовпах), що мають полегшити її впровадження на практиці: ідентифікація, пристрої, мережі, дані, програми та робочі навантаження.

ANSSI ОПУБЛІКУВАЛА ПАКЕТ ДОКУМЕНТІВ, ЩО МАЮТЬ ДОПОМОГТИ ОРГАНІЗАЦІЯМ ВІДНОВИТИСЬ ПІСЛЯ КІБЕРІНЦИДЕНТІВ

17 квітня французька ANSSI оприлюднила на своєму сайті пакет документів, які описують кроки організації стратегічного, операційного та технічного рівня, які потрібно вжити для відновлення діяльності організації, що постраждала від кіберінциденту. Пакет документів відкритий для зауважень та пропозицій.

СТРАХОВІ КОМПАНІЇ НАМАГАЮТЬСЯ СКОРИСТАТИСЬ НЕЧІТКІСТЮ КІБЕРБЕЗПЕКОВИХ ЗАГРОЗ ЗАДЛЯ УНИКНЕННЯ ВИПЛАТ

20 квітня видання Security Intelligence оприлюднило матеріал, який висвітлює проблемні питання ринку страхування в розрізі кіберзагроз та реалізованих кібератак. Автор посилається на нещодавню заяву компанії Lloyd's, в якій вони зазначили, що їх страхові поліси не покривають випадки кібератак, групами, що спонсоровані державами. Звертається увага на те, що все частіше страхові компанії намагаються знайти аргументи для зменшення простору своїх зобов'язань, в т.ч. користуючись риторикою урядовців та експертів про те, що у світі триває кібервійна, а отже в період війни страхові відшкодування неможливі.

CHATGPT ПОВЕРНУВСЯ В ІТАЛІЮ ПІСЛЯ ТОГО, ЯК РОЗВ'ЯЗАВ ПРОБЛЕМИ З КОНФІДЕНЦІЙНІСТЮ ДАНИХ

29 квітня ЗМІ повідомили, що компанія-розробник ChatGPT – OpenAI – офіційно повернулася до Італії після того, як задовольнила вимоги органів із захисту даних до кінцевої дати 30 квітня 2023 року.

OpenAI опублікувала нові роз'яснення, в яких повідомила, що фільтрує та видаляє таку інформацію, як мова ворожнечі, вміст для дорослих, сайти, які в основному збирають особисту інформацію, і спам. Компанія також підкреслила, що «не шукає активно особисту інформацію для навчання їхніх моделей» і що «не буде використовувати будь-яку особисту інформацію у навчанні для створення профілів людей, зв'язку з ними, реклами, щоб спробувати продавати їм будь-що або продавати саму інформацію».

Заборона тривала з 3 квітня, коли Італійський наглядовий орган із захисту даних Garante per la Protezione dei Dati Personali наказав компанії тимчасово припинити обробку даних користувачів, заявивши, що має намір розслідувати діяльність компанії на предмет того, чи вона незаконно обробляє такі дані в порушення Закону ЄС про Загальний регламент захисту даних (GDPR).

5. КРИТИЧНА ІНФРАСТРУКТУРА

НАСОСНІ СИСТЕМИ PROPUMP AND CONTROLS МАЮТЬ КІЛЬКА СЕРЙОЗНИХ ВРАЗЛИВОСТЕЙ, ЯКІ МОЖУТЬ ПРИЗВЕСТИ ДО ЗНАЧНИХ ПРОБЛЕМ

Дослідник кібербезпеки промислових систем з Zero Science Lab. заявив про виявлення вразливості у насосних системах виробництва ProPump and Controls. Вразливість містить в собі віддалене виконання коду, підробку міжсайтового запиту (CSRF), обхід автентифікації, міжсайтовий сценарій (XSS), ін'єкції команд та низку інших. Зловмисник може використати уразливості, щоб віддалено зламати систему та отримати повний контроль над пристроєм. Це може дозволити їм спричинити збій через DoS-атаку або виконувати різні типи нечесних дій, залежно від того, для чого використовується цільовий контролер. 23 березня CISA опублікувала опис цієї вразливості та набір поради щодо її мінімізації.

ЗВІТ ЩОДО ГЛОБАЛЬНОГО РИНКУ ПОСЛУГ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У 2023 РОЦІ

5 квітня фірма Report Linker оприлюднила звіт щодо процесів на глобальному ринку захисту критичної інфраструктури. Серед них можна відзначити:

- загалом ринок зріс з $137.88 мільярдів у 2022 році до $146.16 мільярдів у 2023, демонструючи зведений річний темп зростання (CAGR) у 6,0%;
- зростання та поширення хмарних технологій та пристроїв Інтернету речей буде підштовхувати зростання ринку захисту критичної інфраструктури у майбутньому;
- у 2022 році Північна Америка була найбільшим регіоном на ринку захисту критичної інфраструктури. Очікується, що Азійсько-тихоокеанський регіон буде регіоном, який найшвидше розвиватиметься в прогнозованому періоді;
- розвиток технологій становить ключовий тренд, що набуває популярності на ринку захисту критичної інфраструктури. Основні компанії, що працюють у сфері захисту критичної інфраструктури зосереджені на розробці технологічно просунутих продуктів, щоб зміцнити свою позицію на ринку.

ВЕЛИКИЙ ВИРОБНИК КОМП'ЮТЕРНИХ КОМПЛЕКТУЮЧИХ MSI ЗАЗНАВ АТАКИ

7 квітня компанія MSI, що займається виробленням материнських плат, графічних процесорів, ноутбуків, ПК та іншого обладнання, поширила заяву, в якій закликала користувачів «отримувати оновлення прошивки/BIOS лише з її офіційного вебсайту» та уникати використання файлів з інших джерел.

Це прозвучало на фоні заяв групи Money Message, що їм вдалось отримати доступ до численних даних компанії (в т.ч. баз даних MSI CTMS і ERP, а також прошивок BIOS). Група погрожувала оприлюднити ці дані, які нібито становлять 1,5 ТБ, якщо MSI не заплатить викуп у розмірі чотирьох мільйонів доларів протягом кількох днів.

ФУНКЦІОНУВАННЯ ІРИГАЦІЙНИХ СИСТЕМ В ІЗРАЇЛІ БУЛО ПОРУШЕНО ХАКЕРСЬКИМИ АТАКАМИ

9 квітня The Jerusalem Post повідомила, що хакери атакували контролери води для іригаційних систем на фермах у долині річки Йордан, а також системи контролю очищення стічних вод, що належать Galil Sewage Corporation. Ферми були попереджені Ізраїльським національним кіберуправлінням перед інцидентом, отримавши вказівки відключити віддалені підключення до цих систем через високий ризик кібератак.

Понад десять ферм у долині Йордану та інших регіонах не змогли цього зробити, і їх контролери води були зламані. Це призвело до тимчасового вимкнення автоматизованих систем поливу, що змусило фермерів перейти до ручного поливу. Ціллю хакерів були програмовані логічні контролери (PLC), виготовлені ізраїльською компанією Unitronics.

У АМЕРИКАНСЬКИХ ПОСАДОВЦІВ Є СУМНІВИ ЩОДО ЦИФРОВОЇ БЕЗПЕКИ МЕРЕЖІ FIRSTNET

12 квітня сенатор США Рон Уайден повідомив, що відповідно до наявних у нього даних (а також з посиланням на неназваного співробітника CISA) є серйозні сумніви у захисті від цифрового втручання мережі FirstNet. FirstNet – це стільникова мережа, створена після атак 11 вересня 2001 року, яка використовується службовцями громадської безпеки, такими як працівники екстрених служб, пожежники та правоохоронні органи. Наразі CISA та NSA не прокоментували заяву сенатора, а представники FirstNet заявили про суворе дотримання всіх вимог безпеки.

ЕНЕРГЕТИЧНИЙ СЕКТОР ЗАЛИШАЄТЬСЯ НА ЧЕТВЕРТОМУ МІСЦІ СЕРЕД НАЙБІЛЬШ АТАКОВАНИХ СЕКТОРІВ – ЗВІТ X-FORCE THREAT INTELLIGENCE INDEX 2023

13 квітня було оприлюднено звіт X-Force Threat Intelligence Index 2023, який концентрується на кіберзагрозах для енергетичної галузі. Найбільшою загрозою для енергетичних організацій у 2022 році була експлуатація програм публічного доступу (public-facing applications), на які припадає 40% усіх заражень. Фішинг спричинив 20% випадків заражень, а ботнети – 19%. Програми-вимагачі склали 15%. Крадіжка даних і вимагання були найбільш часто згадуваними результатами цих атак (23%), а збір облікових даних становить 15% від всіх атак.

ICS СТАЮТЬ ВСЕ ВРАЗЛИВІШИМИ, А КІЛЬКІСТЬ ВИЯВЛЕНИХ CVE В ТАКИХ СИСТЕМАХ ЗРОСТАЄ – TRELLIX

18 квітня Trellix оприлюднив своє дослідження щодо ситуації із виявленими вразливостями (CVE) у промислових системах (ICS). Використовуючи як приклад ситуацію з порушенням роботи сталелитейної компанії Khuzestan Steel Co. у червні 2022 року, що призвело переривання виробництва сталі, паралізувавши послуги в Ірані, спеціалісти Trellix вказують на загрозливу ситуацію, яка складається для сфери ICS.

Важливий висновок: на відміну від більш традиційних IT-систем, ICS мають численні специфічні елементи з рідко оновлюваними програмним забезпеченням. Це створює все зростаючий простір загроз для всіх промислових об'єктів.

ЗЛОМ LAZARUS X_TRADER СТОСУВАВСЯ Й КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Як 21 квітня повідомила Symantec Threat Hunter Team, північнокорейське хакерське угруповання Lazarus, що стоїть за каскадною атакою на ланцюг постачання, спрямованою на 3CX, також зламало дві OKI в енергетичному секторі (в США та Європі) та два інших підприємства, залучені у торгівлі фінансовими інструментами, використовуючи троянську програму X_TRADER. Атаки відбулися з вересня 2022 року по листопад 2022 року.

MITER ПРЕДСТАВИЛА ІНСТРУМЕНТ MITER CALDERA ДЛЯ АНАЛІЗУ КІБЕРРИЗИКІВ ОТ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

24 квітня корпорація MITER презентувала свій новий інструмент – MITER Caldera. Базований на іншій розробці організації MITER ATT&CK ® для ICS інструмент має допомогти OKI швидко та просто протестувати власні OT системи на вразливості, поліпшити діяльність власних синіх та червоних команд, а також емулювати механізми та можливі вектори атаки зловмисників.

6. АНАЛІТИЧНІ ОЦІНКИ

ДОСЛІДЖЕННЯ ЩОДО НТЦ ВУЛКАН, ПІДРЯДНИКА РОСІЙСЬКОГО ГРУ – MANDINAT

На початку квітня з'явилось дослідження кібербезпекової компанії Mandiant щодо діяльності НТЦ Вулкан – одного з підрядників Міністерства оборони російської федерації, але здебільшого російського ГРУ. Дослідження описує випадки виконання робіт цією організацією в інтересах підрозділу 74455 ГРУ, також відомого як Sandworm Team. Ці роботи включали розробку інструментів, навчальних програм та платформу червоної команди для здійснення різних типів наступальних кібероперацій, включаючи кібершпигунство, проведення інформаційних операцій та атак на ОТ промислових структур (передусім залізниць, повітряного та морського транспорту).

