НКЦК

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

CYBER DIGEST

Огляд подій в сфері кібербезпеки,
травень 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

За ініціативи Національного координаційного центру кібербезпеки при РНБОУ Україна стала повноцінним членом Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE) як країна-контрибутор. Зроблено ще один крок на шляху України до НАТО. Як повноправний член CCDCOE, Україна взяла участь у засіданні Керівного комітету центру. Також відбулась робоча зустріч для обговорення практичної співпраці, під час якої особливу увагу було приділено залученню України до щорічних кібернавчань Центру – Locked Shields. Наступного року для розробки сценарію для Locked Shields-2024 планується використати досвід України у кібервійні. CCDCOE також провів тренінг для українських фахівців у сфері кібербезпеки на тему: «Критична інформаційна інфраструктура».

ЄС продовжує посилювати політику обмеження іноземної (не європейської) присутності на своєму ринку. ЄС також висуває все більш жорсткі вимоги до інших гравців ринку, оскільки прагне обмежити вплив китайських компаній на розгортання мережі 5G (наприклад, Португалія прийняла нове рішення щодо цього) і розширити міжнародні зв'язки (наприклад, з Південною Кореєю). Формуються нові вимоги до іноземних операторів хмарних сервісів, збільшуються видатки на дослідження у сфері кібербезпеки, Євросоюз активно готується до запуску програми Європейський кіберщит.

Цього місяця багато уваги приділялося питанням кібербезпеки фінансового сектору. НКЦК розпочав навчання «Управління вразливостями» для фахівців банківського сектору України. З метою гармонізації законодавства України у сфері платіжних послуг із законодавством ЄС та посилення його імплементації Нацбанк встановив до надавачів платіжних послуг вимогу застосувати посилену автентифікацію користувачів з метою зниження ризиків шахрайства. Національна поліція припинила діяльність розгалуженої злочинної мережі, провівши слідчі дії у 20 регіонах держави, у якій брали участь понад 500 співробітників. У результаті викрили 56 зловмисників, які розсилали фішингові посилання для отримання даних банківських карток громадян. Нацполіція спільно з ФБР ліквідувала мережу сервісів для обміну криптовалюти, здобутої злочинним шляхом.

США також активно зосереджуються на безпеці критичної інфраструктури, формуючі нові пріоритети безпеки в цій сфері та впроваджуючи політику нульової довіри для федеральних агенцій. До останніх відноситься і Пентагон, який поряд з пошуком нових кібербезпекових рішень (наприклад в проведенні спільних операцій космічних та кібербезпекових сил) займається питанням реформи безпеки внутрішніх мереж. Поряд із запровадженням нульової довіри Пентагон переглядає власну стратегію IT розвитку та можливої залежності від невеликого кола постачальників.

Кібербезпекові органи альянсу Five Eyes продовжують демонструвати високий рівень спільної роботи та скоординованих зусиль. У травні вони опублікували кілька спільних матеріалів про ворожу кіберактивність, направили спільні кібербезпекові групи до європейських країн (зокрема, до Латвії) та підвищили ефективність спільних дій.

Хакерські групи продовжують перегруповуватись та знаходити нові інструменти та тактики. Хоча кількість ransomware інцидентів зменшилась у 2022 році, а ransomware угрупування зазнали збитків минулого року, їхня діяльність все ще є небезпечною. Постійно з'являються нові групи, а RaaS стає все популярнішим. Спонсоровані державою хакери все частіше націлюються на малі та середні підприємства, щоб використовувати їх для більш масштабних атак. Тим часом спроби страхових компаній не виплачувати страхові суми жертвам кібератак з посиланням на «стан кібервійни» (як це сталось в кейсі Merck) виявились невдалими.

Дедалі більша увага хакерів до систем ICS/OT також становить небезпеку – постійно з'являються нові вразливості, і такі цілі привертають все більше уваги на хакерських форумах. У продуктах відомих виробників промислового обладнання (Rockwell Automation, Siemens, Teltonika, Lacroix) все частіше знаходять небезпечні для підприємств вразливості, щомісяця з'являються нові віруси, націлені на ICS (May's Cosmic Energy).

Пропри те, що загрози від ransomware залишаються найбільш медійними, реальні фінансові загрози від кібератак здебільшого припадають на компрометацію бізнес електронної пошти – на них припадає понад 50% усієї шкідливої діяльності. Аналітичні та урядові служби США продовжують аналізувати резонансні випадки руйнівних атак, таких як Colonial Pipeline та Solar Winds, та пропонують шляхи зміцнення кібербезпеки, особливо у світлі потенційної ескалації протистояння між США та Китаєм, яке, за оцінками американської розвідувальної спільноти, майже однозначно призведе до атак на ОКІ США з боку Пекіну.

Перша світова кібервійна триває і росія не зменшує свою активність. Російські злочинні синдикати переформовуються, щоб забезпечити більшу ефективність. Українські кібербезпекові структури постійно попереджають про нові кіберзагрози з боку росії, продовжуються вдалі операції російських хакерів за кордоном (наприклад, кібератаки на сайти деяких урядових установ Франції). Тим часом стає дедалі ефективнішим виявлення російського кібершпигунства– у травні було встановлено, що давня шпигунська компанія протягом багатьох років використовувала ШПЗ «Sanke» для збору розвідувальної інформації з державних органів багатьох країн.

Аналітики продовжують робити висновки з кіберскладової російсько-української війни. Серед основних оцінок: багато хто недооцінює кібероборону – ефективно побудований захист справді здатний зупинити або стримувати ворожу кіберактивність; кіберскладові конфліктів не будуть швидкоплинними – це буде довгі позиційні бої між учасниками протистояння; цілі та завдання Трансатлантичного партнерства включають стримування можливостей росії досягти своїх цілей в Україні.

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

ЄВРОПЕЙСЬКИЙ ЦЕНТР КОМПЕТЕНЦІЇ З КІБЕРБЕЗПЕКИ ВІДКРИВ НОВУ ШТАБ-КВАРТИРУ В БУХАРЕСТІ

9 травня Європейський центр компетенції з кібербезпеки (ECCC), заснований для підтримки інновацій та промислової політики у сфері кібербезпеки, відкрив нову штаб-квартиру кампусі Бухарестського технологічного університету в Румунії. Центр відповідає за управління фінансуванням ЄС, виділеним на кібербезпеку, через прийняття робочих програм з кібербезпеки, а також керує кіберпроєктами в рамках Програми цифрової Європи та Horizon Europe. Очікується, що він також керуватиме проєктами щодо розбудови центрів безпеки в рамках пропозиції Комісії щодо створення Європейського кіберщита.

СІНГАПУР РОЗРОБЛЯЄ НОВИЙ ЗАКОН ДЛЯ ШВИДШОЇ БОРОТЬБИ ІЗ КІБЕРЗЛОЧИНАМИ

9 травня повідомлялося, що Сінгапур розробляє новий закон, який дозволить уряду видавати директиви для боротьби з «масштабною та швидкою» кіберзлочинністю. Закон передбачатиме блокування доступу до ймовірних шахрайських сайтів. Наприклад, постачальники онлайн-послуг можуть отримати вказівки вимкнути певний вміст, як-от вебсторінки чи публікації, включно з копіями вмісту, щоб їх не можна було переглядати у Сінгапурі. Вони також можуть отримати вказівку заблокувати доступ до URL-адреси. Магазини програм також можуть отримати вказівки видалити програму зі свого магазину в Сінгапурі, щоб запобігти подальшому завантаженню користувачами в країні. За даними Міністерства внутрішніх справ, запропоноване законодавство може бути застосоване до дев'яти категорій кримінальних злочинів, включаючи діяльність, що зачіпає національну безпеку, незаконні азартні ігри та підбурювання до насильства.

ЄС ПЛАНУЄ ПОСИЛИТИ ВИМОГИ КІБЕРБЕЗПЕКИ ДЛЯ AMAZON, GOOGLE, MICROSOFT

Як стало відомо 9 травня, Європейський Союз працює над новим документом, який має посилити вимоги до кібербезпеки для таких компаній як Amazon, Alphabet, Google, Microsoft або інших постачальників хмарних послуг за межами ЄС. Ці вимоги включатимуть необхідність створити спільне підприємство з компанією, що базується в ЄС, і мати в ній лише міноритарну частку. Співробітники цих компаній, які мають доступ до даних ЄС, повинні будуть пройти спеціальні перевірки та бути громадянами однієї з країн ЄС. Раніше Торгова палата США заявила, що такі плани ставить американські компанії в нерівне становище. ЄС заявив, що ці кроки необхідні для захисту даних і прав на конфіденційність громадян Союзу.

CISA ОПРИЛЮДНИЛА БІЛУ КНИГУ ПРІОРИТЕТІВ ДЛЯ ДОСЛІДЖЕНЬ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

10 травня CISA опублікувала Білу книгу для систематизації потреб держави в наукових дослідженнях у сфері захисту критичної інфраструктури. Цей документ має стати своєрідною настановою для наукових досліджень, що здійснюються державним коштом, аби зробити їх кориснішими для державного сектору як на національному, так і місцевому рівні. Документ визначає низку проблемних напрямків, які потребуватимуть додаткової уваги з боку науковців, а також окремі настанови щодо того, як зробити дослідження більш релевантним очікуванням споживачів.

В США ЗАВЕРШИЛИСЬ ЧЕТВЕРТІ ЩОРІЧНІ КІБЕРЗМАГАННЯ ЗА КУБОК ПРЕЗИДЕНТА

15 травня було оголошено переможців четвертих щорічних кіберзмагань на Кубок президента, які проводяться CISA. Представники CISA та Офісу Національного кібердиректора (ONCD) привітали переможців, серед яких є співробітники Агентства національної безпеки та військової розвідки. У конкурсі 2022 року взяли участь майже 240 команд і понад 1100 осіб, які змагалися за найвищі нагороди. Десять відомств і установ вперше відправили конкурсантів. ONCD розглядає ці змагання як частину заходів з реалізації загальної Національної стратегії кадрів і освіти у кіберпросторі.