ДОСЛІДЖЕННЯ ЩОДО ДІЯЛЬНОСТІ 0DAY TECHNOLOGIES, ОДНОГО З ПІДРЯДНИКІВ ФСБ – RECORD FUTURE

Першого квітня Record Future поширило результати свого розслідування щодо 0Day Technologies (0DT) – одного з підрядників, яких використовує ФСБ для розвитку своїх спроможностей стеження за опонентами влади, проведенням кібератак та поширення дезінформації. Згідно з дослідженням 0DT виконує роботи для підрозділу 71330 ФСБ (він же DragonFly, EnergeticBear, Crouching Yeti), який звинувачували в атаках на критичну національну інфраструктуру США та Великобританії.

Також в інтересах підрозділу 64829 ФСБ 0DT створив Fronton – ботнет Інтернету речей (IOT). Fronton використовується як інфраструктура командування та контролю (C2) для SANA – платформи дезінформації, яка дозволяє користувачам швидко розгортати мережі ботів соціальних мереж. Як прикриття своєї діяльності та для набору співробітників 0DT використовує Московський державний університет (МДУ).

ДЕТАЛЬНИЙ АНАЛІЗ TTPS ROYAL RANSOM ВІД КОМПАНІЇ TRELLIX

Третього квітня кібербезпекова компанія Trellix оприлюднила детальне дослідження щодо Royal Ransom – одного з найбільших гравців ринку ransomware. У ньому описані техніки, тактики та процедури, які використовуються Royal Ransom у своїй діяльності, як саме відбувається атака та як діють злочинці у відносинах з атакованими об'єктами.

ВСЕРЕДИНІ КІБЕРЗЛОЧИННОГО БІЗНЕСУ – ДОСЛІДЖЕННЯ TREND MICRO

Третього квітня компанія Trend Micro Incorporated оприлюднила дослідження, в якому розглянуто форми організації кіберзлочинного бізнесу в залежності від його розміру. Як зазначають дослідники, кримінальні організації швидко професіоналізуються. В дослідженні окреслено три типи організацій залежно від розміру:

- Групи кіберзлочинців часто організовуються як компанії. Складніші структури розвиваються, коли група збільшує свій дохід і членство.
- Великі злочинні групи дуже складні за організацією, але їх небагато. Більшість ландшафту складається з невеликих груп злочинців, які отримують помірні доходи. Вони складаються з кількох членів, які працюють за моделлю партнерства.
- Більші злочинні групи мають корпоративні відділи, такі як відділи кадрів (HR) та інформаційних технологій (IT). У них навіть можуть бути програми для працівників, наприклад, визнання зразкового працівника місяця та оцінка ефективності.
- Великі злочинні організації відрізняються не лише розміром. Ними, як правило, важче керувати, вони стикаються з більшою кількістю політичних питань і мають справу з більшою кількістю поганих виконавців. Також вони стикаються з великою кількістю проблем довіри. Розширення без розв'язання цих питань негативно впливає на злочинну організацію в довгостроковій перспективі.

БРИТАНСЬКІ НАСТУПАЛЬНІ КІБЕРОПЕРАЦІЇ: ВІДПОВІДАЛЬНА КІБЕРПОТУГА НА ПРАКТИЦІ

Національні кіберсили Великобританії (NCF) 4 квітня опублікували звіт, в якому стверджують, що їх діяльність (наступальні кібероперації) кардинально відрізняється від діяльності супротивників. Якщо китайські та російські операції вони характеризують, як «безрозсудні», наступальна хакерська діяльність Британії має бути «підзвітною», «точною» та «вивіреною».

Звіт містить найдетальніше пояснення британського наступального кіберпотенціалу на сьогодні. Презентуючи його, агентство заявило, що рухається у вірному напрямку, «забезпечуючи більшу прозорість і вдаючись до ширшої взаємодії з громадськістю, ніж це робилося раніше». Також воно заявило, що це є важливою частиною «демонстрації прагнення Великої Британії бути відповідальною та демократичною кібердержавою».

ЩО ПОТРІБНО ЗНАТИ ПРО ГРУПУ ХАКЕРІВ ANONYMOUS SUDAN

У звіті, опублікованому на CYE Blog 4 квітня, описується діяльність угруповання Anonymous Sudan. Дослідники стверджують, що воно знаходиться у Судані та є частиною мережі Anonymous. Мотивації та цілі Anonymous Sudan не дуже зрозумілі, але їхні дії часто спрямовані на підвищення обізнаності про конкретні політичні та соціальні проблеми. З початку російсько-української війни ця група стверджувала, що підтримує російську сторону, тому часто атакує українські цілі. У звіті зазначається, що деякі дослідники вважають угруповання російським, але на сьогодні нема чітких доказів цього.

ЄВРОПА ОНОВЛЮЄ СВІЙ АРСЕНАЛ КІБЕРБЕЗПЕКИ

У статті, опублікованій 5 квітня, Янна Бранколіні (Janna Brancolini) наголошує на важливій ролі державно-приватного партнерства для убезпечення української банківської та транспортної інфраструктури від російських фізичних та кібератак. Вона стверджує, що акцент ЄС на приватності в його місії з просування кібербезпеки може вбити клин між державними та приватними партнерами, що матиме негативні наслідки для безпеки.

«Успіх України залежав від міцного приватно-державного партнерства та бажання відкинути контрпродуктивні ідеї щодо цифрового суверенітету. Сьогодні питання без відповіді полягає в тому, чи засвоїли європейські політики ці уроки. Чи будуть вони прагнути зміцнити приватно-державне партнерство? Чи вони відреагують, запровадивши контрпродуктивну хмарну сертифікацію та схеми локалізації даних?» – питає авторка тексту.

ПЕРЕБАЛАНСУВАННЯ ВІДПОВІДАЛЬНОСТІ: ІМПЛЕМЕНТАЦІЯ НАЦІОНАЛЬНОЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ США

6 квітня в Atlantic Council відбулась дискусія щодо імплементації національної стратегії кібербезпеки США за участі виконуючої обов'язки національного кібердиректора Кемби Волден, директорки Агентства з кібербезпеки та безпеки інфраструктури Джен Істерлі, посла з особливих доручень Бюро кіберпростору та цифрової політики Державного департаменту США Натаніеля Фіка та головного помічник заступника генерального прокурора Міністерства юстиції США Маршалла Міллера. Під час дискусії американські топ-посадовці представили своє бачення основних стовпів стратегії, основні зміни в підходах у порівнянні з попередніми документами та бачення шляхів імплементації документу.

READ THE MANUAL LOCKER: ПРИВАТНИЙ ПОСТАЧАЛЬНИК RAAS

13 квітня компанія Trelix опублікувала звіт, в якому досліджує угруповання Read The Manual (RTM), що надає послуги ренсомвер на замовлення. Вони діють переважно проти корпоративного сектору та дотримуються дуже жорстких правил.

Банда вимагає від афілійованих гравців залишатися активними або повідомляти про відхід, щоб не пройшло десять днів без сповіщення – у цьому випадку порушник буде заблокований у панелі групи. Для доступу до панелі потрібні логін і пароль для афілійованих осіб, а також введення коду CAPTCHA. Коли користувач увійшов до панелі, він може додати жертв і встановити таймер для оприлюднення даних. Також чітко окреслені цілі, які атакувати недозволенно. Серед них країни СНД, морги, лікарні, організації, що займаються вакциною проти COVID-19.

І хоча є певні підстави вважати, що учасники угруповання мають відношення до різних сторін російсько-української війни, їх діяльність, швидше має фінансові, ніж політичні мотиви.

ЗБІЛЬШЕННЯ АТАК ПРОГРАМ-ВИМАГАЧІВ НА 60%: У БЕРЕЗНІ 2023 РОКУ КІЛЬКІСТЬ ЖЕРТВ НАЙБІЛЬША ЗА ДВА РОКИ

Як 18 квітня повідомила Corvus Threat Intel, у березні 2023 року компанія зафіксувала 452 нові жертви програм-вимагачів на сайтах витоку інформації. Це найвища кількість, зафіксована протягом місяця, за останні два роки. 22% заявлених жертв програм-вимагачів у березні були пов'язані з кампанією банди програм-вимагачів CL0P, націленої на GoAnywhere.

По секторах, кількість атак на телекомунікації зросла на 800%. Половина цих організацій розташована в Сполучених Штатах, інші – у Великобританії, Франції, Лівані та Камеруні. У лікарнях та закладах охорони здоров'я кількість атак зросла на 750%. Багато організацій, які постраждали, були медичними технологічними компаніями. Урядові установи зазнали зростання кількості атак на 220% порівняно з лютим. Ці цілі були атаковані не менше ніж 10 різними групами програм-вимагачів, включаючи BianLian, Lockbit, Play і Stormous.

СПОНСОРОВАНІ ДЕРЖАВОЮ ЗЛОВМИСНІ АКТОРИ НАЦІЛЮЮТЬСЯ НА МЕРЕЖЕВУ ІНФРАСТРУКТУРУ – ЗВІТ CISCO TALOS

18 квітня безпекова компанія Cisco Talos оприлюднила своє дослідження, в якому доводить, що різноманітні зловмисні актори (передусім російські та китайські) сконцентрувались на різноманітних пристроях маршрутизації/комутації (передусім – виробництва Cisco). Вони є ідеальною мішенню для зловмисників, які хочуть бути непомітними і мати доступ до важливих для них мереж інших організацій. Ключова рекомендація дослідників – вчасне оновлення програмного забезпечення і дотримання рекомендацій виробників обладнання в частині кібербезпеки.

ВІДСУТНІСТЬ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ (MFA) Є ОДНІЄЮ З НАЙСЛАБШИХ МІСЦЬ БЕЗПЕКИ ПІДПРИЄМСТВ – CISCO TALOS

26 квітня Cisco Talos підбила підсумок тенденцій реагування на інциденти за перший квартал 2023 року. Одним з важливих висновків дослідників є те, що відсутність багатофакторної автентифікації (MFA) залишається однією з найбільших перешкод для безпеки підприємств. Майже 30 відсотків інцидентів стосувались організацій, які або не мали MFA, або мали його лише в кількох облікових записах і критично важливих службах.

ENISA ОПУБЛІКУВАЛА ОЦІНКУ СТАНДАРТІВ КІБЕРБЕЗПЕКИ ШТУЧНОГО ІНТЕЛЕКТУ

27 квітня ENISA оприлюднила свій звіт «Кібербезпека ШІ та стандартизація». Звіт містить огляд стандартів – опублікованих, розроблюваних і запланованих – та їх оцінку з метою виявлення потенційних прогалин у сфері стандартизації ШІ. Звіт зосереджений на аспектах кібербезпеки штучного інтелекту та запропонованому Європейською комісією минулого року проєкті «Закон про штучний інтелект». Один з висновків звіту – необхідним і доцільним є створення схеми сертифікації кібербезпеки ЄС щодо ШІ.

ЧИ МОЖЕ ІНІЦІАТИВА БІЛОГО ДОМУ ЗМУСИТИ ТЕХНОЛОГІЧНІ КОМПАНІЇ ПИСАТИ БЕЗПЕЧНІШИЙ КОД?

Автор аналітичного тексту Еліас Гролл висловлює сумніви, що одне з важливих завдань, яке ставлять перед собою адміністрація Байдена у нещодавно опублікований Національній стратегії кібербезпеки, буде реалізоване. Він не вірить в те, що адміністрація змусить компанії-розробники ПЗ пріоритезувати безпеку над швидкістю шляхом запровадження відповідальності для розробників ПЗ у найближчій перспективі.

Серед перешкод, на думку автора, настрої в Палаті представників Конгресу США, де сьогодні більшість має Республіканська партія, налаштована проти посилення ролі уряду. З іншого боку, на заваді можуть стати технічні питання, пошук відповідей на які може тривати багато років. Серед них, питання, яким чином окреслити «безпечну гавань», тобто умови написання ПЗ, дотримання яких звільнятиме компанії від відповідальності за можливі помилки у коді.

ОГЛЯД ГЛОБАЛЬНОЇ ХМАРНОЇ КОНКУРЕНЦІЇ

З огляду на важливість цифрової сфери для подальшого економічного розвитку та технологічних змін, що впливатимуть на розподіл сил у глобальній системі, Джеймс Ендрю Льюіс (James Andrew Lewis) розглядає тенденції у сфері хмарних обчислень, які є основою цифровізації. Він наголошує на сперечаннях між питаннями розвитку та суверенітету та звертає увагу на плани Китаю створювати свою сферу економічного та технологічного впливу, до якої тяжіють країни Латинської Америки, Африки та Індо-Тихоокеанського регіону, а, також, деякі країни південної Європи.

ЗВІТ ПРО ФІШИНГ І ЗЛОВМИСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ЗА ПЕРШИЙ КВАРТАЛ 2023 РОКУ ВІД КОМПАНІЇ VADE

Як повідомила компанія Vade у звіті, опублікованому 13 квітня, показники фішингу зросли на 102% порівняно з попереднім кварталом.

APRIL 2023 THREAT HORIZONS REPORT ВІД GOOGLE

У звіті порівнюються тактика злочинних хакерських угруповань із хакерами, підтримуваними урядами країн, та зазначається, що останні у перспективі швидше за все розпочнуть здійснювати атаки на хмару, як роблять це звичайні кіберзлочинці.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

НА ЗАСІДАННІ НАЦІОНАЛЬНОГО КЛАСТЕРА КІБЕРБЕЗПЕКИ У ВАРШАВІ ОБГОВОРИЛИ ПИТАННЯ ГАРМОНІЗАЦІЇ СИСТЕМ КІБЕРБЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ІЗ СТАНДАРТАМИ ЄС

У Варшаві відбулося XVIII засідання Національного кластера кібербезпеки на тему: «Гармонізація систем кібербезпеки критичної інфраструктури зі стандартами ЄС». Захід організовано НКЦК спільно з Фондом цивільних досліджень та розвитку США за підтримки Державного департаменту США.

«Це перший Кластер за межами України. На ньому розглядається надзвичайно актуальне питання – гармонізація української системи кібербезпеки зі стандартами ЄС. Але варто зазначити, що в цьому процесі маємо враховувати досвід нашої держави у війні з рф. Тож наше засідання не тільки сприяє глибшому розумінню специфіки сфери кібербезпеки ЄС, а й дозволяє поділитись із нашими партнерами унікальним досвідом України у кібервійні», – сказав заступник Секретаря Ради національної безпеки і оборони Украни Сергій Демедюк, відкриваючи засідання Кластера.

Учасники заходу обговорили питання щодо особливості законодавства у сфері кібербезпеки України та ЄС, практичні кроки для зближення, важливість державно-приватного партнерства в цьому процесі, а також розглянули найкращі практики та досвід Європейського Союзу. У засіданні взяли участь близько 300 представників державного сектору, міжнародної та донорської спільноти, посольств та приватних установ.

С. ДЕМЕДЮК: ВИЗНАЧЕННЯ ПОНЯТТЯ «КІБЕРВІЙНА» СПРИЯТИМЕ ПРИТЯГНЕННЮ ДО ВІДПОВІДАЛЬНОСТІ ТИХ, ХТО ЧИНИТЬ ВОЄННІ ЗЛОЧИНИ ПРОТИ УКРАЇНИ, НЕ СТУПАЮЧИ НА ЇЇ ЗЕМЛЮ

Заступник Секретаря РНБО України Сергій Демедюк взяв участь у щорічній Всеукраїнській науково-практичній конференції, присвяченій розв'язанню проблем управління інформаційною безпекою держави.

У заході, організованому Національною академією СБУ, також взяли участь представники МОУ, СБУ, Генштабу ЗСУ, Нацполіції, ДССЗЗІ, Комітету Верховної Ради України з питань національної безпеки, оборони та розвідки, Київської торгово-промислової палати, НАН України, ЗВО та медіаспільноти.

З-поміж питань, які розглядалися під час конференції, особливу увагу було приділено важливості нормативного визначення поняття «кібервійни».

«Сьогодні кожен відповідно до своїх знань і досвіду визначає поняття «кібервійни». Але жодна країна світу досі не має єдиного чіткого формулювання. Маємо визначитися з поняттям «кібервійна» та його тлумаченням. Це сприятиме притягненню до відповідальності тих, хто чинить воєнні злочини проти України та її громадян, не ступаючи на українську землю», – зазначив заступник Секретаря РНБО України Сергій Демедюк.

Під час конференції учасники обговорили шляхи протидії інформаційним і психологічним впливам рф на українських військових та посилення захисту інформації з обмеженим доступом в умовах війни. Також було запропоновано розпочати унікальне наукове дослідження кібервійни. Для цього планують залучити представників усіх суб'єктів забезпечення кібербезпеки, об'єктів критичної інфраструктури, громадських організацій та наукових установ.

НКЦК ДОСЛІДИВ КІБЕРАТАКИ РОСІЙСЬКОГО УГРУПОВАННЯ APT28, ПОВ'ЯЗАНОГО З ГРУ ГШ МІНОБОРОНИ РФ

Національний координаційний центр кібербезпеки дослідив атаки російського хакерського угруповання APT28, в яких активно використовується критична вразливість CVE-2023-23397. З-поміж основних висновків:

- угрупування APT28 здійснює атаки за допомогою вразливості нульового дня у поштовому клієнті Outlook щонайменше протягом року.
- за цей час жертвами атак стали компанії: оператори газотранспортних систем, приватні підприємства супутникової розвідки та систем радіолокації, установи і організації МЗС та НАТО, компанії розробники та постачальники IT-рішень тощо;
- перша атака була виявлена в березні 2022 року після початку повномасштабного вторгнення. Відтоді зафіксовано ряд атак на підприємства та організації країн Європи та Близького Сходу з використанням нової критичної вразливості.

Детально ознайомитись зі звітом про атаки APT28 з використанням вразливості CVE-2023-23397 можна за посиланням.

В УКРАЇНІ ЗАПУСТИЛИ DEFENSE TECH CLUSTER BRAVE1, ЯКИЙ СТИМУЛЮВАТИМЕ РОЗВИТОК ВІЙСЬКОВИХ ІННОВАЦІЙ ТА ОБОРОННИХ ТЕХНОЛОГІЙ

Міністерство цифрової трансформації, Міністерство оборони, Генеральний штаб Збройних сил України, Рада національної безпеки і оборони, Міністерство економіки та Міністерство з питань стратегічних галузей промисловості презентували defense tech cluster BRAVE1.

Це єдина платформа для співпраці defense tech компаній, держави та військових, а також інвесторів, волонтерських фондів, медіа і всіх, хто допомагає наближати перемогу через технології. Будь-яка людина, стартап або компанія зможуть представити свою ідею або продукт BRAVE1 та здобути грант від держави. Таким чином, бізнес отримає можливості для розвитку, а наші військові — технології перемоги.

Компанії defense tech індустрії отримають організаційний та експертний супровід розробок, а також доступ до акселераторів та інкубаторів. Ідеться про системну роботу над удосконаленням розробок, підвищення знань щодо масштабування бізнесу, набуття цінності для інвесторів, менторство.

Досвід взаємодії державних і приватних стейкхолдерів у межах BRAVE1 та підтримка галузі не лише допоможе армії, а й стане потужним продуктом для експорту. Адже українські defense tech рішення доводять свою ефективність у найзапекліших боях.

Подати власний проєкт та отримати доступ до військової експертизи, грантів й інших можливостей, які надає кластер, можна за посиланням: https://brave1.gov.ua/

І. ВІТЮК: МІЖНАРОДНИЙ ТРИБУНАЛ МАЄ РОЗГЛЯДАТИ КІБЕРАТАКИ РФ НА УКРАЇНУ ЯК ВОЄННИЙ ЗЛОЧИН

Результати кримінальних проваджень СБУ щодо російських кібератак на Україну мають розглядатися Міжнародним трибуналом як воєнний злочин. Це дозволить притягнути до відповідальності вище військово-політичне керівництво країни-агресора, зокрема і спецслужб. Про це заявив начальник Департаменту кібербезпеки СБУ Ілля Вітюк на Всеукраїнській науково-практичній конференції, яку щороку проводить Національна академія Служби безпеки.

«Сьогодні, коли постало питання Міжнародного трибуналу щодо злочинів рф в Україні, то і російські кібератаки мають розглядатися як воєнний злочин. Наприклад, ті ж кібератаки на об'єкти енергетики, особливо в зимовий час. Виведення цих систем із ладу спричиняє жертви серед цивільного населення. А це – справжній воєнний злочин», – наголосив Ілля Вітюк.

«Якщо говорити про персональну відповідальність за ці злочини, то нести її мають не лише виконавці, а й люди, які віддають подібні злочинні накази. Наприклад, має бути покараний директор

НКЦК РОЗПОЧАВ СПІВПРАЦЮ З НАЦІОНАЛЬНИМ ДИРЕКТОРАТОМ З ПИТАНЬ КІБЕРБЕЗПЕКИ РУМУНІЇ ЗАДЛЯ СТВОРЕННЯ БЕЗПЕЧНОГО КІБЕРПРОСТОРУ ТА ПРОТИДІЇ КІБЕРАТАКАМ

Національний координаційний центр кібербезпеки та Національний Директорат з питань кібербезпеки Румунії підписали меморандум про взаєморозуміння у сфері співробітництва з кібербезпеки.

«російські хакери – це загроза не лише для України, а й для всього світу. Вони продовжують атакувати наших партнерів – держави, які надають всебічну підтримку Україні для перемоги у цій війні. Тому об'єднання зусиль і координація у протидії кіберзагрозам надзвичайно важливі сьогодні. Крім того, Україна нині здобуває унікальний досвід, яким ми готові ділитися з міжнародною спільнотою задля забезпечення миру та безпеки у кіберпросторі», – зазначив заступник Секретаря РНБО України Сергій Демедюк.

Співпраця в рамках меморандуму передбачає обмін досвідом і найкращими практиками у сфері кібербезпеки, участь в освітніх та науково-технічних проєктах та обмін інформацією щодо кіберінцидентів, способів виявлення вразливостей та реагування на кіберзагрози тощо.

МІНЦИФРА, ДЕРЖСПЕЦЗВ'ЯЗКУ ТА МІНІСТЕРСТВО ЦИФРОВІЗАЦІЇ ЯПОНІЇ ПІДПИСАЛИ МЕМОРАНДУМ ПРО СПІВПРАЦЮ

Україна та Японія домовились про співпрацю у сфері цифрової трансформації – Мінцифра, Держспецзв'язку та Міністерство цифровізації Японії вперше уклали тристоронній меморандум. Це початок потужного діджитал-співробітництва між країнами.

Документ підписали на онлайн-зустрічі Віцепрем'єр-міністра з інновацій, розвитку освіти, науки та технологій — Міністра цифрової трансформації України Михайла Федорова з Міністром цифровізації Японії Таро Коно.

«Уряд Японії зараз сфокусувався на покращенні сфери держсервісів. Тому півтора року тому там з'явилося Міністерство цифровізації. В Україні цей процес триває вже понад 3 роки – будуємо найзручнішу цифрову державу, запускаємо нові онлайн-послуги навіть попри виклики війни. Переконаний, що японсько-українські відносини мають великий потенціал, адже обмін цифровими кейсами між нашими країнами буде корисний обом сторонам», – зазначив Михайло Федоров.