ПЕНТАГОН ПЛАНУЄ ЗМЕНШИТИ СВОЮ ЗАЛЕЖНІСТЬ ВІД ПРОДУКТІВ MICROSOFT РОЗШИРИВШИ КОЛО ПОСТАЧАЛЬНИКІВ

Стаття Newsweek від 16 травня підкреслює стурбованість Пентагону щодо залежності відомства від продуктів Microsoft. Історії про вразливості Outlook, якими активно користувались ворожі хакери, лише підсилила ці процеси, змушуючи Пентагон збільшити кількість постачальників засобів безпеки. Ця залежність може створити «єдину точку відмови» – ситуацію, коли використання однієї вразливості продукту дозволить атакувати всю мережу одночасно. Аби цього уникнути Пентагон активніше планує залучати додаткові рішення безпеки, навіть якщо вони будуть дублювати рішення Microsoft.

ПЕНТАГОН ПРОДОВЖУЄ ЗАХОДИ ІЗ ВПРОВАДЖЕННЯ ПОЛІТИКИ НУЛЬОВОЇ ДОВІРИ В МЕРЕЖАХ ВІДОМСТВА

18 травня Девід Маккеоун, заступник головного інформаційного директора Міністерства оборони, а також старший офіцер з інформаційної безпеки відомства, заявив, що вони наполегливо працюють, щоб повною мірою реалізувати Дорожню карту переходу Пентагону до політики нульової довіри у 2027 році. За його словами, наразі ключова робота зосереджена на консультаціях з приватним сектором – передусім хмарними провайдерами. Макеоун підкреслив, що хоча кінцевий результат безумовно важливий, але вже зараз, з кожним кроком на шляху до нової політики безпеки, мережі відомства стають все безпечнішими.

КІБЕРКОМАНДУВАННЯ США ОПРИЛЮДНИЛО СВОЇ СТРАТЕГІЧНІ ПРІОРИТЕТИ

18 травня командувач Кіберкомандування США генерал Пол Накасоне оприлюднив стратегічні пріоритети командування. Було визначено три основні пріоритети: відточування (створення сил світового класу через готовність, стійкість та вдосконалення місії); посилення військової переваги в умовах криз і конфліктів (через згуртованість і співпрацю); і ефективне виконання повноважень (створення та підтримка вирішальної переваги для національної безпеки).

ПОРТУГАЛІЯ ЗРОБИЛА ЩЕ ОДИН КРОК ДО ЗАБОРОНИ КИТАЙСЬКОГО ОБЛАДНАННЯ ДЛЯ 5G

23 травня Рада з кібербезпеки Португалії (CSSC) випустила резолюцію, яка може змусити операторів зв'язку не використовувати китайське обладнання у своїх високошвидкісних мобільних мережах 5G. CSSC не назвав Китай або будь-яких китайських постачальників поіменно, але попередив про «високий ризик для безпеки з боку постачальників або провайдерів, розташованих у країнах, де уряди здійснюють контроль, втручання або тиск на їх діяльність у третіх країнах». CSSC є дорадчим органом прем'єр-міністра.

ГЕНЕРАЛ-ЛЕЙТЕНАНТ ТІМОТІ ХО МОЖЕ СТАТИ НАСТУПНИМ КЕРІВНИКОМ АГЕНТСТВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА КІБЕРКОМАНДУВАННЯ США

24 травня з'явилася новина про можливість призначення наступного керівника Агентства національної безпеки та Кіберкомандування США. Ним стане генерал-лейтенант Тімоті Хо, нинішній заступник командувача Кіберкомандування США. Він змінить генерала армії Пола Накасоне, який очолював обидві організації з травня 2018 року та, як очікується, піде у відставку цього року. Поточна модель «один голова — два міністерства» буде збережена, хоча дискусії про те, чи потрібно буде призначати окремих голів двох важливих міністерств, тривають.

КОСМІЧНІ СИЛИ США РАЗОМ З КІБЕРКОМАНДУВАННЯМ ДОСЛІДЖУЮТЬ МОЖЛИВОСТІ НАСТУПАЛЬНИХ КІБЕРОПЕРАЦІЙ З КОСМОСУ

На заході Інституту Мітчелла 24 травня генерал-лейтенант Стівен Уайтінг сказав, що експерти з двох напрямків — космічних сил та кіберспеціалісти — працюють разом, щоб визначити можливості для використання наступального кіберпотенціалу в контексті космічних цілей – злам супутників та захист своїх.

ЄВРОКОМІСІЯ ВИДІЛЯЄ 107 МІЛЬЙОНІВ ЄВРО ДЛЯ ПОСИЛЕННЯ КІБЕРБЕЗПЕКИ В ЄВРОПІ

25 травня Єврокомісія та Європейський центр компетенції з кібербезпеки (ECCC) оголосили новий конкурс на загальну суму 71 млн євро в рамках програми «Цифрова Європа» на 2023-2024 рр. Мета конкурсу – реалізація заходів у сфері кібербезпеки, спрямованих на посилення оперативної співпраці та спільного потенціалу з державами-членами на рівні ЄС. З 71 мільйона євро 35 буде спрямовано на створення механізмів реагування на надзвичайні ситуації у сфері кібербезпеки. Ще на 36,5 мільйонів було продовжено попередній конкурс, який стимулюватиме розвиток «кібертренувальних майданчиків» (3,4 млн євро), посилить можливості SOC (26,3 млн євро) і стимулюватиме інноваційні рішення в кібербезпеці (6,8 млн євро).

ЗС СІНГАПУРУ ПЛАНУЮТЬ ЗАЛУЧИТИ МОЖЛИВОСТІ ШІ ДО СФЕРИ КІБЕРЗАХИСТУ

Підрозділ кіберзахисту Збройних сил Сінгапуру, відомий як Служба цифрової та розвідувальної інформації (DIS), у травні уклав угоду з AI Singapore про «посилення національної експертизи в галузі ШІ» для цифрового захисту. Запущений Національним дослідницьким фондом у травні 2017 року AI Singapore спрямований на створення можливостей ШІ країни та відповідної екосистеми, яка включатиме місцеві стартапи та компанії, які розробляють продукти ШІ. Міністерство оборони Сінгапуру заявило, що DIS може використовувати індустрію AI Singapore для розвитку талантів для потреб оборони.

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

СІНГАПУР І США ПРОВОДЯТЬ ТРАНСКОРДОННІ НАВЧАННЯ ДЛЯ ПЕРЕВІРКИ СТІЙКІСТЬ БАНКІВ

На початку травня відбулись триденні навчання для перевірки здатності банків, що працюють на ринках США та Сінгапуру, реагувати на транскордонні кіберінциденти. Навчання організовано Валютно-фінансовим управлінням Сінгапуру (MAS) і Міністерством фінансів США. Мета полягала у перевірці протоколів обміну даними та координації реагування на інциденти за участю банків в обох юрисдикціях. У спільній заяві урядових установ зазначено, що транскордонні навчання є критично важливими на тлі зростаючих онлайн-загроз для фінансових послуг і зв'язків між фінансовими екосистемами двох країн.

ЄС ТА ПІВДЕННА КОРЕЯ ГОТУЮТЬСЯ ДО ПОГЛИБЛЕННЯ СПІВПРАЦІ У СФЕРІ КІБЕРБЕЗПЕКИ

22 травня Європейський Союз та Республіка Корея виступили зі спільною заявою за підсумками десятого саміту ЄС – Республіка Корея. У пункті 21 заяви зазначено, що сторони посилюватимуть співпрацю проти кіберзагроз, включаючи кіберзлочинність і програми-вимагачі, а також кібератаки державних і недержавних суб'єктів. ЄС і Південна Корея також планують найближчим часом провести консультації щодо кіберполітики.

CISA, FBI, NSA, MS-ISAC ОПУБЛІКУВАЛИ ОНОВЛЕНИЙ ПОСІБНИК #STOPRANSOMWARE

23 травня Об'єднана цільова група з програм-вимагачів (JRTF) опублікувала оновлений посібник #StopRansomware, щоб допомогти організаціям зменшити ризик інцидентів з програмами-вимагачами, надавши найкращі методи виявлення, запобігання, реагування та відновлення, включаючи покрокові підходи до зменшення вірогідності потенційних атак. Оновлення додає додаткові уроки з інцидентів за останні два роки, рекомендації щодо резервного копіювання безпеки в хмарі та поради щодо виявлення та аналізу загроз.

NSA СПІЛЬНО З СОЮЗНИКАМИ ВИЯВЛЯЮТЬ ІНФРАСТРУКТУРУ ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ RUSSIAN SNAKE ПО ВСЬОМУ СВІТУ

9 травня NSA заявило, що спільно з партнерами по всьому світу займаються виявленням та знищенням інфраструктури ШПЗ Snake. Його виявлено у понад 50 країнах. За даними американських експертів, російські спецслужби роками використовували цей інструмент для збору розвідданих, зокрема для отримання доступу та викрадення конфіденційних документів на теми міжнародних відносин та іншої дипломатичної інформації. Вірус атрибутовано як такий, що належить одному з підрозділів 16-го центру федеральної служби безпеки росії (ФСБ).

США СПІЛЬНО З АВСТРАЛІЄЮ, КАНАДОЮ, НОВОЮ ЗЕЛАНДІЄЮ ТА БРИТАНІЄЮ ВИПУСТИЛИ ПОПЕРЕДЖЕННЯ ПРО ФІНАНСОВАНУ ДЕРЖАВОЮ КІБЕРАКТИВНІСТЬ КНР

24 травня CISA, NSA і FBI разом з Австралійським центром кібербезпеки (ACSC), Канадським центром кібербезпеки (CCCS), Національним центром кібербезпеки Нової Зеландії (NCSC-NZ) і Національним центром кібербезпеки Сполученого Королівства (NCSC-UK) опублікували спільну консультацію з кібербезпеки, яка містить технічні відомості про зловмисні кампанії кібератора, спонсорованого Китайською Народною Республікою (КНР). У публікації описано, як кібератори КНР використовують законні інструменти керування мережею, щоб інтегруватися у звичайну системну та мережеву діяльність і уникнути ідентифікації багатьма продуктами для виявлення та реагування на кінцеві точки (EDR).