У межах меморандуму Японія допомагатиме Україні розвивати інновації та посилювати кіберзахист. Сьогодні Україна протистоїть ворогу не лише на фронті, а й у кіберпросторі. Технологічні рішення Японії допоможуть посилити українські цифрові кордони та захистити інформаційні системи об'єктів критичної інфраструктури. Також під час зустрічі міністри домовилися про обмін найкращими практиками розвитку IT-галузі та розбудови електронного уряду.

ПІДПИСАНО МЕМОРАНДУМ ПРО СПІВПРАЦЮ У СФЕРАХ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ МІЖ МІНОБОРОНИ УКРАЇНИ ТА КОМПАНІЄЮ INTERNET2.0

Заступник Міністра оборони України з питань цифрового розвитку, цифрових трансформацій та цифровізації Віталій Дейнега та співзасновник австралійської компанії INTERNET2.0 Роберт Поттер підписали Меморандум про співробітництво між оборонним відомством та компанією INTERNET2.0.

Меморандум офіційно підтверджує наміри сторін розвивати співробітництво за напрямом обміну досвідом у сферах зв'язку та інформатизації, впровадження й розвитку новітніх інформаційних технологій і процесів та цифровізації у сфері оборони. Метою підписання документу є також вивчення і демонстрація інноваційних технологій у сфері оборони, програмного та апаратного забезпечення, розробником якого є австралійська компанія, зокрема Cloaking Firewall, Malcore.

Серед іншого, основні зусилля підписантів будуть зосереджені на вивченні можливостей використання інформаційно-аналітичної системи Advanced Practices, розробником якої є INTERNET2.0, для покращення ситуаційної обізнаності, оцінки загроз, прогнозування кризових ситуацій, реагування та відновлення.

КІБЕРНАВЧАННЯ, ТРЕНІНГИ ТА ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ У СФЕРІ КІБЕРЗАХИСТУ – ДЕРЖСПЕЦЗВ'ЯЗКУ ТА CYBER RANGES УКЛАЛИ МЕМОРАНДУМ ПРО СПІВПРАЦЮ

Держспецзв'язку відвідали представники провідної міжнародної компанії CYBER RANGES Corp., яка спеціалізується на розробці технологічних рішень та проведенні навчань із кіберзахисту з використанням технологій наступного покоління і високоточного моделювання.

Заступники голови Держспецзв'язку Віктор Жора та Олександр Потій ознайомили керівника відділу маркетингу та розвитку бізнесу CYBER RANGES Марчелло Хінксман-Аллегрі з можливостями тренінгового центру, що діє на базі Кіберцентру UA30, а також розповіли про роботу Урядової команди реагування на комп'ютерні надзвичайні події CERT-UA та про важливу роль Держспецзв'язку у забезпеченні кіберзахисту України.

Під час візиту між Держспецзв'язку та CYBER RANGES був укладений меморандум про співробітництво, який серед іншого передбачає:

- обмін інформацією, досвідом та найкращими практиками у сфері кіберзахисту, проведення навчальних курсів, тренінгів, спільних навчань на платформі CYBER RANGES PCTE;
- просвітницьку діяльність щодо кіберзагроз;
- участь у програмах підвищення кваліфікації у сфері кіберзахисту, організації кваліфікаційної експертизи та проведення процедур присвоєння / підтвердження професійних кваліфікацій за профстандартами України у сфері кіберзахисту на базі технологій CYBER RANGES тощо.

АПАРАТ РНБО УКРАЇНИ ЗА ПІДТРИМКИ ДЕРЖДЕПАРТАМЕНТУ США ПРОВІВ П'ЯТИДЕННИЙ ВОРКШОП ДЛЯ СПЕЦІАЛІСТІВ ПІДПРИЄМСТВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Апарат Ради національної безпеки і оборони України провів п'ятиденний семінар «Безпека та стійкість критичної інфраструктури» для фахівців об'єктів критичної інфраструктури державного та приватного секторів України.

Захід відбувся за сприяння Міністерства національної безпеки США, Агентства з кібербезпеки та безпеки інфраструктури США (CISA) та Фонду цивільних досліджень і розвитку США (CRDF Global).

Мета тренінгу – розбудова спроможностей та стійкості українських об'єктів критичної інфраструктури, а також їх взаємодії як на рівні окремих об'єктів, так і на загальнодержавному рівні.

Семінар включав різноманітні інтерактивні сесії, лекції, дискусії та групові заняття під керівництвом експертів CISA. Крім того, учасники мали змогу обмінятися досвідом та взяти участь у дискусіях щодо спільних зусиль у відповідних галузях.

У заході взяли участь близько двадцяти учасників. З-поміж них представники Апарату РНБО України, Держспецзв'язку, СБУ, ДСНС, Міністерства охорони здоров'я України, Міністерства енергетики України, «Укртрансгазу», «Укренерго», «Нафтогазу України», Центру безпекових досліджень Національного інституту стратегічних досліджень тощо.

ПРЕДСТАВНИКИ НКЦК ОЗНАЙОМИЛИ СЛУХАЧІВ НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ОБОРОНИ УКРАЇНИ З ФУНКЦІОНУВАННЯМ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ ТА МОЖЛИВОСТЯМИ НКЦК

Понад 50 слухачів курсу підготовки офіцерів стратегічного рівня для сектора безпеки і оборони Національного університету оборони України імені Івана Черняховського ознайомилися із засадами функціонування і розбудови системи кібербезпеки України, а також технічними можливостями Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України.

У зустрічі на технічному майданчику НКЦК взяли участь керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Наталія Ткачук та спеціалісти НКЦК.

Під час заходу йшлося про національну систему кібербезпеки України та важливість координуючої ролі та місця НКЦК. Військовослужбовцям продемонстрували технічні можливості НКЦК, які використовуються фахівцями для оперативного виявлення та аналізу кіберінцидентів. Також обговорено проблемні питання сфери кібербезпеки та шляхи їх вирішення.

Особливу увагу було приділено питанню координації під час реагування на кібератаки. Фахівці НКЦК поінформували слухачів про технічні можливості та інструменти для виявлення ознак кібератак. Також наголошувалося на важливості взаємного обміну інформацією між усіма суб'єктами забезпечення кібербезпеки України, зокрема з використанням платформи MISP НКЦК.

НКЦК ПРОВІВ НАВЧАННЯ «УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ» ДЛЯ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ ЕНЕРГЕТИЧНОГО СЕКТОРУ УКРАЇНИ

Національний координаційний центр кібербезпеки за підтримки CRDF Global в Україні з 13 березня по 20 квітня 2023 року провів навчальний захід із серії «Управління вразливостями» (VDP).

У десятій програмі взяли участь понад 30 профільних технічних спеціалістів, які представляли 20 організацій енергетичного сектору України, з-поміж яких Міністерство енергетики України, НАЕК «Енергоатом», НЕК «Укренерго», регіональні обленерго тощо. Учасники показали високу зацікавленість у вирішенні завдань на фінальному CTF. Переможці шеститижневого тренінгу для працівників енергетичного сектору отримали призи, які допоможуть їм і далі розвивати свої професійні навички.

Метою таких заходів є покращення практичних навичок з виявлення вразливостей в інформаційних системах та забезпечення комплексного кіберзахисту в основних суб'єктах забезпечення кібербезпеки, державних установах, об'єктах критичної інфраструктури та інших організаціях у рамках державно-приватного партнерства.

ДЛЯ СИЛ БЕЗПЕКИ Й ОБОРОНИ ПРОВЕЛИ ПЕРШИЙ СЕРТИФІКОВАНИЙ ТРЕНІНГ З OSINT ТА HUMINT

Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації (ДержНДІ), який діє при Держспецзв'язку, в партнерстві з Італійською командою з питань безпеки, тероризму та управління надзвичайними ситуаціями (ITSTIME) провели перший сертифікований тренінг з розвідки на основі даних із відкритих джерел (OSINT) та пошуку інформації з використанням персональних контактів (HUMINT) для фахівців органів сил безпеки та оборони України.

Під час тренінгу італійські фахівці зосередили увагу на стратегіях і практиках використання цифрових технологій та соціальних мереж ворогом з метою збору інформації в інтернеті, deep web та dark net. А також навчали українських фахівців орієнтуватися в цифрових мережах противника, визначати можливі цілі та проводити інформаційні операції у ворожих мережах.

Учасники також вдосконалювали навички моніторингу різних типів загроз, формування стратегій запобігання та розроблення планів реагування на надзвичайні ситуації, ризики та кризи. Цей сертифікований тренінг, поміж іншого, поглиблює розуміння важливості стратегічної комунікації та запобігання ворожій пропаганді в умовах гібридної війни.

КОМАНДА CERT-UA ВИБОРОЛА ТРОФЕЙ QUANTICO CYBER EAGLE НА КІБЕРНАВЧАННЯХ КОРПУСУ МОРСЬКОЇ ПІХОТИ США

Чотири команди Державної служби спеціального зв'язку та захисту інформації України за запрошенням Корпусу морської піхоти США взяли участь у навчаннях з кібербезпеки «Quantico Cyber Eagle», які в кінці березня пройшли на полігоні CYBER RANGES technology у місті Квантіко (США).

Мета заходу, в якому взяли участь 11 команд, – навчання елітних кіберфахівців, здатних проводити сучасні оборонні операції і протистояти розумному і винахідливому противнику. Такі виклики вимагають від кіберфахівців тренувань у симуляційних середовищах, що відображають загрози, які постійно змінюються.

Основою сценарію стала імітація кібератаки спецслужб рф на посольство вигаданої країни НАТО. Схожість тактик, технік та процедур, які використовуються для проведення реальних кібератак на нашу країну та країни НАТО, дала українським командам можливість попрактикуватися та відточити свої вміння оперативного реагування на кіберінциденти. Також учасники могли перевірити навички командної роботи в середовищі моделювання з високою точністю, яке відтворювало тактику та методи, що використовують ворожі суб'єкти в кіберпросторі.

НКЦК ДОЛУЧИВСЯ ДО МІЖНАРОДНОЇ КОНФЕРЕНЦІЇ «КІБЕРБОРОТЬБА: РОЗВІДКА, ЗАХИСТ ТА ПРОТИДІЯ»

Керівник управління забезпечення діяльності НКЦК профільної служби Апарату РНБО України Сергій Прокопенко 20 квітня 2023 року взяв участь у міжнародній конференції «Кіберборотьба: розвідка, захист та протидія». Захід організовано Військовим інститутом телекомунікацій та інформатизації імені Героїв Крут за підтримки Національного координаційного центру кібербезпеки, Командування військ зв'язку та кібербезпеки ЗСУ та міжнародних партнерів CRDF Global, E-Governance Academy (Естонія), Regional Cyber Defence Center (Литва) та Nikola Vaptsarov Naval Academy (Болгарія).

Мета конференції – аналіз шляхів співпраці наукових колективів європейських країн у сучасних проєктах збереження миру та безпеки, а також використання сучасних навчальних кіберполігонів та платформ для проведення навчання фахівців з кібербезпеки.

«Зараз необхідно зосередитися на поглибленому аналізі досвіду України у кібервійні та можливостях прогнозування розвитку ситуації. І цим досвідом ми обов'язково маємо ділитися з нашими міжнародними партнерами, взаємодіючи на всіх рівнях – міждержавному, приватному, та академічному. Адже тільки така співпраця сприятиме створенню нових підходів для протидії нашому спільному ворогу та допомагатиме ефективніше попереджувати майбутні кібератаки», – зазначив Сергій Прокопенко, відкриваючи захід.