США ТА КАНАДА НАПРАВИЛИ КІБЕРЕКСПЕРТІВ ДО ЛАТВІЇ ДЛЯ ПОСИЛЕННЯ ЦИФРОВОГО ЗАХИСТУ

10 травня Recorded Future повідомило, що Кіберкомандування США нещодавно завершило другу місію в Латвії, спрямовану на захист мережі балтійської країни від цифрових атак і виявлення зловмисної діяльності, яка може бути використана проти США та їхніх союзників.
Сили кібернаціональної місії співпрацювали з CERT.LV для посилення захисту ОКІ країни. Вперше експерти зі США та Канади співпрацювали, щоб одночасно досліджувати мережі іншої країни на наявність зразків зловмисного програмного забезпечення та визначати інструменти та методи протидії.
Очікується, що попит на цифрову експертизу США зросте через триваючий напад росії на Україну. Команди США та Канади працювали в окремих мережах, але обмінювались інформацією одна з одною та з латвійськими офіційними особами. Виконувані Кіберкомандуванням hunt forward missions дозволяють США виявляти зловмисну активність до того, як вона загрожуватиме США, і допомагати зміцнювати критично важливі системи проти кіберзагроз, які впливають на всі країни.

ЗАЯВА ЄС – ЗАСІДАННЯ РАДИ БЕЗПЕКИ ООН ЗА ФОРМУЛОЮ АРРІА: ВІДПОВІДАЛЬНІСТЬ ДЕРЖАВ ЗА КІБЕРАТАКИ НА КРИТИЧНУ ІНФРАСТРУКТУРУ

Виступаючи від імені ЄС 26 травня Посол Олоф Скоог підкреслив нещодавнє помітне зростання зловмисної поведінки в кіберпросторі. Цілеспрямовані кібератаки на критичну інфраструктуру мали руйнівний вплив на економіку ЄС та його партнерів, а також на повсякденне життя громадян. Пан Скоог згадав заходи, вжиті ЄС для покращення безпеки кіберпростору. Він також наголосив на важливій ролі приватного сектору в захисті ОКІ. Водночас він підкреслив, що кіберпростір не є місцем беззаконня, і всі країни-члени ООН погодилися дотримуватися норм міжнародного права. Він закликав до напрацювання спільного розуміння того, як норми міжнародного права застосовуються до кіберпростору, наголосивши, що те, що є незаконним у кінетичному світі, також є незаконним у кіберпросторі. Він закликав створити постійну платформу для діалогу в рамках Першого комітету через Програму кібердій (Cyber Programme of Action).

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

ІРАНСЬКА APT ВИКОРИСТОВУЄ ЗЛОВМИСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ BELLACIAO ПРОТИ ЦІЛЕЙ У США, ЄВРОПІ ТА АЗІЇ

30 квітня The Record повідомило, що спонсоровану державою іранську хакерську групу звинувачують у розгортанні нового типу шкідливого програмного забезпечення під назвою BellaCiao проти кількох жертв у США, Європі, Індії, Туреччині та інших країнах.
Дослідники фірми з кібербезпеки Bitdefender приписали зловмисне програмне забезпечення угрупованню APT35/APT42, також відомій як Mint Sandstorm або Charming Kitten, що є APT, якою нібито керує Корпус вартових ісламської революції.
BellaCiao – це тип зловмисного програмного забезпечення, призначеного для доставлення інших шкідливих програм на пристрої жертв за командою зловмисника.
«Воно розроблене для того, щоб бути повністю прихованим і насправді не спілкується з джерелами загроз. Це ПЗ абсолютно пасивне в отриманні інструкцій, поки воно працює. Я ніколи раніше не бачив техніки, яку вони використовують», — сказав Мартін Зугек, директор із технічних рішень у Bitdefender.

ІРАН ПРИСКОРЮЄ СВОЇ ОПЕРАЦІЇ КІБЕРВПЛИВУ ПО ВСЬОМУ СВІТУ – MICTOSOFT

У своїх висновках, оприлюднених 2 травня, Microsoft заявила, що Іран поєднує кібероперації та операції впливу, щоб «сприяти геополітичним змінам, які відповідають цілям режиму».
У 2022 році компанія зафіксувала 24 унікальні кібероперації впливу, що становить значне зростання у порівнянні з сімома у 2021 році. 17 з них відбулись у період з червня по грудень.
За словами Microsoft, ці атаки відбуваються за передбачуваною схемою.
Один з прикладів описує, як у листопаді минулого року кіберперсона під назвою BlackMagic зламала десятки ізраїльських вебсайтів, злила дані про доставлення та особисті дані з логістичних компаній, а також опублікувала відео, на якому нібито оператор змінює пункти призначення в журналах розподілу продукції ізраїльської транспортної компанії.

КИТАЙСЬКА ХАКЕРСЬКА ГРУПА EARTH LONGZHI ВІДРОДЖУЄТЬСЯ, ВИКОРИСТОВУЮЧИ ВДОСКОНАЛЕНЕ ЗЛОВМИСНЕ ПЗ – TREND MICRO

2 травня Trend Micro повідомила, що спонсорована державою китайська хакерська організація відновилась після понад шести місяців бездіяльності, започаткувавши нову кампанію проти урядових, медичних, технологічних та виробничих установ, розташованих на Тайвані, Таїланді, Філіппінах і Фіджі.
Trend Micro приписує низку нещодавніх вторгнень кібершпигунській групі, яку компанія відстежує під назвою Earth Longzhi, яка є підгрупою в APT41 (така ж HOODOO або Winnti) і перетинається з різними іншими кластерами, такими як Earth Baku, SparklingGoblin і GroupCC.

НОВА RANSOMWARE CACTUS ШИФРУЄ СЕБЕ ДЛЯ УНИКНЕННЯ ВИЯВЛЕННЯ АНТИВІРУСНИМ ПЗ

Новий оператор програм-вимагачів під назвою Cactus використовує вразливості в пристроях VPN, щоб отримати первинний доступ до мереж «великих комерційних організацій», сказав Koll у звіті від 7 травня. Програма-вимагач активна принаймні з березня та вимагає від жертв значні суми грошей. І хоча Cactus використовує звичайні для ransomware методи – шифрування файлів і крадіжки даних – його операції супроводжуються шифруванням для захисту двійкових файлів програм-вимагачів. CACTUS – це нова програма-вимагач, яка недостатньо використовувалась для збору показників щодо ціни викупу або наслідків несплати викупу. Дослідники рекомендують усі служби VPN оновити та запровадити менеджери паролів, щоб мінімізувати загрози. Kroll також рекомендує використовувати багатофакторну автентифікацію, щоб запобігти бічному переміщенню в скомпроментованих мережах.

ПІВНІЧНОКОРЕЙСЬКІ ХАКЕРИ KIMSUKY ВИКОРИСТОВУЮТЬ НОВИЙ ІНСТРУМЕНТ РОЗВІДКИ RECONSHARK В ОСТАННІХ КІБЕРАТАКАХ

4 травня SentinelLabs опублікувала звіт, в якому говориться, що спостерігала за постійними атаками з боку спонсорованої державою Північної Кореї APT Kimsuky, яка має довгу історію нападів на організації в Азії, Північній Америці та Європі.
Поточна кампанія використовує новий компонент зловмисного програмного забезпечення, який SentinelLabs називає ReconShark, який активно доставляється конкретним особам через фішингові електронні листи, посилання OneDrive, які ведуть до завантаження документів і виконання шкідливих макросів.
ReconShark – це інструмент розвідки з унікальним способом виконання команд і зв'язку з серверами. Нещодавню діяльність пов'язують із ширшою діяльністю, яку SentinelLabs впевнено приписує Північній Кореї.

CISCO ПОПЕРЕДЖАЄ ПРО НОВИЙ ІНСТРУМЕНТ GREATNESS ДЛЯ ФІШИНГУ ЯК ПОСЛУГИ

10 травня Cisco попередила, що новий інструмент «фішинг як послуга» (PaaS) під назвою Greatness дозволяє хакерам-початківцям використовувати «деякі з найдосконаліших» функцій для здійснення кібератак. Хакери імітують сторінки входу Microsoft 365, щоб отримати доступ до корпоративних мереж заради отримання фінансової вигоди. Платформа PaaS пропонує багато функцій, включаючи конструктор вкладень і посилань, дуже переконливі приманки та сторінки входу, обхід MFA, фільтрацію IP та інтеграцію з ботами Telegram, тож навіть новачок може успішно здійснити фішингову атаку. Підприємства у сферах охорони здоров'я, виробництва та технологій найчастіше стають мішенями, причому США є країною з найбільшою кількістю жертв. За нею йде Велика Британія, Австралія, Південна Африка та Канада. Ці тенденції демонструють необхідність для організацій залишатись пильними під час виявлення та пом'якшення фішингових атак, націлених на співробітників, системи та конфіденційні дані.

У США ЗЛАМАЛИ ДАНІ 237 000 ДЕРЖАВНИХ СЛУЖБОВЦІВ

Особиста інформація 237 000 нинішніх і колишніх службовців федерального уряду була розкрита в результаті витоку даних у Міністерстві транспорту США (USDOT), повідомляє Reuters 13 травня.

НОВЕ RANSOMWARE RA GROUP КОМПРОМЕТУЄ КОМПАНІЇ В США ТА ПІВДЕННІЙ КОРЕЇ – CISCO TALOS

15 травня експерти Cisco Talos опублікували свої виставки щодо нового ransomware RA Group, яке активне з квітня 2023 року. За їхньою оцінкою це модифіковане ransomware Babuk, вихідний код якого автор оприлюднив у вересні 2021 року. Нова група націлена на компанії, що займаються управлінням капіталом, страхові компанії та фармацевтику.

РОСІЯ ВІДМОВЛЯЄТЬСЯ ВИДАВАТИ ХАКЕРІВ, ЩО АТАКУВАЛИ MEDIBANK

23 травня Information Age повідомив, що рф відмовилася співпрацювати з австралійською поліцією у розслідуванні торішньої хакерської атаки на медичну страхову компанію Medibank. У ній стався знаковий витік даних, у результаті якого особисті дані 9,7 мільйона її нинішніх і колишніх клієнтів стали доступними для російських зловмисників. За даними видання, австралійська поліція поділилася інформацією з російською владою, але ті не відповіли взаємними діями. У рф знають, хто здійснив атаку, але відмовляються видавати зловмисників.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

NIST ГОТУЄ ТРЕТЮ РЕДАКЦІЮ SP 800-171

10 травня NIST оголосив про оновлення SP 800-171 – стандарту, що регулює захист контрольованої несекретної інформації в не федеральних системах і організаціях. Оновлення включають:

- переглянуті критерії, які використовуються NIST для розробки вимог безпеки;
- кращу узгодженість вимог безпеки в SP 800-171 Rev. 3 із SP 800-53 Rev. 5, щоб допомогти у впровадженні та оцінці.

NSA ОПУБЛІКУВАЛО РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ ДОМАШНІХ МЕРЕЖ

10 травня NSA оприлюднило найкращі практики, які допоможуть домогосподарствам краще захистити свої домашні мережі. Рекомендації поділяються на дві категорії – зміни у самій мережі та зміни в поведінці користувачів мережі. Хоча рекомендації є добре відомі, настанови NSA зосереджені саме на поведінковому блоці, який включає поради щодо розділення різних форм онлайн-активності, обмеження використання публічних бездротових мереж, використання належної гігієни паролів тощо.

NCSC НАМАГАЄТЬСЯ ЗМЕНШИТИ ЗАНЕПОКОЄННЯ УЧАСНИКІВ РИНКУ ЩОДО ІНФОРМУВАННЯ ДЕРЖАВИ ПРО КІБЕРАТАКИ

11 травня Елеанор Фейрфорд, заступник директора з управління інцидентами NCSC, і Міхаела Джембей, директор з регуляторної кібербезпеки в Офісі комісара з інформації (ICO), випустили спільну публікацію, спрямовану на розвіювання хибних уявлень про процес інформування держави про кіберінциденти. Відмова від інформування державних кіберстейкхолдерів про кіберінциденти залишається однією з головних проблем у розробці ефективних засобів протидії кібератакам. Багато приватних компаній уникають такого інформування, побоюючись подальшого оприлюднення інформації про такі інциденти – у цьому матеріалі є відповіді на 6 основних міфів.

ЗЛОВМИСНИКИ АКТИВНО ВИКОРИСТОВУЮТЬ ПОПУЛЯРНІСТЬ AI ПРОДУКТІВ ДЛЯ ПРОСУВАННЯ ЗЛОВМИСНИХ ПРОДУКТІВ

12 травня компанія Trend Micro оприлюднила результати дослідження щодо активності хакерів навколо популярності AI продуктів. Хакерські групи традиційно використовують сучасні інформаційні тенденції для більш ефективного проведення фішингових атак або використовують соціальну інженерію для збільшення доставлення шкідливого коду. Наразі вони зосереджені на AI продукти - хакери активно створюють підроблені субпродукти (сайти, застосунки тощо), які начебто дають доступ до найвідоміших AI продуктів. Насправді це типові фішингові сайти, які заражають системи відвідувачів.

NCSC СТВОРИЛО НОВІ ІНТЕРАКТИВНІ ІНСТРУМЕНТИ ПІДВИЩЕННЯ ОБІЗНАНОСТІ ОРГАНІЗАЦІЙ ЩОДО АТАК НА ЛАНЦЮЖКИ ПОСТАЧАННЯ

25 травня NCSC випустив кілька нових безплатних інтерактивних інструментів, розроблених, щоб спростити організаціям захист від атак на ланцюги постачання. Один із них має допомогти відобразити існуючий ланцюг постачань в організації. Другий – оцінити кібербезпеку цих ланцюгів.

США ПРОСУВАЮТЬ НОВУ СТРАТЕГІЮ ВСТАНОВЛЕННЯ ГЛОБАЛЬНИХ СТАНДАРТІВ ДЛЯ ШІ, КВАНТОВОЇ ТЕХНІКИ ТА МАШИННОГО НАВЧАННЯ

4 травня Білий дім оприлюднив нову стратегію, спрямовану на просування міжнародних правил, які встановили б деякі обмеження на розвиток штучного інтелекту, машинного навчання, квантових обчислення та інших технологій. Метою є забезпечення безпеки та взаємодія технологій і систем.
Зростаюча роль Китаю в міжнародних організаціях зі стандартизації спонукала США активізувати свою участь у розробці стандартів, зосередившись на критично важливих нових технологіях, життєво важливих для економічної та національної безпеки.
Стратегія має чотири головні цілі:

- інвестувати в технологічні дослідження та розробки,
- заохочувати участь приватного сектору та науковців,
- покращувати освіту та підготовку кадрів за стандартами США
- підтримувати цілісність стандартів, заснованих на достоїнствах технологій, через справедливий процес.

MERCK МАЄ ПРАВО ОТРИМАТИ 1,4 МІЛЬЯРДА ДОЛАРІВ У СПРАВІ ПРО КІБЕРАТАКУ ПІСЛЯ ВІДХИЛЕННЯ СУДОМ ПОЗОВУ СТРАХОВИКІВ ПРО «ВОЄННІ ДІЇ»

Суд Нью-Джерсі 3 травня постановив, що Merck може мати право на страхові виплати після кібератаки на компанію у 2017 році, повідомляє Fierce Pharma. Компанія стала жертвою кібератаки NotPetya у червні 2017 року. Пізніше уряд звинуватив у нападі російську розвідку та висунув звинувачення шістьом російським офіцерам.
Страховики Merck оскаржили виплату компанії в розмірі 1,4 мільярда доларів на підставі виключення з поліса «ворожих/воєнних дій», повідомляє Wall Street Journal. Однак цього тижня апеляційний суд заявив, що положення про виключення не повинно застосовуватися до невійськових афілійованих компаній, незалежно від їх походження. Це перемога Merck, але очікується подальший судовий процес.

ПОЧАТОК КІНЦЯ ПАРОЛЯ

3 травня Google оголосив про дебют ключа доступу, описавши його як «найпростіший і найбезпечніший спосіб входу в програми та вебсайти, а також важливий крок до «майбутнього без паролів».

ЧИ ПОТРІБНО ЗАБОРОНИТИ ВИПЛАТИ ВИКУПУ ШАХРАЯМ, ЩО ВИКОРИСТОВУЮТЬ ПРОГРАМИ-ВИМАГАЧІ?

Виступаючи на Ransomware Task Force 5 травня, заступниця радника Білого дому з національної безпеки Енн Нойбергер сказала, що заборона на виплату викупу шахраям, що використовують програми-вимагачі, протягом минулого року була основною темою обговорення серед членів Ініціативи протидії ransomware, як потенційний спосіб порушити екосистему програм-вимагачів.
Однак експерти з кібербезпеки кажуть, що заборона платежів може завдати ще більшої шкоди жертвам і спонукати компанії шукати обхідні шляхи. Сьогодні дискусія триває.

ДЖЕН ІСТЕРЛІ: АТАКА НА COLONIAL PIPELINE: ЧОГО МИ НАВЧИЛИСЯ ТА ЩО МИ ЗРОБИЛИ ЗА ОСТАННІ ДВА РОКИ

7 травня, через два роки після атаки на Colonial Pipeline, директорка CISA Джен Істерлі опублікувала статтю, в якій детально описується ряд заходів, спрямованих на розбудову стійкості національної критичної інфраструктури в США.
Вона наголосила, що виходячи з оцінок американської розвідувальної спільноти у разі неминучого серйозного конфлікту з США Китай майже напевно розгляне можливість наступальних кібероперацій проти критичної інфраструктури США. На її думку, США повинні підготуватись до такого сценарію, зробивши такі першочергові кроки:

1. переконатися, що технологія, яка лежить в основі послуг, на які американці покладаються щогодини щодня, надійна та безпечна;
2. надати найвищий пріоритет питанням кібербезпеки;
3. продовжувати інвестувати в модель JCDC постійної та проактивної оперативної співпраці між урядом і промисловістю, де за замовчуванням є обмін інформацією про зловмисну кіберактивність, знаючи, що загроза для одного є загрозою для всіх.

ROYAL RANSOMWARE АТАКУВАЛО ІНФОРМАЦІЙНІ СИСТЕМИ ДАЛЛАСУ

3 травня Служба інформаційно-технологічних послуг Далласа (ITS) заявила, що близько 200 із тисячі пристроїв у цьому американському місті були уражені вірусом. Атака порушила роботу комп'ютерної диспетчерської системи Департаменту поліції Далласа. Постраждали деякі платіжні системи міста, а міські суди були змушені закритись. За наявними даними зловмисники вимагали викуп від 1 до 11 мільйонів доларів.

ГЕНЕРАТИВНИЙ ШІ ПІДТРИМУЄ АНАЛІТИКІВ КІБЕРБЕЗПЕКИ. ОБМЕЖЕННЯ НАВЧАЛЬНИХ ДАНИХ CHATGPT ПІДВИЩУЄ ТОЧНІСТЬ

Щоб уникнути тенденції платформи штучного інтелекту ChatGPT вигадувати факти та приховувати помилки, Recorded Future використовував вузько визначені набори даних для навчання генеративної платформи Компанія створила платформу штучного інтелекту на основі більш ніж десятирічного експертного аналізу та надала платформі GPT OpenAI понад 40 000 аналітичних нотаток від відділу аналізу загроз Insikt Group. штучного інтелекту для підтримки своїх аналітиків і клієнтів.
Дані Intelligence Cloud також були додані для створення автоматизованого інструменту підтримки кібербезпеки, який автоматично збирає та аналізує інформацію, сказав доктор Крістофер Алберг, генеральний директор і співзасновник Recorded Future. Це значно полегшує роботу аналітика.

РОСІЙСЬКІ APT ВСЕ ЧАСТІШЕ КОМПРОМЕТУЮТЬ МАЛИЙ ТА СЕРЕДНІЙ БІЗНЕС ДЛЯ ПОДАЛЬШИХ ЦІЛЬОВИХ АТАК – PROOFPOINT

24 травня експерти Proofpoint опублікували своє дослідження ландшафту загроз для малого та середнього бізнесу. Одним із висновків дослідження є те, що російські APT-групи (такі як TA473, TA422 або TA499), дедалі частіше намагаються атакувати МСП не заради прибутку, а щоб отримати кращі позиції для подальших атак. Дослідники наводять декілька таких кейсів, зокрема те, як скомпрометовані МСП використовувались для атаки на урядові установи в США та Європі, або цілі в Україні.