Участь у конференції взяли представники сектору безпеки та оборони України, США, Норвегії та Естонії, які обговорили питання щодо криптографічних рішень кібербезпеки, інтелектуального аналізу інцидентів та сигнальних структур в кіберпросторі, підтримки рішень для забезпечення кіберзахисту тощо.

ІННОВАЦІЇ ТА ІНІЦІАТИВИ З ЦИФРОВОЇ ТРАНСФОРМАЦІЇ В ЗСУ: ВІТАЛІЙ ДЕЙНЕГА ВЗЯВ УЧАСТЬ У КОНФЕРЕНЦІЇ НАТО TIDE SPRINT

Заступник Міністра оборони України з питань цифрового розвитку, цифрової трансформації та цифровізації Віталій Дейнега взяв участь у конференції НАТО TIDE Sprint, організованої у Норвегії (м. Ліллегаммер) Командуванням НАТО з питань трансформації.

На пленарному засіданні Віталій Дейнега поінформував учасників про поточні інновації та ініціативи з цифрової трансформації на підтримку Збройних Сил України. Зокрема, про розробку рішень ситуаційної обізнаності, використання безпілотних літальних апаратів та нестандартні підходи до застосування ЗСУ в умовах ведення російською федерацією повномасштабної війни.

Заступник Міністра оборони України з питань цифрового розвитку, цифрової трансформації та цифровізації наголосив на важливості тісної взаємодії з цивільним сектором, а також на зосередженні та врахуванні технологічних потреб військовослужбовців в районі ведення бойових дій.

УКРАЇНА ГОТОВА ДО ПОГЛИБЛЕННЯ СПІВПРАЦІ З ПАРТНЕРАМИ У СФЕРІ КІБЕРЗАХИСТУ

Протидія ворожим військовим кібероперaціям вимагає якісної взаємодії та значного інтелектуального ресурсу, які необхідно примножувати. Україна здобула унікальний практичний досвід за дев'ять років війни та готова будувати більш щільну взаємодію з колегами з Чорноморського регіону, зокрема через участь у спільних науково-дослідних R&D та навчальних проєктах.

Про це йшлося під час експертної дискусії на Чорноморській безпековій конференції Міжнародної Кримської Платформи в Бухаресті, Румунія. «Ми маємо поглиблювати нашу співпрацю. Я маю на увазі не лише обмін інформацією про події та певними знаннями, а й спільну роботу, участь у спільних науково-дослідних R&D та навчальних проєктах. Разом ми зможемо досягти якісніших результатів», – підкреслив Назар Тимошик, член Урядової команди реагування на комп'ютерні надзвичайні події CERT-UA.

ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО СТАЛО ОДНИМ ІЗ КЛЮЧОВИХ ФАКТОРІВ НАШОЇ КІБЕРСТІЙКОСТІ – ЗАСТУПНИК ГОЛОВИ ДЕРЖСПЕЦЗВ'ЯЗКУ

Постійна і систематична робота над розвитком державного-приватного партнерства, якому в Держспецзв'язку приділяли значну увагу протягом останніх років, допомогла Україні ефективніше протистояти російським кібератакам. Про це під час панельної дискусії Advancing Public-Private Partnership in Cyber Threat Intelligence and Cyber Crisis Response конференції European Cyber Agora, що проходить у Брюсселі у змішаному форматі, зазначив заступник голови Держспецзв'язку Віктор Жора.

«Взаємодія з приватним сектором для спільної боротьби із загрозами, для посилення нашої спроможності протистояти російській кіберагресії, нарощування кадрового потенціалу є одним із ключових факторів нашої стійкості під час повномасштабної війни», – підкреслив під час онлайн-виступу Віктор Жора.

Він поділився українським досвідом налагодження ефективних механізмів взаємодії у форматі «держава–приватний сектор» та закликав учасників конференції приділяти більше уваги такій співпраці, поглиблюючи вже наявне партнерство та розвиваючи нові напрямки.

УКРАЇНА ПОЧИНАЄ БУДУВАТИ СИСТЕМУ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІДПОВІДНО ДО НАЙКРАЩИХ СВІТОВИХ ПРАКТИК ТА ЧИННИХ ВИМОГ ЄВРОПЕЙСЬКОГО ЗАКОНОДАВСТВА

Про це розповів заступник голови Держспецзв'язку Олександр Потій під час участі в панельній дискусії «Захист критичної інфраструктури при майбутній перебудові енергетики». Він зазначив, що Україна вивчає директиви ЄС NIS 2 (EU 2022/2555) та RCE (EU 2022/2557) щодо захисту критичної інфраструктури і співпрацює з країнами, які вже розпочали їхнє впровадження.

Крім того, Україна плідно співпрацює з Американською агенцією з кібербезпеки та захисту критичної інфраструктури (CISA). Саме ця організація має провідний досвід у питаннях захисту ОКІ. Держспецзв'язку та CISA уклали меморандум про співпрацю, вже були проведені навчання відповідно до методики CISA.

Учасники заходу розповіли про те, що однією з головних мішеней ворога під час повномасштабної війни є енергетична інфраструктура. Від жовтня 2022 року по лютий 2023 по українській енергосистемі було випущено 1 500 ракет і дронів-камікадзе, 100 з-поміж них вразили великі енергетичні об'єкти. Внаслідок обстрілів Україна втратила 61% генерації. Для проходження наступної зими потрібно вже зараз активізувати зусилля для підготовки до загроз та захисту енергетичної інфраструктури.

Панельна дискусія відбувалась у межах проєкту EUROSCOPE, що досліджує наближення України до членства в ЄС.

УРЯД ЗАТВЕРДИВ ПОРЯДОК РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

Кабінет Міністрів України постановою затвердив розроблений фахівцями Держспецзв'язку Порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. Документ ухвалений на виконання Плану реалізації Стратегії кібербезпеки України.

Затвердження Порядку дасть можливість формувати процеси реагування на кіберінциденти та кібератаки відповідно до завчасно спланованих заходів із кіберзахисту, які спрямовані на:

- швидке виявлення та захист від кіберінцидентів та кібератак;
- належне інформування про такі події, запобігання, мінімізацію та усунення негативних наслідків;
- виправлення вразливостей, а також відновлення сталості та надійності функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем та інших об'єктів кіберзахисту.

Держспецзв'язку впродовж трьох місяців з дня набрання чинності постанови має затвердити методичні рекомендації щодо реагування суб'єктами кібербезпеки на зазначені у Порядку події у кіберпросторі.

Затвердження Порядку реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі розвиває підходи, які були закладені в організаційно-технічній моделі кіберзахисту, розробленій Держспецзв'язку наприкінці 2021 року.

УРЯД УХВАЛИВ ПОСТАНОВУ ЩОДО ВИКОРИСТАННЯ ПЛАТФОРМИ ДЛЯ ШВИДКОГО СТВОРЕННЯ І КЕРУВАННЯ ДЕРЖАВНИМИ РЕЄСТРАМИ

Команди Мінцифри та Держспецзв'язку працюють над інноваційним рішенням — Платформою для розгортання та супроводження державних електронних реєстрів. Завдяки інструменту міністерства і державні органи швидко й зручно створюватимуть публічні реєстри та керуватимуть ними.

Зараз в Україні є понад 450 державних реєстрів. 80% з них технологічно застарілі і вразливі до кібератак. Платформа для розгортання реєстрів стане основою для цифрової трансформації. Адже всі дані будуть впорядковано зберігатися в реєстрах, що пришвидшить запуск онлайн-послуг та діджиталізацію загалом. На Платформі реєстрів можна не лише створювати нові, а й технічно переробити і поступово переносити застарілі реєстри. Усі зміни фіксуються і відбуваються тільки через бізнес-процеси. Це унеможливлює незаконні зміни даних.

Також для розробки реєстрів на Платформі не потрібні великі команди чи фахівці високого рівня. Опанувати інструменти розробки можна легко і швидко. Для розробників проводитиметься навчання і надаватимуться консультації.

ПОСИЛЮЄМО ЗАХИСТ НАЦІОНАЛЬНИХ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ – ПОСТАНОВА УРЯДУ

Завдання держави – не тільки побудова дієвої системи захисту, а й забезпечення резервування даних для швидкого відновлення у разі потреби. Для цього ще у 2021 році, у межах виконання Стратегії кібербезпеки України, було підтримане рішення щодо створення Національного реєстру резервування державних інформаційних ресурсів, забезпечення роботи та розвитку якого було покладено на Держспецзв'язку.

Уряд ухвалив ще одну важливу у цьому напрямі постанову «Деякі питання функціонування Національного центру резервування державних інформаційних ресурсів», якою затвердили:

- Порядок функціонування Національного центру резервування державних інформаційних ресурсів. У ньому чітко визначені функції та повноваження суб'єктів Національного центру резервування.
- Порядок передання органами державної влади, військовими формуваннями, підприємствами, установами та організаціями резервних копій національних електронних інформаційних ресурсів до Національного центру, а також – механізм їх збереження і доступу до них. В тому числі – в ньому визначено види резервування національних електронних інформаційних ресурсів, вимоги до договорів щодо збереження резервних копій, вимоги до захисту інформації та кіберзахисту під час зберігання, порядок переміщення до закордонних дипломатичних установ України протягом періоду дії воєнного стану та повернення після його закінчення тощо.

«Ухвалена постанова дозволить мінімізувати ризики, забезпечить подальшу безперервність роботи національних електронних інформаційних ресурсів і можливість відновлення даних у разі її пошкодження чи видалення. Наша спільна мета – убезпечення та збереження критично важливої інформації, яка стосується як наших державних органів та підприємств, так і громадян», – зазначає голова Держспецзв'язку Юрій Щиголь.

ДЕРЖСПЕЦЗВ'ЯЗКУ ЗАПРОШУЄ БІЗНЕС ТА ПРОФІЛЬНІ АСОЦІАЦІЇ НАДАТИ ПРОПОЗИЦІЇ ЩОДО РОЗШИРЕННЯ КЛАСИФІКАТОРА ПРОФЕСІЙ З КІБЕРБЕЗПЕКИ

Реформування української професійної освіти у сфері кіберзахисту потребує залучення бізнесу та профільних асоціацій, зокрема до розробки професійних стандартів у сфері кібербезпеки. Про це йшла мова під час зустрічі «Професії та кар'єра у сфері кібербезпеки», що відбулася 5 квітня в Києві.

«Ще кілька років тому в державному класифікаторі професій було тільки дві професії — професіонал з організації інформаційної безпеки і фахівець у сфері захисту інформації. Наразі ми внесли до класифікатора 27 актуальних професій, розробили та затвердили професійні стандарти до шести з них. А цього року плануємо розробити профстандарти для ще 14 професій», – зазначив на заході заступник голови Держспецзв'язку Олександр Потій.

Завдяки внесенню цих профстандартів до Реєстру кваліфікацій, які було розроблено за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури в Україні», заклади вищої освіти можуть скоригувати освітні програми та запровадити відповідні спеціалізації підготовки, а фахівці та роботодавці – здійснювати підбір фахівців за професіями.

СИСТЕМАТИЧНІСТЬ ТА ІНТЕНСИВНІСТЬ РОСІЙСЬКИХ КІБЕРАТАК ЛИШАЄТЬСЯ ВИСОКОЮ – ЗВІТ

Від початку 2023 року, порівняно з попереднім кварталом, знизилась кількість атак проросійських угруповань на комерційний, фінансовий сектор, Уряд та місцеві органи влади, сектор безпеки та оборони. При цьому інтенсивність атак на сектор енергетики та ЗМІ залишається на тому ж рівні.

Про це йдеться у Звіті про роботу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, опублікованому Державним центром кіберзахисту.