5. КРИТИЧНА ІНФРАСТРУКТУРА

КРИТИЧНА ВРАЗЛИВІСТЬ SIEMENS RTU МОЖЕ ДОЗВОЛИТИ ХАКЕРАМ ДЕСТАБІЛІЗУВАТИ ЕНЕРГОМЕРЕЖУ

5 травня компанія Siemens оголосила, що виправила критичну вразливість, яка могла вплинути на деякі енергетичних пристроїв ICS. Своєю чергою це може дозволити хакерам дестабілізувати енергомережу. Уразливість, яка відстежується як CVE-2023-28489, впливає на мікропрограму CPCI85 продуктів Sicam A8000 CP-8031 і CP-8050, і нею може скористатися неавтентифікований зловмисник для віддаленого виконання коду. Вразливість актуальна для віддалених терміналів (RTU), призначених для дистанційного керування та автоматизації в секторі енергопостачання, зокрема для підстанцій.

США ДОСЛІДЖУЮТЬ РИЗИКИ ДЛЯ КІБЕРБЕЗПЕКИ ВІД ДІЯЛЬНОСТІ ROCKWELL AUTOMATION

11 травня повідомлялося, що кілька департаментів уряду США беруть участь у розслідуванні потенційних ризиків для кібербезпеки, пов'язаних з діяльністю американського промислового гіганта Rockwell Automation у Китаї. Урядовці особливо зацікавлені в Rockwell у Даляні (Китай). За попередніми даними, співробітники підприємства могли отримати доступ до інформації, яка могла бути використана для компрометації клієнтських систем компанії. Продукти Rockwell Automation широко використовуються в критичній інфраструктурі, державному, військовому та енергетичному секторах Сполучених Штатів. До розслідування залучені міністерства оборони, енергетики та юстиції. За минулий рік CISA опублікувала та оновила понад дюжину рекомендацій щодо вразливостей Rockwell Automation.

УРАЗЛИВОСТІ В ПРОДУКТАХ TELTONIKA МОЖЕ НАРАЖАТИ ТИСЯЧІ ПРОМИСЛОВИХ ОРГАНІЗАЦІЙ НА ВІДДАЛЕНІ АТАКИ

16 травня експерти з компаній промислової кібербезпеки Otorio і Claroty повідомили про потенційно серйозну вразливість, виявлену в продуктах Teltonika. Вони можуть наражати організації на віддалені хакерські атаки.
Teltonika Networks – литовська компанія, яка виробляє LTE-маршрутизатори, шлюзи, модеми та інші мережеві рішення, що використовуються в глобальній промисловості, енергетиці, комунальному господарстві, розумних містах, транспорті, підприємствах, роздрібній торгівлі. Постачальника було повідомлено, і він вже випустив патчі.

LACROIX ЗАКРИВ ВИРОБНИЧІ МАЙДАНЧИКИ ПІСЛЯ АТАКИ RANSOMWARE

17 травня гігант технологічного обладнання Lacroix Group заявив, що закрив три виробничі майданчики на тиждень після атаки програм-вимагачів. Lacroix є міжнародним розробником і виробником вбудованих і промислових систем Інтернету речей (IIoT), включаючи автомобільне та аерокосмічне обладнання, обладнання для водної та енергетичної інфраструктури, а також рішення для розумної дорожньої інфраструктури. За даними компанії, в ніч на 12 травня вона виявила цілеспрямовану кібератаку на заводи з виробництва електронних систем у Франції, (Beaupréau), Німеччині (Willich) і Тунісі (Zriba).

ДОСТУП ДО СИСТЕМ ICS/OT ЕНЕРГЕТИЧНОГО СЕКТОРУ ПРОПОНУЄТЬСЯ НА ХАКЕРСЬКИХ ФОРУМАХ – SEARCHLIGHT CYBER

17 травня компанія з кібербезпеки Searchlight Cyber опублікували новий звіт, заснований на моніторингу дописів, опублікованих на форумах кіберзлочинців і у Dark Web з лютого 2022 року по лютий 2023 року. Хоча в багатьох випадках зловмисники пропонували доступ до корпоративних систем енергетичних компаній, деякі пропонували доступ та інші ресурси, спрямовані на системи ICS/OT США, Канаді, Великобританії, Італії, Франції та Індонезії.
У компанії не змогли підтвердити правдивість пропозицій, але відзначили загальне зростання інтересу зловмисників до ICS/OT.

НОВЕ ЗЛОВМИСНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ COSMICENERGY ICS, ПОВ'ЯЗАНЕ З РОСІЄЮ, МОЖЕ ПОРУШИТИ РОБОТУ ЕЛЕКТРОМЕРЕЖ – MANDIANT

25 травня Mandiant опублікував детальний аналіз нового шкідливого програмного забезпечення, яке, ймовірно, пов'язане з росією та призначене для націлювання на промислові системи управління (ICS), зокрема, зокрема викликаючи збої в електромережах. Воно називається CosmicEnergy та орієнтоване на взаємодію з пристроями IEC 60870-5-104 (IEC-104).
Зловмисне програмне забезпечення надсилає віддалені команди для втручання в роботу вимикачів ліній електропередач і автоматичних вимикачів, викликаючи збої в електроживленні. Mandiant вважає, що це становить реальну загрозу для постраждалих активів електромереж. Протокол IEC 60870-5-104 який зазвичай використовуються для передачі та розподілу електроенергії в таких регіонах, як Європа та Близький Схід.

6. АНАЛІТИЧНІ ОЦІНКИ

RAAS ГРУПИ СТВОРИЛИ ЕФЕКТИВНУ БІЗНЕС-МОДЕЛЬ, ЩО УСКЛАДНЮЄ БОРОТЬБУ З НИМИ

Ransomware-as-a-Service групи на кшталт Qilin створили ефективні бізнес-моделі для свого зловмисного ПЗ, що ускладнює боротьбу з ними. За словами експертів Group-IB, які проникли в це угрупування, філії Qilin (ті, хто платить за використання програм-вимагачів Qilin для власних атак та проводять атаки) можуть отримати 80 відсотків сплаченого викупу (якщо сплачений викуп становить 3 мільйони доларів США або менше). Якщо сума викупу перевищує три мільйони доларів, скорочення філії може зрости до 85 відсотків. Для зловмисників, яким не потрібно розробляти власне програмне забезпечення-вимагач, такі високі винагороди допомагають зосередитися на пошуку жертв.

ДЕТАЛІ ВІДОМОЇ НА СЬОГОДНІ АТАКИ НА ЛАНЦЮГ ПОСТАЧАННЯ SOLAR WINDS

У статті, опублікованій 2 травня, Кім Зеттер докладно розповідає про те, що відомо про розслідування атаки на ланцюжок постачання Solar Winds, від перших припущень у 2019 році про те, що щось відбувається, до слідчих, які розкривають хакерську діяльність, до недавніх викриттів CISA та Національної кібернетичної місії США (на RSA Conference минулого місяця) про їхню реакцію на кампанію.

КІЛЬКІСТЬ RANSOMWARE АТАК У 2022 РОЦІ ЗМЕНШИЛАСЬ – IBM X-FORCE THREAT INTELLIGENCE INDEX 2023

Новий звіт IBM X-Force Threat Intelligence Index 2023 був опублікований 17 травня. Зазначається, що кількість інцидентів з програмами-вимагачами знизиться з 21% до 17% у 2022 році.
Загалом дослідники вважають, що 2022 рік був важким для ransomware груп – деякі були ліквідовані правоохоронними органами або розпались, а інші постраждали від внутрішнього витоку інформації. Хоча достеменно невідомо чи дійсно зменшилася кількість інцидентів, але кількість сплачених викупів дійсно зменшилася, ймовірно через те, що організації краще захищають свої резервні копії, а санкції OFAC (Управління з контролю за іноземним доступом) роблять платежі більш ризикованими.

ЕЛЕКТРОННА ПОШТА ЗАЛИШАЄТЬСЯ ОДНИМ ІЗ КЛЮЧОВИХ ВЕКТОРІВ КІБЕРАТАК – TREND MICRO

4 травня компанія Trend Micro опублікувала результати свого дослідження щодо ландшафту кіберзагроз електронної пошти 2022 року. За даними компанії, загалом до 2022 року було попереджено 146 мільярдів загроз, 55% з яких – електронні листи. Слід відзначити, що на невідоме зловмисне програмне забезпечення (тобто щойно створене зловмисне програмне забезпечення нульової години тощо) становило більшість загроз і загалом використання невідомого шкідливого програмного забезпечення зросло на 46% порівняно з попереднім роком. Ці висновки підтверджують позицію ФБР про те, що злом корпоративної електронної пошти (BEC) – є набагато більшою загрозою, ніж програми-вимагачі, оскільки BEC завдає набагато більшої шкоди програми-вимагачів.

79% КІБЕРПРОФЕСІОНАЛІВ ПРИЙМАЮТЬ РІШЕННЯ БЕЗ АНАЛІЗУ ЗАГРОЗ – MANDIANT

Відповідно до нового дослідження Mandiant, опублікованого 4 травня, переважна більшість (79%) експертів приймають рішення про реагування на кіберзагрози без детального аналізу самої загрози. Хоча всі вони визнають важливість цього компонента, вони не змогли повною мірою скористатись перевагами інструменту через брак часу та перевантаження.

ЧИ НЕ ЗАБАГАТО МИ ХОЧЕМО ВІД КІБЕРУ?

У статті від 2 травня про War on the Rocks, Еріка Лонерган і Майкл Познанський оскаржують висновки розвідувальної спільноти США щодо китайської загрози у кіберпросторі. Автори вважають, що використовувати кіберінструменти проти OKI США з метою примусу буде складно, тому що досягти ефекту примусу взагалі важко, а кіберінструменти у цій сфері не є особливим. Тим часом політики продовжують сподіватися, що з їх допомогою вдасться досягти бажаного результату. Автори закликають політиків визнати обмеження кіберінструментів і прагнути використовувати їх ефективніше, швидше за все для збору інформації, яка може бути використана для застосування нецифрових форм стримування та примусу.

ЯК КОМАНДУВАННЯ ТА УПРАВЛІННЯ ХРОБАКОМ МОРРІСА ЗМІНИЛО КІБЕРБЕЗПЕКУ

У статті Security Intelligence Джонатан Рід підкреслює роль серверів C2 у здійснення кібератак, починаючи з Morris Worm. Він зазначив, що у 2022 році кількість серверів C2, які використовувалися для проведення кібератак, зросла на 30%. Минулого року було виявлено понад 17 000 серверів, у порівнянні з 13 629 у 2021 році. У статті наголошується, що захист вимагає багаторівневої системи. Автор перераховує деякі необхідні заходи, однак, добре відомі експертам з кібербезпеки.

КІЛЬКІСТЬ КАМПАНІЙ РОЗСИЛКИ ЗЛОВМИСНИХ ПОВІДОМЛЕНЬ, ЩО ЗЛОВЖИВАЮТЬ БОТАМИ TELEGRAM, НАДЗВИЧАЙНО ЗРОСЛА В ПЕРШОМУ КВАРТАЛІ 2023 РОКУ, ПЕРЕВИЩИВШИ ВЕСЬ 2022 РІК НА 310%

2 травня компанія Cofense опублікувала огляд тенденцій у сфері фішингу за 1 квартал 2023 року. У першому кварталі кількість повідомлень про активні загрози зросла на 20 відсотків порівняно з попереднім кварталом і на 34 відсотки порівняно з першим кварталом 2022 року. Найпоширеніші сімейства та типи зловмисного ПЗ були в основному такими ж, як і в четвертому кварталі. Однак найпомітнішою зміною у типах шкідливого програмного забезпечення стало збільшення на 38% використання клавіатурних шпигунів.
Qakbot залишається найуспішнішою сім'єю зловмисних програм, які потрапляли до папок «Вхідні», на 185% частіше, ніж Emotet, попри надзвичайно великий обсяг розповсюдження.
У першому кварталі 2023 року кількість людей, які використовують ботів Telegram для виведення грошей, різко зросла на 397%.
Крім того, використання ботів Telegram уже досягло нових максимумів у першому кварталі 2023 року порівняно з усім минулим роком і, як очікується, залишиться або навіть перевищить цей рівень. З початком літа Cofense очікує збільшення спроб фішингу.

ЗА ДАНИМИ REUTERS, КИТАЙСЬКІ ХАКЕРИ ПРОВОДЯТЬ ТРИВАЛУ АТАКУ НА УРЯДУ КЕНІЇ – ОФІЦІЙНІ ОСОБИ КЕНІЇ ЦЕ ЗАПЕРЕЧУЮТЬ

24 травня Reuters повідомило з посиланням на свої джерела та власний аналіз, що Китай проводить довгострокову масштабну кампанію проти кенійського уряду, особливо для того, щоб отримати інформацію про стан економіки країни та її можливості сплатити зовнішніх боргів, більшість з яких китайські. Кенія використала понад 9 мільярдів доларів китайських позик для фінансування проєктів будівництва або модернізації залізниць, портів і автомагістралей. Ще 25 травня головний секретар внутрішньої безпеки та національної адміністрації Раймонд Омолло виступив проти оприлюдненої інформації, назвавши її «пропагандою».

У ЦЕНТРІ УВАГИ ЗАГРОЗИ: ЧАСТКА ШКІДЛИВИХ ВКЛАДЕНЬ HTML ПОДВОЮЄТЬСЯ ПРОТЯГОМ РОКУ

3 травня Barracuda опублікувала дослідження, яке показало, що кількість HTML-атак подвоїлася порівняло з минулим роком. Дослідники відзначають, що зростає не тільки загальна кількість атак, але й кількість унікальних атак. «Із загальних 475 938 зловмисних артефактів HTML 23 березня майже дев'ять із десяти (405 438 — 85%) були унікальними. Це означає, що майже кожна атака відрізнялась від інших». HTML-атаки поширені у фішингових кампаніях, коли користувачі завантажують HTML-додатки з електронних листів.
Barracuda рекомендує організаціям запровадити інструменти захисту електронної пошти для виявлення та блокування зловмисних вкладень HTML, навчити співробітників виявляти фішингові електронні листи, запровадити багатофакторну автентифікацію та розглянути модель безпеки з нульовою довірою. А також підготувати план реагування на інциденти, який містить способи зриву кампанії, якщо зловмисники проникнуть у мережу організації.

АМЕРИКАНСЬКА РОБОЧА ГРУПА З ПРОГРАМ-ВИМАГАЧІВ ВИПУСТИЛА РЕТРОСПЕКТИВНИЙ ЗВІТ ЗА ДВА РОКИ

5 травня члени спеціальної групи Ransomware Task Force, створеної Управлінням звітності уряду США (GAO) для відстеження тенденцій програм-вимагачів і розробки протоколів для усунення загрози, опублікували звіт про хід роботи. «Ми досягаємо прогресу, але завжди є над чим працювати», – зазначив один із членів робочої групи. Близько 92% пропозицій Taks Force вже реалізовано, і щонайменше вони призвели до «певного зменшення ефективності [вимагачів]».
Робоча група закликала приватні компанії проявити ініціативу щодо створення нових «найкращих практик» у сфері кібербезпеки. «Уряди – не є єдиним засобом покращення базової кібербезпеки. У той час як кіберстраховики та перестраховики працюють над розподілом ризиків, таких як програми-вимагачі, вони можуть відігравати більшу роль у покращенні безпеки страхувальників». Автори звіту також виступають за «перегляд структури стимулів», зокрема запровадження податкових пільг МСП, які дотримуються встановлених передових практик кібербезпеки.

BLACKBERRY ПОВІДОМЛЯЄ ПРО ЗБІЛЬШЕННЯ КІЛЬКОСТІ КІБЕРАТАК

Звіт про аналіз загроз, опублікований BlackBerry 5 травня, показав, що з грудня 2022 року по лютий 2023 року щохвилини відбувалося 12 кібератак на організації, які використовували програмне забезпечення та служби кібербезпеки компанії, 1,5 з яких були атаками на основі нових типів зловмисного програмного забезпечення.
У звіті BlackBerry також відзначаються зміни у географії атак. Наразі Бразилія є другою за кількістю жертв після США країною, а Канада та Японія – третім та четвертим відповідно. Сінгапур вперше увійшов до десятки найбільш атакованих країн.
Віцепрезидент із дослідження загроз і розвідки BlackBerry Ісмаель Валенсуела сказав, що зростання темпів атак свідчить про те, що кіберзлочинці вкладають значні кошти в автоматизацію, і це починає окупатися. Замість того, щоб намагатися розробити складніші атаки, кіберзлочинці, здається, зосереджуються на збільшенні обсягу атак на основі перевірених і надійних методів.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

УКРАЇНА СТАЛА ЧЛЕНОМ ОБ'ЄДНАНОГО ЦЕНТРУ ПЕРЕДОВИХ ТЕХНОЛОГІЙ З КІБЕРОБОРОНИ НАТО

16 травня 2023 року Україна стала повноцінним членом Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE) зі статусом країни-контрибутора. З цієї нагоди у Центрі, що знаходиться в Таллінні (Естонська Республіка), відбулася офіційна церемонія підняття прапору нашої держави як нового члена CCDCOE.
Приєднання України до CCDCOE було ініційовано Національним координаційним центром кібербезпеки при РНБО України.
«Історичний день для нашої країни, і, безумовно, важливий крок для вступу України в НАТО. Членство в CCDCOE дозволить нам ефективніше взаємодіяти на міжнародній арені у сфері кібербезпеки та кібероборони, а також обмінюватися досвідом з країнами-членами Центру. Адже сьогодні Україна на передовій світової кібервійни, яку рф веде проти нас, країн Європи та інших демократичних держав. І ми маємо мобілізувати усі необхідні ресурси, об'єднати сили та засоби для того, щоб разом раз і назавжди дати відсічі ворогу», – зазначив Секретар РНБО України Олексій Данілов.
Членство в CCDCOE дозволить оперативно обмінюватись інформацією щодо виявлення та протидії сучасним кіберзагрозам, відпрацьовувати навички спільного реагування на кібератаки, проводити спільні операції оборони і стримування у кіберпросторі, а також брати участь у формуванні стратегічних підходів та вироблення нових політик у сфері кібербезпеки та кібероборони на міжнародному рівні. Україна отримає доступ до передових технологій та провідних досліджень, які проводяться CCDCOE.

НКЦК ПОГЛИБЛЮЄ СПІВПРАЦЮ З ПРОВІДНОЮ КОМПАНІЄЮ З КІБЕРБЕЗПЕКИ RECORDED FUTURE

Заступник Секретаря РНБО України Сергій Демедюк, керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Наталія Ткачук та керівник Управління забезпечення діяльності НКЦК Сергій Прокопенко під час робочої зустрічі з генеральним директором і співзасновником Recorded Future Крістофером Альбергом обговорили шляхи поглиблення практичного співробітництва між НКЦК та цією компанією.
«Сьогодні кібератаки – це повноцінна складова війни росії проти України. І для перемоги у кібервійні ми використовуємо всі наявні ресурси – постійно взаємодіємо з провідними компаніями та урядами демократичних країн світу, посилюємо співпрацю для обміну інформацією, проводимо навчання, разом протидіємо агресії рф. Адже лише завдяки спільним зусиллям ми можемо пришвидшити перемогу України та здолати спільного ворога. І ми вдячні компанії Recorded Future за допомогу та високо цінуємо їхню підтримку», – зазначив С. Демедюк.