Загалом протягом І кварталу 2023 року за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було детектовано 7 мільйонів підозрілих подій інформаційної безпеки (при первинному аналізі); опрацьовано 34 тисячі критичних подій інформаційної безпеки (потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу); зафіксовано та оброблено безпосередньо аналітиками безпеки 202 кіберінциденти.

СБУ ЛІКВІДУВАЛА У КРОПИВНИЦЬКОМУ БОТОФЕРМУ, ЯКА СТВОРИЛА ПОНАД ТРИ ТИСЯЧІ ФЕЙКОВИХ АКАУНТІВ ДЛЯ ІНФОРМДИВЕРСІЙ ПРОТИ УКРАЇНИ

Кіберфахівці Служби безпеки нейтралізували у Кропивницькому ботоферму, яка діяла на користь російських спецслужб. У результаті слідчо-оперативних дій затримано організатора ворожого «осередку». Він масово створював анонімні акаунти у соцмережах і продавав їх через даркнет. Середня вартість одного боту – 200 грн.

Встановлено, що зловмисник створив майже три тисячі фейкових акаунтів, які планував продати на загальну суму понад півмільйона гривень. Основними його «клієнтами» були представники російських спецслужб, а також підконтрольні їм прокремлівські пропагандисти.

Боти потрібні були агресору для «розгону» дезінформації нібито від імені українських громадян про ситуацію на фронті, а також для спроб дискредитації підрозділів Сил оборони. Таким чином ворог намагався розхитувати внутрішньополітичну обстановку в різних регіонах України в умовах війни.

КІБЕРПОЛІЦІЯ ВИКРИЛА ЗЛОВМИСНИКА У ЗБУТІ БАЗ ІЗ ПЕРСОНАЛЬНИМИ ДАНИМИ ГРОМАДЯН УКРАЇНИ ТА ЄС

Чоловік у месенджері продавав відомості, що містили персональні дані понад 300 мільйонів осіб із різних країн. Під час проведення санкціонованого обшуку фігурант перешкоджав діям правоохоронців і завдав тілесних ушкоджень кіберполіцейському. Зловмисника затримали.

36-річний мешканець Нетішину був адміністратором закритих груп і каналів у месенджері Telegram, де здійснював продаж персональних даних громадян України та Європейського союзу. Зокрема у розпорядженні зловмисника були відомості щодо паспортних даних, номерів платників податків, свідоцтв про народження, водійських посвідчень, даних банківських рахунків.

Загалом бази містили персональну інформацію понад 300 мільйонів осіб, громадян України та країн ЄС. В залежності від обсягу даних фігурант просив за них від 500 до 2000 доларів.

Попередньо встановлено, що покупцями були і громадяни країни-агресора. Оплату за продаж баз даних громадянам рф фігурант отримував за допомогою заборонених на території України валют.

У рамках досудового розслідування кримінального провадження за ч. 2 ст. 361-1 (Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут), ст. 362 (Несанкціоновані дії з інформацією, яка обробляється в комп'ютерах, автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї) Кримінального кодексу України та на підставі ухвали суду правоохоронці прийшли до фігуранта для проведення обшуку.

За фактом нападу на кіберполіцейського слідчі Шепетівського районного управління поліції розпочали досудове розслідування за ч. 2 ст. 345 (Погроза або насильство щодо працівника правоохоронного органу) Кримінального кодексу України. Санкція статті передбачає обмеження волі на строк до п'яти років або позбавленням волі на той самий строк. Тривають слідчі дії.

ЗА МАТЕРІАЛАМИ СБУ СУДИТИМУТЬ ДВОХ ЗРАДНИКІВ, ЯКІ ДОПОМАГАЛИ ФСБ ЗДІЙСНЮВАТИ ХАКЕРСЬКІ АТАКИ НА УРЯД УКРАЇНИ

Кіберфахівці Служби безпеки спільно з ДБР та ОГП зібрали доказову базу на ще двох військових-зрадників, які допомагали рф у війні проти України. Фігурантами є двоє колишніх співробітників СБУ в АР Крим, які у 2014 році перейшли на бік ворога і вступили до лав фсб. Там вони увійшли до складу підконтрольного російській спецслужбі хакерського угруповання «Armageddon».

Встановлено, що з 1 січня 2020 до 10 березня 2021 років зловмисники здійснили серію масштабних кібератак на урядові структури України. Під час одного з кіберінцидентів фсб намагалась отримати доступ до секретних даних вищих органів влади нашої держави. Втім, завдяки оперативному реагуванню СБУ, вдалося нейтралізувати наслідки та усунути передумови для проникнення російської спецслужби до урядових інформаційних ресурсів України.

За результатами комплексних заходів правоохоронці встановили причетність обох зрадників до підривної діяльності агресора. Зокрема, у 2021 році кіберфахівці СБУ здійснили безпрецедентну операцію і поіменно встановили зловмисників, перехопили їхні розмови, а також отримали беззаперечні докази їх причетності до кібератак на Україну. І це при тому, що вони використовували власні вірусні програми фсб, а також засоби анонімізації та «прикриття» у мережі Інтернет.

Тоді було встановлено одразу 8 ворожих хакерів, 5 із яких відразу отримали підозру. Наразі правоохоронці закінчили розслідування щодо двох із них. Вони звинувачуються за двома статтями Кримінального кодексу України: ч. 1 ст. 111 (державна зрада) та ч. 2 ст. 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів) та автоматизованих систем). Зловмисникам загрожує до 15 років позбавлення волі.

КІБЕРПОЛІЦІЯ ХАРКІВЩИНИ ВИКРИЛА УЧАСНИКІВ ДВОХ ЗЛОЧИННИХ УГРУПОВАНЬ У ПРИВЛАСНЕННІ МАЙЖЕ ДВА МІЛЬЙОНИ ГРИВЕНЬ ЗА ДОПОМОГОЮ ФІШИНГУ

Зловмисники діяли за аналогічними схемами: отримували дані банківських карт громадян за допомогою фішингових посилань, які копіювали інтерфейс сторінок онлайн-банкінгів, сайтів платформ оголошень, інтернет-магазинів тощо. Від протиправних дій постраждали більше тисячі громадян. Загальна сума збитків, завданих потерпілим, становить майже два мільйони гривень.

Учасників двох злочинних груп викрили співробітники управління протидії кіберзлочинам у Харківській області спільно з Головним слідчим управлінням Нацполіції та за сприяння співробітників служб безпеки Монобанку та ПриватБанку.

В одному угрупованні об'єдналися 13 осіб, які створили та адміністрували спільноту в Telegram, де розміщували інструкції та фішингові посилання для інших членів шахрайської групи. Далі зловмисники в месенджерах розсилали ці посилання під виглядом пропозицій оформлення фінансових виплат, отримання коштів за проданий товар. Дані, введені користувачами на фішингових сайтах, автоматично ставали відомі фігурантам.

Організатор схеми здійснював компрометацію платіжних карток клієнтів банку та за допомогою платіжних систем «виводив» гроші потерпілих на підконтрольні рахунки. Аналогічну схему реалізували й троє жителів Дніпропетровщини.

Відкрито кримінальні провадження за ч. 1, 2 ст. 255 (Створення, керівництво злочинною спільнотою або злочинною організацією, а також участь у ній), ч. 4 ст. 190 (Шахрайство) Кримінального кодексу України. Фігурантам може загрожувати до дванадцяти років позбавлення волі з конфіскацією майна.

«ДРУГ ПРОСИТЬ У БОРГ»: КІБЕРПОЛІЦІЯ ДНІПРОПЕТРОВЩИНИ ВИКРИЛА ГРУПУ ЗЛОВМИСНИКІВ У ШАХРАЙСТВІ

Для реалізації злочинної схеми фігуранти створювали фейкові сторінки користувачів месенджеру та просили у їхніх друзів позичити гроші. У такий спосіб зловмисникам вдалося привласнили понад 300 тисяч гривень. Організаторам угруповання правоохоронці оголосили підозру.

Шестеро громадян, мешканці Кам'янського та Верхівцевого, у месенджері шукали відкриті групові чати та створювали фейкові сторінки учасників. Далі з акаунтів-клонів писали іншим учасникам чатів із проханням позичити гроші або долучитися нібито до благодійних зборів для військових. У такий спосіб зловмисники ошукали близько 70 осіб.

ЗАХИСТ ЕНЕРГЕТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРАТАК ВІДПРАЦЬОВУВАЛИ НА КОМАНДНО-ШТАБНИХ НАВЧАННЯХ ДЕРЖСПЕЦЗВ'ЯЗКУ

Держспецзв'язку за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України» провела перші командно-штабні навчання зі стійкості критичної інфраструктури Critical Infrastructure Resilience Exercises (далі — CIREX), розроблені на базі методичних рекомендацій Агентства США з питань кібербезпеки та захисту інфраструктури (CISA).

Головна ціль CIREX полягала в опрацюванні питань протистояння кіберзагрозам та координації зусиль у відбитті кібератак. Участь у навчанні взяли представники енергетичного сектору, які протягом дня відпрацьовували механізми реагування на кібератаки типу Ransomware (програм-здирників відповідно до чинної таксономії кіберінцидентів).

Заступник Міністра енергетики України з питань цифрового розвитку, цифрових трансформацій і цифровізації Фарід Сафаров підкреслив, що пишається командою, яка займається кіберзахистом в енергетичній галузі. Він додав, що у боротьбі з хакерами «один у полі — не воїн».

Участь у навчаннях взяли представники НЕК «Укренерго», Групи ДТЕК, КП «Київтеплоенерго», НАК «Нафтогаз України», ДП НАЕК «Енергоатом», а також Міністерства енергетики України та функціональних органів із захисту критичної інфраструктури, зокрема Служби безпеки України, Національної поліції України та Апарату РНБО України.

ДЕРЖСПЕЦЗВ'ЯЗКУ ПРОВЕЛА ДРУГІ ВСЕУКРАЇНСЬКІ ЗМАГАННЯ З КІБЕРБЕЗПЕКИ UA30CTF

Державна служба спеціального зв'язку та захисту інформації України провела всеукраїнські молодіжні онлайн-змагання із кібербезпеки у форматі Capture the Flag – UA30CTF. У них взяли участь понад 400 учасників, об'єднаних у 107 команд із різних куточків України.

Змагання проходили у форматі гри #Jeopardy CTF. Протягом 12 годин команди вирішували 25 завдань на пошук та експлуатацію вразливостей у поєднанні з вирішенням цікавих логічних завдань.

Перше місце здобула команда LunarLobsters, друге та третє – Knotty Kitten та Arctic Warriors. Із загальним рейтингом можна ознайомитись тут.

GOOGLE ЗАПУСТИВ В УКРАЇНІ ОНЛАЙН-ГРУ «INTERLAND: БЕЗПЕКА ДІТЕЙ В ІНТЕРНЕТІ»

Онлайн-гру створено для того, щоб допомогти дітям набути важливих цифрових навичок. Це гарантуватиме безпеку дітей в Інтернеті та допоможе їм стати відповідальними цифровими громадянами. Запуск гри відбувся за інформаційної підтримки Міністерства цифрової трансформації України і національного проєкту Дія.Цифрова освіта.

В Інтернеті можна зіткнутися з такими небезпеками, як онлайн хуліганство, кібербулінг, шахрайство та інші цифрові загрози. Тому вчити дітей навичок безпеки в Інтернеті важливо, щоб захистити їх та гарантувати їм відповідальне користування Інтернетом.