ПИТАННЯ КІБЕРБЕЗПЕКИ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ОБГОВОРИЛИ НА НАЦІОНАЛЬНОМУ КЛАСТЕРІ КІБЕРБЕЗПЕКИ

Учасники XIX засідання Національного кластера кібербезпеки на тему «Кібербезпека у сфері охорони здоров`я та медицини: основні виклики та загрози» обговорили питання захисту медичних даних та протидію кібератакам в інформаційних системах сфери охорони здоров'я.
Відкриваючи засідання, керівник управління забезпечення діяльності НКЦК профільної служби Апарату РНБО Сергій Прокопенко зазначив, що ворожі атаки рф мають дві мети – руйнування інфраструктури та доступ до персональних даних громадян.
«Захист персональних та медичних даних дуже важливий, особливо коли наша країна перебуває у стані війни. російські хакери постійно намагаються викрасти дані українців для кібератак та інформаційних кампаній. Тому ми повинні приділяти особливу увагу питанням кібербезпеки на стратегічному, організаційному та технічному рівнях. Адже будь-хто в державному та приватному секторах може стати елементом атаки на ланцюг постачання», – зазначив С. Прокопенко.
Понад 200 представників з 80 організацій взяли участь у заході у форматі онлайн.
Ключовими спікерами заходу були представники МОЗ України, Національної служби здоров'я України (НСЗУ), eHealth, CISA та інших організацій, відповідальних за цифровізацію та кібербезпеку галузі.

УКРАЇНСЬКА ДЕЛЕГАЦІЯ У СТАТУСІ ЧЛЕНА CCDCOE ВПЕРШЕ ВЗЯЛА УЧАСТЬ У ЗАСІДАННІ КЕРІВНОГО КОМІТЕТУ ЦЕНТРУ

Українська делегація взяла участь у засіданні Керівного комітету Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE), яке відбулося 29 травня 2023 року у Таллінні. Голова української делегації – заступник Секретаря Ради національної безпеки і оборони України Сергій Демедюк зазначив, що підняття прапору України в CCDCOE стало важливим кроком нашої держави на шляху вступу до НАТО.
«Україна, яка вже понад вісім років змушена відстоювати свою незалежність та боротись з країною-терористом на усіх фронтах, показала високий рівень стійкості й у кіберпросторі. Проте російські хакери – це загроза не тільки для нашої держави, а й для всього світу. Для забезпечення міжнародної безпеки та основоположних цінностей усього демократичного світу ми маємо об'єднатись та разом протистояти спільному ворогу», – сказав С. Демедюк.
Також заступник Секретаря РНБО України подякував членам Керівного комітету за підтримку України, зазначивши, що CCDCOE продемонстрував єдність у питанні вступу нашої держави до Центру.

МІНЦИФРА ВЗЯЛА УЧАСТЬ У ЗАСІДАННІ МІНІСТРІВ ЦИФРОВІЗАЦІЇ G7

29–30 квітня в Японії відбулося засідання міністрів цифровізації — G7 Digital and Tech Ministers' Meeting 2023. Українську делегацію представила Валерія Іонан, заступниця Міністра цифрової трансформації з питань євроінтеграції. Зустріч пройшла в межах підготовки до саміту країн «Великої сімки».
Під час засідання ключова увага була приділена принципам управління новими технологіями. Учасники обговорили цифровізацію суспільства, транскордонну передачу даних, використання штучного інтелекту, забезпечення стійкої цифрової інфраструктури та виклики у сфері кібербезпеки.
«Засідання G7 формують глобальний порядок денний. Для України велика честь бути учасником конференції такого рівня та мати змогу ділитися досвідом розбудови цифрової держави і стійкості. Вдячні країнам «Великої сімки» за одностайну підтримку України та готовність до стратегічної співпраці», — зазначає Валерія Іонан.
Наприкінці засідання міністри G7 уклали спільну декларацію, у якій визначили напрями співпраці щодо розвитку цифрових інновацій. Уряди погодилися, що технологічна інфраструктура відіграє ключову роль у вирішенні глобальних проблем, як-от зміна клімату, наслідки пандемії Covid-19 та війна проти України. Також «Велика сімка» визначили пріоритетом подолання цифрового розриву та розбудову телекомунікаційної інфраструктури.

В АПАРАТІ РНБО УКРАЇНИ ВІДБУЛАСЯ РОБОЧА ЗУСТРІЧ З ПИТАНЬ ПОДАЛЬШОЇ ВЗАЄМОДІЇ ОСНОВНИХ СУБ'ЄКТІВ КІБЕРБЕЗПЕКИ З CCDCOE

Національний координаційний центр кібербезпеки 23 травня 2023 року провів робочу зустріч в Апараті РНБО України під головуванням заступника Секретаря РНБО України Сергія Демедюка щодо питань взаємодії представників основних суб'єктів кібербезпеки України з Об'єднаним центром передових технологій з кібероборони НАТО (CCDCOE). Обговорено механізм взаємодії та участь українських фахівців у заходах CCDCOE.
Керівник служби з питань інформаційної та кібербезпеки Апарату РНБО України, секретар НКЦК Наталія Ткачук зазначила, що тепер Україна може краще взаємодіяти на міжнародній арені у сфері кібербезпеки та кібероборони.
«Членство в CCDCOE також сприятиме посиленню спроможностей національної системи кібербезпеки України. Зараз на базі НКЦК ми впроваджуємо ефективний механізм взаємодії з нашим представником в CCDCOE для оперативного обміну інформацією щодо виявлення і протидії сучасним кіберзагрозам та відпрацювання навичок спільного реагування на кібератаки в інтересах всіх суб'єктів кібербезпеки України, а також забезпечення активної участі України у формуванні стратегічних підходів та політик щодо ключових питань кібербезпеки та кібероборони на міжнародному рівні», – додала Н. Ткачук.
Також під час заходу було обговорено участь представників основних суб'єктів кібербезпеки у заходах, організованих CCDCOE. Окрему увагу приділено залученню України до щорічних кібернавчань Центру – Locked Shields. Адже у цьому році Україна разом зі США та Естонією посіла друге місце у цих змаганнях. А наступного року для розробки сценарію для Locked Shields-2024 планується використати досвід України у кібервійні.

СТАРТУВАВ НОВИЙ ЕТАП ІНФОРМАЦІЙНОЇ КАМПАНІЇ #ШАХРАЙГУДБАЙ: КІБЕРПОЛІЦІЯ НАГАДУЄ ПРО ВАЖЛИВІ ПРАВИЛА ПЛАТІЖНОЇ БЕЗПЕКИ

Всеукраїнська інформаційна кампанія з платіжної безпеки #ШахрайГудбай покликана поліпшити обізнаність громадян і нагадати про основні правила безпеки під час безготівкових розрахунків. З нагоди старту нового етапу кампанії відбувся круглий стіл за участі генеральних партнерів, зокрема Департаменту кіберполіції.
«З початку цього року до Департаменту кіберполіції надійшло вже понад 20 тисяч звернень громадян, з них – понад 75% щодо шахрайства в Інтернеті. Аналогічні відсоткові показники ми спостерігали й минулого року, відповідно протидія онлайн-шахрайству залишається одним з основних напрямів роботи кіберполіції», – наголосив начальник Департаменту кіберполіції Юрій Виходець.
Він зазначив, що завдяки спільній ініціативі Національного координаційного центру кібербезпеки РНБО, Національного центру оперативно-технічного управління мережами телекомунікацій, Нацбанку та Кіберполіції було налагоджено механізм для фільтрації фішингових доменів і подальшого їх блокування. З початку цього року заблоковано більше 16 тисяч доменних імен, які шахраї використовували для створення фішингових посилань і завдяки цьому, кількість злочинів пов'язаних з фішингом знизилась майже на 30%.
Інформаційна кампанія триватиме до кінця року у всіх регіонах України. Національний банк разом із партнерами інформуватимуть громадян про те, як вберегтися від платіжного шахрайства.

ДЕРЖСПЕЦЗВ'ЯЗКУ ВІДВІДАЛА РУМУНСЬКА ТЕХНІЧНА ДЕЛЕГАЦІЯ З КІБЕРБЕЗПЕКИ

Румунська технічна делегація з кібербезпеки на чолі з головою Національного Директорату з питань кібербезпеки Румуні Державним секретарем Деном Кімпеаном відвідала Державну службу спеціального зв'язку та захисту інформації України.
Під час зустрічі з головою Держспецзв'язку Юрієм Щиголем, а також заступниками голови Держспецзв'язку Віктором Жорою та Олександром Потієм представники румунської сторони обговорили розширення співпраці між DNSC та Держспецзв'язку, в тому числі питання співпраці, пов'язані з кіберзагрозами та кібератаками агресора в межах російсько-української війни.
Особлива увага була приділена обміну досвідом у сфері захисту критичної інфраструктури та гармонізації нормативної бази з нормами ЄС, налагодженню співпраці з органами NATO та ЄС і настановам щодо узгодження та взаємодії з органами ЄС. Крім того, румунська делегація відвідала Кіберцентр UA30 та поспілкувалася з представниками Урядової команди реагування на комп'ютерні надзвичайні інциденти (CERT-UA).

НАТАЛІЯ ТКАЧУК ВЗЯЛА УЧАСТЬ У ЧОРНОМОРСЬКОМУ РЕГІОНАЛЬНОМУ ФОРУМІ ВИПУСКНИКІВ ПРОГРАМ ЄВРОПЕЙСЬКОГО ЦЕНТРУ ДОСЛІДЖЕНЬ ПРОБЛЕМ БЕЗПЕКИ ІМ. ДЖ. МАРШАЛЛА

Керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Наталія Ткачук взяла участь у Чорноморському регіональному форумі випускників програм Європейського центру досліджень проблем безпеки ім. Дж. Маршалла. Учасники заходу обговорили питання щодо визначення та нейтралізації перешкод для вступу України та Молдови до ЄС, а також протидії гібридному впливу рф.
Українська сторона поділилася успішним досвідом із протидії інформаційній та кіберагресії рф в умовах воєнного стану та розбудови національної стійкості. Н. Ткачук під час виступу наголосила, що нині Україна – єдина країна у світі, яка змогла здобути перевагу у протистоянні кібератакам та інформаційній агресії рф.
«Досвід України є неоціненним для країн Європи. Критичне мислення українського народу вже на такому високому рівні, що маємо національний імунітет від російської пропаганди. Завдяки Україні весь демократичний світ нарешті усвідомив, що росія весь цей час була та залишається країною-терористом», – зазначила Н.Ткачук.