Онлайн-гра «Interland: Безпека дітей в Інтернеті» відсьогодні доступна українською мовою і є безкоштовною, тож доступна кожному, і, що найважливіше, її реалізовано у зрозумілому та цікавому для дітей форматі. В Interland в уявному світі діти зможуть навчитися, як обережно ділитися інформацією в мережі, розпізнавати фейки та боротися з хакерами, фішерами та кіберхуліганами. Отримати доступ до Interland можна за посиланням.

КИЇВСТАР НАДАВ 300 МЛН ГРИВЕНЬ НА РОЗВИТОК ЦИФРОВОЇ УКРАЇНИ

Національний телеком-оператор переказав на державний рахунок останню частину інвестицій із загальної суми 300 млн грн. Кошти виділили для реалізації державних проєктів із цифрового розвитку та кіберзахисту України.

«Під час повномасштабної війни цифрова інфраструктура стала основою ефективної роботи держави. Працює митниця, виплачуються пенсії, зарплати, повноцінно працює Уряд. Майже щотижня Мінцифра запускає нові послуги в Дії. І все це під час першої у світі кібервійни. Дякуємо компанії Київстар за внесок у розвиток цифрової України. Така підтримка дозволяє нам реалізовувати топпроєкти для посилення безпеки та надійності цифрової інфраструктури», – зазначив Віцепрем'єр-міністр з інновацій, розвитку освіти, науки та технологій – Міністр цифрової трансформації Михайло Федоров.

Як повідомляє Мінцифра, ці кошти спрямовуються на пріоритетні проєкти із цифрової трансформації нотаріату (е-нотаріат) та товарно-транспортних накладних (е-ТТН), на цифровізацію послуг ДРАЦСів тощо. А також на модернізацію та розвиток державних реєстрів, посилення інформаційної безпеки, зміцнення кіберзахисту країни.

8. ПЕРША СВІТОВА КІБЕРВІЙНА

КІБЕРВИМІРИ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Європейська ініціатива з дослідження кіберконфліктів (ECCRI) оприлюднила звіт (підготовлений на замовлення NCSC-UK) з семінару, присвяченому російським методам ведення кібервійни, що відбувся 28 лютого 2023 року. Дослідження зосереджено на досягнутому росією, зокрема на високому темпі кібероперацій, на відміну від багатьох і очевидних способів, якими російські кібероперації не виправдали довоєнних очікувань. У звіті містяться такі основні висновки:

- згідно зі своєю доктриною інформаційного протиборства, росія застосовувала різноманітні кібероперації під час війни в безпрецедентному масштабі.
- основні цілі воєнних операцій – диверсії, вплив, шпигунство – залишилися незмінними. Кібероперації надають нові можливості для досягнення давніх цілей.
- кібератівність в Україні відбувається паралельно зі сплесками та затишшями кібератівності.
- ГРУ застосовує гнучкий підхід з використанням «чистих вайперів», якими легко маніпулювати та запускати без виснаження значних ресурсів.
- західні спостерігачі вірогідно переоцінюють координацію між російськими злочинцями та урядом.
- відрізнити групи кіберзлочинців і політичних активістів стає все важче.
- такі ініціативи, як IT-армія, ризикують стерти важливі принципи розмежування між учасниками бойових дій і некомбатантами.
- відбувається зміна обов'язків, яку повинні визнати як державний, так і приватний сектори, при цьому галузь надає масштабні потужності.
- хоча Україна виграла від єдності цілей багатьох різних західних акторів, цей конфлікт може не дати хорошої дорожньої карти на майбутнє.

УКРАЇНСЬКІ ХАКТИВІСТИ ВИКОРИСТОВУЮТЬ НОВІ СПОСОБИ ОТРИМАТИ ДАНІ ПРО РОСІЙСЬКИХ ВІЙСЬКОВИХ ЗЛОЧИНЦІВ

Першого квітня видання The Hack Read розповіло про те, як українські хактивісти переконали дружину чинного полковника російської армії взяти участь у патріотичній фотосесії. Потім вона переконала ще 12 дружин військових приєднатися, що дозволило хактивістам отримати особисту та конфіденційну інформацію щодо їх чоловіків.

УКРАЇНСЬКІ ХАКТИВІСТИ ЗМОГЛИ СКЕРУВАТИ ЗІБРАНІ РОСІЯНИНОМ КОШТИ НА КУПІВЛЮ ДРОНІВ НА ІНШІ ЦІЛІ

Третього квітня видання Ліга повідомило, що українські хакери з групи «Кібер Спротив» не дозволили російському блогеру купити для армії РФ безпілотники – з його карткою «попрацювали» та замовили в інтернет-магазині замість дронів секс-іграшки на суму $25 000. Про це повідомляється в Telegram-каналі групи.

КІБЕРУМИРОТВОРЕННЯ ЗАХОДУ ДОПОМОГЛО ДАТИ ПУТІНУ ЗЕЛЕНЕ СВІТЛО

У колонці, опублікованій 3 квітня Washington Post колишній верховний головнокомандувач НАТО в Європі, адмірал США у відставці Джеймс Ставрідіс висловив думку, що відсутність адекватної відповіді заходу на агресивну поведінку рф як у кіберпросторі дало зелене світло агесії путіна. На його думку, стався провал стримування та дипломатії.
Адмірал Ставрідіс пропонує підвищити підготовку американських дипломатів у технічних питаннях, розробити чіткі критерії, після яких на кібератаку має бути дана чітка та жорстка відповідь. Усвідомити, що у кіберпросторі необхідна терпимість до конфлікту низької інтенсивності для того, щоб встановити довготривалі механізми стримування, хоча наявність такого конфлікту і становить ризик ескалації. «США необхідно розвинути почуття стримування в кіберпросторі, і для цього необхідно агресивніші відповіді, ніж вони були готові використовувати досі», – вважає Ставрідіс.

ВИТІК КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ПРО СИТУАЦІЮ В УКРАЇНІ СПОНУКАЄ ПЕНТАГОН ДО РОЗСЛІДУВАННЯ

7 квітня The New York Times повідомила, що влада США розслідує очевидний витік конфіденційної інформації, який стосується планів США щодо підтримки України. Файли поширили в Twitter і Telegram через російські акаунти. Значна частина інформації здається правдивою (хоча принаймні деяку частину можна отримати з загальновідомих відкритих джерел) і достатньо правдивою, щоб спонукати до розслідування. Інші дані, зокрема оцінки втрат, схоже, були сфальсифіковані в інтересах росії (з заниженими втратами росіян і перебільшеними втратами українців), і вони, здається, являють собою домішку дезінформації, що може бути головною причиною їх публікації.

УКРАЇНСЬКІ ХАКЕРИ ЗЛАМАЛИ ПОШТУ ШПИГУНА РФ, ЯКИЙ ВТРУЧАВСЯ У ВИБОРИ США

Як 11 квітня повідомила “Українська правда”, українські хакери зламали пошту російського шпигуна Серія Моргачева, якого розшукує американська ФБР за злам кампанії Гілларі Клінтон у 2016 році. За повідомленням Inform Napalm, поштова скринька Моргачева потенційно може містити інформацію про хакерські операції Росії, в тому числі про операцію проти Клінтон і демократів.

ПРОРОСІЙСЬКІ ХАКЕРИ ЗАЯВЛЯЮТЬ, ЩО СТОЯТЬ ЗА КІБЕРАТАКОЮ НА HYDRO-QUEBEC

Проросійська хакерська група NoName057 (16) взяла на себе відповідальність за DDoS атаку на сайт канадської компанії Hydro-Quebec вранці 13 квітня. Деякі частини сайту енергокомпанії Квебеку все ще були недоступні приблизно об 11:00 ранку. У Hydro-Quebec кажуть, що жодні особисті дані не були скомпрометовані. В онлайн-дописі група NoName057 (16) оголосила, що стоїть за зломом, але не уточнила, чому він був спрямований на Hydro-Quebec.

Раніше того тижня відбулися атаки на вебсайти прем’єр-міністра Джастіна Трюдо, Laurentian Bank of Canada та різних канадських портів, включаючи порт Монреаль і Порт де Квебек.

ПІДТРИМУВАНІ КРЕМЛЕМ ХАКЕРИ ВЕДУТЬ ШПИГУНСЬКУ КАМПАНІЮ ПРОТИ ДИПЛОМАТИЧНИХ СЛУЖБ КРАЇН ЄС І НАТО – CERT.PL

російські державні хакери запустили шпигунську кампанію проти міністерств закордонних справ і дипломатичних установ у країнах-членах НАТО, Європейському Союзі та, «меншою мірою», в Африці, повідомило 13 квітня головне агентство з кібербезпеки Польщі.

Кампанія пов'язана з підтримуваною кремлем хакерською групою Nobelium, також відомою як APT29 або [BlueBravo]. Nobelium відповідальний за кілька резонансних інцидентів, включаючи атаку на ланцюг постачання SolarWinds у 2020 році. Її пов'язують з російською Службою зовнішньої розвідки (СВР). І хоча угруповання знаходиться під пильним наглядом, цього разу вони використали раніше невідомий інструмент, повідомляє cert.pl.

РОСІЙСЬКІ ХАКЕРИ У 2022 РОЦІ ВДАЛО АТАКУВАЛИ НЕНАЗВАНУ КОМЕРЦІЙНУ СУПУТНИКОВУ КОМПАНІЮ – CSIS SPACE THREAT ASSESSMENT 2023

14 квітня аналітичний центр CSIS оприлюднив свій звіт «Оцінка космічних загроз 2023», у якому дає комплексний аналіз аерокосмічної складової російсько-української війни. Звіт розглядає і кіберскладову та її вплив на функціонування супутників та радіоелектронну боротьбу. Звіт вказує (з посиланням на виступ представника CISA на конференції), що у 2022 році російським хакерам вдалось проникнути у неназвану комерційну супутникову компанію і це виявили лише через місяці. Одним з висновків звіту є і те, що український приклад показує як країни, які менші за своїх супротивників, можуть ефективно протистояти останнім у випадку наявності переваги у космосі.

РОСІЙСЬКІ КІБЕРАТАКИ НЕ ЗАВДАЛИ КАНАДІ СУТТЄВОЇ ШКОДИ – РОЗВІДКА

Як 15 квітня повідомив речник канадського урядового Центру з безпеки комунікацій Робін Хавко, спецслужба розслідує низку кібератак, які трапилися під час візиту до Канади прем'єр-міністра України Дениса Шмигаля. Одночасно він наголосив, що кібератаки на сайти державної влади Канади не завдали системної шкоди. російським хакерам вдалося на кілька годин вивести з ладу офіційне інтернет-представництво голови уряду Канади. За день до того технічні проблеми були на сайті канадського сенату.

«Центр з безпеки комунікацій та його Канадський центр кібербезпеки зазначають, що розподілені атаки типу «відмова в обслуговуванні» (DDoS) не є рідкістю проти країн, куди приїжджають українські урядовці», – зазначив речник.

УКРАЇНСЬКІ ХАКЕРИ СФОРМУВАЛИ ВЛАСНИЙ ФРОНТ СПРОТИВУ РОСІЇ У КІБЕРВІЙНІ – BBC

У своєму матеріалі від 15 квітня Джо Тіді розповідає про результати власних дискусій з представниками українського хакерського ком'юніті, які ведуть власний фронт спротиву російській агресії. Він вказує на те, що значна кількість українських хакерів не просто здійснюють оборонні заходи, але вдаються до контратак проти російських інформаційних ресурсів. Водночас така діяльність здійснюється ними часто на свій розсуд. Хоча зв'язки між такими хактивістами та українською владою часто обговорюються, однак прямо вони не перетинаються або лише у тих випадках, коли мобілізуються на військову службу.

KILLNET ПРОВІВ DDOS-АТАКУ ПРОТИ ВЕБСАЙТУ ЄВРОПЕЙСЬКОГО УПРАВЛІННЯ ПОВІТРЯНИМ РУХОМ

19 квітня вебсайт Європейського управління повітряним рухом був атакований зловмисниками з угрупування KillNet. Атака спричинила перебої в роботі вебсайту та вебдоступності, однак жодного впливу на європейську авіацію не сталось. Атака частково вплинула на внутрішню та зовнішню комунікацію агентства, що змусило 2000 співробітників організації використовувати інші засоби комерційної комунікації.

РОСІЙСЬКІ ХАКЕРИ ПОСИЛЮЮТЬ АТАКИ НА ЕНЕРГЕТИЧНИЙ СЕКТОР СХІДНОЇ ЄВРОПИ – GOOGLE

Згідно з новим дослідженням Google Threat Analysis Group (TAG), російські хакери активізували атаки на енергетичний сектор Східної Європи протягом перших трьох місяців цього року. У дописі опублікованому 19 квітня, дослідники описують скоординовані кампанії, керовані декількома відомими державними хакерськими групами, серед яких:

- пов'язана з ГРУ РФ FROZENBARENTS (відома, як Sandworm), яка атакує енергетичний сектор, продовжує операції зламування та витоку інформації,
- пов'язана з ГРУ РФ FROZENLAKE, яка проводить фішингові кампанії проти українців,
- білоруська PUSHCA, яка продовжує таргетувати регіональних провайдерів вебпошти.

Україна залишається однією з основних мішеней фішингових атак. З січня по березень на фішингові кампанії, підтримувані російським урядом, припало 60% зафіксованих спроб, йдеться у звіті.

РОСІЙСЬКА GROUP-IB ЗАЯВИЛА ПРО ПОВНИЙ ВИХІД З РОСІЙСЬКОГО РИНКУ

20 квітня відома російська кібербезпекова компанія Group-IB заявила, що завершила свій вихід з російського ринку. За їх словами тепер основний офіс компанії знаходиться у Сінгапурі. Зараз основну діяльність компанії скеровує Дмитро Волков, в т.ч. як другий співзасновник Ілля Сачков – знаходиться під арештом за звинуваченням у державній зраді.

Group-IB була неодноразово помічена у тісній співпраці з російськими спеціальними органами (передусім ФСБ).

ПІСЛЯ НАБУТТЯ ЧЛЕНСТВА В НАТО ФІНЛЯНДІЯ ПІДДАЄТЬСЯ ЗРОСТАЮЧІЙ КІЛЬКОСТІ КІБЕРАТАК

21 квітня уряд Фінляндії заявив, що фінські організації все частіше зазнають кібератак. Оголошення прозвучало через два тижні після того, як країна офіційно приєдналася до НАТО.

Генеральна директорка Фінського агентства транспорту та зв'язку (Trafficom) Кірсі Карламаа повідомила журналістам, що Центр кібербезпеки «щороку отримує все більше сповіщень, і постійно зростає інтерес до фінських мереж і організацій». Вона наголосила, що зростання інтересу став постійною тенденцією.

У заяві агентства росію названо джерелом зростання кіберактивності, підкресливши перехід москви від збору розвідданих на місцях до цифрової сфери. «російські кібероперації проти Фінляндії також почастішали, оскільки росія була змушена звернутися до кіберсередовища, оскільки її розвідувальні операції стали складнішими», – повідомило агентство.

Карламаа додала, що атаки програм-вимагачів стали більш цілеспрямованими, зміни відбулися наприкінці минулого року. Предметом особливого інтересу стали державні органи та компанії критичної інфраструктури.

ANONYMOUS SUDAN ВЗЯЛИ НА СЕБЕ ВІДПОВІДАЛЬНІСТЬ ЗА ЗЛАМ САЙТУ ІЗРАЇЛЬСЬКОГО МОССАДУ – ЗМІ

25 квітня газета Times of Israel повідомила, що група Anonymous Sudan взяла на себе відповідальність за злом сайту ізраїльської розвідки Моссад. Угруповання заявило в дописі в Telegram, що «ця атака є лише підготовчою атакою... до великої атаки». Видання додає, що Anonymous Sudan також несе відповідальність за злом вебсайтів низки ізраїльських банків та установ протягом останнього місяця.

АНБ ПОПЕРЕДЖАЄ ПРО АТАКИ RANSOMWARE НА УКРАЇНУ ТА НА ЛОГІСТИЧНІ МЕРЕЖІ ПОСТАЧАННЯ ДОПОМОГИ

російські хакери намагаються впровадити програми-вимагачі в логістичну систему постачання України та західних країн, які підтримують Київ у його боротьбі з москвою, заявив 26 квітня кібердиректор Агентства національної безпеки Роб Джойс під час круглого столу на конференції RSA. Він підкреслив, що така тактика є новою в російському арсеналі та, швидше за все, продиктована розумінням важливості логістики, яке рф винесла з власних невдач у цій війні.

РОСІЙСЬКІ ХАКЕРИ АТАКУВАЛИ САЙТ НІМЕЦЬКОГО МІНІСТЕРСТВА

5 квітня ЗМІ повідомили, що російські хактивісти, що діють разом з угрупованням Killnet, намагалися відключити від мережі нещодавно створений вебсайт німецького уряду, присвячений економічній відбудові України, але їм це не вдалося.

РОСІЙСЬКА КІБЕРЗБРОЯ «МОЖЕ ЗАВДАТИ ВЕЛИКОЇ ШКОДИ» США – РІЧАРД А. КЛАРК

4 квітня в інтерв'ю France24 колишній уповноважений представник США з питань боротьби з тероризмом Річард Алан Кларк попередив, що російська кіберзброя потенційно може «завдати великої шкоди» США. Щоб пояснити, чому цього досі не сталося, він процитував «неписане правило», якого, на його думку, дотримуються як США, так і Росія: «[якщо] ви не нападаєте на мене, я не нападатиму на вас». Разом з тим, Кларк наголосив, що така ситуація може змінитися будь-якого дня.

АТАКИ ПРОРОСІЙСЬКИХ ГРУП НА ФІНЛЯНДІЮ ТА ІЗРАЇЛЬ ДЕМОНСТРУЮТЬ ЗРОСТАННЯ КІЛЬКІСТЬ DDOS-АТАК

6 квітня видання TheTechRepublic повідомило, що проросійська хакерська група NoName057(16) заявила, що вона стоїть за DoS атаками на вебсайт парламенту Фінляндії 4 квітня, у день вступу країни до НАТО. За даними фінського новинного сайту YLE, також був зламаний Фінський центр технічних досліджень. NoName057(16) – це та сама група, яка взяла на себе відповідальність за DDoS атаку, знищивши вебсайт парламенту країни в серпні минулого року, а також атакувала Україну, США, Польщу та інші європейські країни.

Прихильні до росії хактивісти з угруповання Killnet також атакували одну з найбільш відомих фірм у сфері безпеки, Check Point, а також університети та медичні центри в Ізраїлі. Група назвала себе «Анонімний Судан», але Надір Ізраель, технічний директор і співзасновник компанії Armis, сказав, що зловмисники, ймовірно, пов'язані з проросійською хактивістською групою Killnet.

Згідно з даними фірми NetScout, що займається керуванням продуктивністю застосунків, Killnet посилив атаки на американські установи цього та минулого року. У новому дослідженні «Відкриття нового ландшафту загроз» NetScout стверджує, що в секторі національної безпеки США кількість DDoS-атак у другій половині 2022 року зросла на 16 815%, багато з яких пов'язані з Killnet.

РОСІЙСЬКІ ХАКЕРИ НАМАГАЮТЬСЯ ЗНИЩИТИ КРИТИЧНУ ІНФРАСТРУКТУРУ ВЕЛИКОЇ БРИТАНІЇ – BLOOMBERG

19 квітня видання Ліга повідомило з посиланням на Bloomberg, що пов'язані з росією хакери намагаються пошкодити або знищити критично важливу національну інфраструктуру Великої Британії. За словами одного з найвищих міністрів в уряді канцлера герцогства Ланкастерського Олівера Довдена, хакери, які працюють на організації, за структурою схожі на групу Вагнера, в останні місяці звернули свою увагу на Велику Британію і становлять загрозу для бізнесу.

РОСІЙСЬКІ СТРАХОВІ КОМПАНІЇ ВТРАТИЛИ ГРОШІ ЧЕРЕЗ АТАКИ УКРАЇНСЬКИХ ХАКЕРІВ – РОСЗМІ

Українська IT-армія у квітні 2023 року організувала низку комплексних DDoS-атак на вебресурси та інфраструктуру страхових організацій у Росії, що призвело до серйозних порушень у їх роботі, 25 квітня повідомило українське видання Ліга з посиланням на Газета.ru.

9. РІЗНЕ

ГОЛОВА КАНАДСЬКОЇ КОМІСІЇ З КОНФІДЕНЦІЙНОСТІ РОЗПОЧАВ РОЗСЛІДУВАННЯ ЩОДО CHATGPT

Офіс уповноваженого з питань конфіденційності Канади (OPC) заявив 4 квітня, що розслідування щодо компанії OpenAI, яка створила ChatGPT, було розпочато у відповідь на «скаргу про збір, використання та розкриття особистої інформації без згоди». Канада – не єдина країна, яка намагається впливати на надшвидке розповсюдження цієї технології.

MICROSOFT ТА FORTRA РОЗПОЧАЛИ СПІЛЬНУ КОМПАНІЮ З ПОШУКУ ТА ВИДАЛЕННЯ СТАРИХ ВЕРСІЙ COBALT STRIKE

6 квітня компанія Microsoft повідомила, що її підрозділ Цифрових злочинів (DCU) спільно з компанією Fortra розпочали спільну компанію з пошуку та видалення старих версій кібербезпекового програмного продукту Cobalt Strike – розробки компанії Fortra, яка використовується злочинцями у протиправних цілях. 31 березня 2023 року Окружний суд США Східного округу Нью-Йорка видав ухвалу суду, яка дозволила Microsoft, Fortra та Health-ISAC здійснювати заходи з руйнування шкідливої інфраструктури, яку використовують злочинці для полегшення своїх атак. Це дасть змогу компаніям зосередитись на пошуку та знищенні зламаних, застарілих копій Cobalt Strike і скомпрометованого програмного забезпечення Microsoft.

ІТАЛІЯ СТАЛА ПЕРШОЮ ЗАХІДНОЮ КРАЇНОЮ, ЯКА ЗАБОРОНИЛА CHATGPT

4 квітня CNBC повідомила, що італійська служба захисту даних наказала OpenAI тимчасово припинити обробку даних італійських користувачів на тлі розслідування ймовірного порушення суворих європейських правил конфіденційності.

Стаття також містить опис підходів до регулювання ШІ у Великій Британії, ЄС, США та Китаї, наголошуючи, що багато країн стурбовані можливими негативними наслідками безконтрольного поширення цієї технології.

ІЗРАЇЛЬСЬКЕ ШПИГУНСЬКЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ВИКОРИСТОВУЄТЬСЯ ДЛЯ СТЕЖЕННЯ ЗА ЖУРНАЛІСТАМИ ТА ПОЛІТИКАМИ

11 квітня дослідницький центр, що займається цифровою криміналістикою, Citizen Lab і Microsoft Threat Intelligence опублікували детальні звіти про ізраїльську компанію QuaDream. Вона розробляє шпигунське програмне забезпечення і з моменту свого заснування у 2016 році залишалася маловідомою. Повідомляється, що компанія продає урядам платформу спостереження під назвою Reign. Дослідники виявили, що програмне забезпечення компанії використовувалося проти журналістів, політичних діячів і громадського діяча на трьох континентах.