ФАХІВЦІ АПАРАТУ РНБО УКРАЇНИ ВЗЯЛИ УЧАСТЬ У КОНФЕРЕНЦІЇ З ПИТАНЬ СТІЙКОСТІ ЗВ'ЯЗКУ ТА ІНТЕРНЕТУ ПІД ЧАС ВІЙНИ

Заступник керівника служби з питань інформаційної безпеки та кібербезпеки – керівник управління інформаційної безпеки профільної служби Апарату РНБО України Володимир Звєрєв 26 травня 2023 року взяв участь у конференції «Україна: стійкість зв'язку та інтернету під час війни».
Учасники заходу обговорили питання забезпечення зв'язку в умовах війни, взаємодію між зацікавленими сторонами та потреби у відновленні телекомунікаційної інфраструктури.
«Завдяки ефективній взаємодії та своєчасному прийняттю рішень РНБО України та НКЦК наша країна не лише вистояла, але й здобула перевагу в інформаційному та кіберпросторі. Держава, критична інфраструктура та бізнес виступили єдиним фронтом, і саме це стало ключовим і вирішальним у нашій боротьбі», – зазначив Володимир Звєрєв.

МІНЦИФРА ТА PALANTIR ПІДПИСАЛИ МЕМОРАНДУМ ПРО СПІВПРАЦЮ У СФЕРАХ ОБОРОНИ Й ВІДБУДОВИ УКРАЇНИ ПІСЛЯ РОСІЙСЬКОГО ВТОРГНЕННЯ

Співпраця передбачає використання технологій Palantir, зокрема при оцінці пошкоджень будівель та інфраструктури, а також використання програмного забезпечення для оптимізації відбудови.
«Для нас велика честь продовжувати розвивати партнерство з такою топкомпанією. Palantir робить свій внесок у перемогу України, надаючи технологічні інструменти та аналітику. Ми з нетерпінням чекаємо початку нового етапу співпраці в межах відновлення України. Співпраця з Palantir з моменту повномасштабного вторгнення також має вагоме значення для економіки та побудови нового іміджу України за кордоном — сміливого і цифрового», – зазначив Михайло Федоров, Віцепрем'єр-міністр з питань інновацій, розвитку освіти, науки і технологій – Міністр цифрової трансформації України.
Palantir — світовий лідер з розробки програмного забезпечення та постачальник хмарних рішень, продуктами якого користується Міністерство оборони США та великі інвестиційні банки. Компанія розширить партнерство з Україною для досягнення спільних цілей. Так, меморандум передбачає:

- посилення цифрових можливостей для надання електронних державних послуг, оборони та відбудови України;
- підтримку та координацію відбудови України на основі цифрових технологій;
- об'єднання зусиль у сфері цифровізації, цифрових інновацій та інтеграції України в міжнародний ринок;
- обмін даними та досвідом у впровадженні провідних світових технологій за підтримки Збройних сил України.

УКРАЇНА ПОКРАЩУЄ ЯКІСТЬ ПІДГОТОВКИ ПРОФЕСІЙНИХ КАДРІВ У ГАЛУЗІ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Державна служба спеціального зв'язку та захисту інформації України і Національне агентство із забезпечення якості вищої освіти 5 травня 2023 року підписали Меморандум про співпрацю.
Задля неупередженої та достовірної експертизи якості підготовки відповідних фахівців у закладах освіти представників Держспецзв'язку залучатимуть як експертів Національного агентства із забезпечення якості вищої освіти. Протягом останнього часу межі освітніх програм у закладах освіти дещо розмились, низка ВНЗ почали відкривати ОПП з приставкою «кібербезпека» та професійними кваліфікаціями, яких не існує, у дипломах. Такі приставки приваблюють абітурієнтів, але часто унеможливлюють підготовку професійних спеціалістів, яких потребує реальний сектор та які мають право обіймати відповідні посади згідно із класифікатором професій України. Особливо це стосувалось охочих вступити на державну службу, до спеціальних підрозділів кіберзахисту, у банки тощо.
Зараз ситуація виправляється. Сформована нова національна рамка професійних кваліфікацій у галузі кібербезпеки та захисту інформації. Проведена гармонізація професій із міжнародними стандартами. Розроблено вже шість найбільш актуальних професійних стандартів, які перекривають 14 різнорівневих посад у сфері кібербезпеки та захисту інформації.

ПОСИЛЮЄМО КІБЕРЗАХИСТ: УРЯД УХВАЛИВ МЕХАНІЗМ ПРОВЕДЕННЯ BUG BOUNTY

Кабінет Міністрів України ухвалив постанову, розроблену Держспецзв'язку, яка визначає порядок пошуку та виявлення потенційних вразливостей в електронних системах. Це дасть змогу запустити повноцінну програму національних Bug Bounty, щоб тестувати інформаційні системи на вразливості, вчасно виявляти ризики і підвищувати захищеність систем.
Процедура Bug Bounty широко застосовується у всьому світі. Проте в Україні проведення Bug Bounty для державних систем було неприйнятним. Наразі ми запроваджуємо застосування сучасних інструментів для перевірки та захисту.
Запуск програм Bug Bounty дозволить:

- підвищити рівень кіберзахисту інформаційних систем;
- протидіяти несанкціонованому доступу до інформаційних систем;
- підвищити кіберстійкість інформаційних систем до інцидентів.

З МЕТОЮ ЗНИЖЕННЯ РИЗИКІВ ШАХРАЙСТВА НАДАВАЧІ ПЛАТІЖНИХ ПОСЛУГ ЗАСТОСОВУВАТИМУТЬ ПОСИЛЕНУ АВТЕНТИФІКАЦІЮ

Нацбанк з метою зниження ризиків шахрайства встановив до надавачів платіжних послуг вимогу застосувати посилену автентифікацію користувачів. Таке рішення зумовлене необхідністю реалізації Закону України «Про платіжні послуги» та гармонізації українського законодавства у сфері надання платіжних послуг із законодавством Європейського Союзу. Так, надавачі платіжних послуг зобов'язані застосовувати посилену автентифікацію користувачів під час:

- отримання ними дистанційного доступу до рахунків;
- ініціювання дистанційної платіжної операції;
- будь-яких інших дій у разі підозри вчинення шахрайства чи інших неправомірних дій (або існування такого ризику).

За результатами процедури посиленої автентифікації користувача надавач платіжної послуги має створити унікальний код автентифікації, який дає змогу пов'язувати операцію на певну суму і конкретного отримувача. Цей код повинен прийматися надавачем платіжних послуг щоразу під час отримання користувачем доступу до рахунку, ініціювання дистанційної платіжної операції тощо.
Такі норми містить постанова Правління Національного банку України від 03 травня 2023 року № 58 "Про затвердження Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку". Її вимоги поширюються на всіх надавачів платіжних послуг.

ПОСИЛЮЄМО КІБЕРСТІЙКІСТЬ ФІНАНСОВОЇ СИСТЕМИ: НКЦК РОЗПОЧАВ НАВЧАННЯ «УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ» ДЛЯ ФАХІВЦІВ БАНКІВСЬКОГО СЕКТОРУ УКРАЇНИ

Національний координаційний центр кібербезпеки спільно з Центром кіберзахисту Нацбанку за підтримки CRDF Global в Україні 15 травня 2023 року розпочав навчання «Управління вразливостями» (VDP) для представників банківського сектору. В одинадцятій програмі із серії «Управління вразливостями» беруть участь понад 30 профільних технічних спеціалістів з близько 30 банків та Нацбанку.
«Програма «Управління вразливостями» вже вдруге проводиться для банківського сектору України, адже під час повномасштабного вторгнення рф в Україну наш банківський сектор піддається постійним атакам російських хакерів. Під час навчання найкращі українські тренери нададуть фахівцям теоретичні та практичні знання за п'ятьма напрямками кібербезпеки. Учасники зможуть підвищити свій кваліфікаційний рівень та вдосконалити навички у сфері забезпечення кібербезпеки інформаційних систем», – зазначила керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Наталія Ткачук, відкриваючи захід.
Навчальний курс VDP триватиме шість тижнів. Під час навчання спеціалісти з кібербезпеки ознайомляться з актуальними викликами та загрозами у сфері захисту критичної інфраструктури банківської системи.

НКЦК ПРОВІВ ДВОДЕННИЙ ТРЕНІНГ З КІБЕРБЕЗПЕКИ ТА КІБЕРРОЗВІДКИ ДЛЯ ФАХІВЦІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ

Національний координаційний центр кібербезпеки за підтримки CRDF Global в Україні та Держдепартаменту США 15-16 травня 2023 року провів дводенний тренінг з кібербезпеки та кіберрозвідки для фахівців сектору безпеки і оборони на тему: «Інструменти, послуги та розвідка загроз у сфері кібербезпеки».
У заході взяли участь понад 20 представників Збройних Сил України та Міністерства оборони України. Навчання проводили експерти організації з кібербезпеки Internet 2.0 згідно з нещодавно підписаним меморандумом про співпрацю.
Учасники тренінгу опанували новітні технології у сфері кібербезпеки, включаючи виявлення та реагування на загрози, сканування вразливостей та аналіз трафіку, збір розвідданих та аналіз документів. Також фахівці перевірили набуті навички, виконавши ряд завдань.

ЗА СПРИЯННЯ НКЦК В ОБ'ЄДНАНОМУ ЦЕНТРІ ПЕРЕДОВИХ ТЕХНОЛОГІЙ З КІБЕРОБОРОНИ НАТО ВІДБУВСЯ ТРЕНІНГ ДЛЯ УКРАЇНСЬКИХ ФАХІВЦІВ У СФЕРІ КІБЕРБЕЗПЕКИ

Об'єднаний центр передових технологій з кібероборони НАТО (CCDCOE) організував тренінг для українських фахівців у сфері кібербезпеки на тему: «Критична інформаційна інфраструктура», який відбувся цього тижня у місті Таллінн. Захід відбувся за підтримки НКЦК та сприяння Консультативної місії Європейського Союзу в Україні (КМЄС).
У навчанні взяли участь фахівці Апарату РНБО України, Ситуаційного центру забезпечення кібербезпеки Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України та Департаменту кібербезпеки Національної поліції України.
Також відбулась робоча зустріч української делегації та представників КМЄС з директором CCDCOE Мартом Ноормою, під час якої було обговорено питання подальшої співпраці у сфері кібербезпеки.

ДЕРЖСПЕЦЗВ'ЯЗКУ ПРОВЕЛА КОНКУРС РАЙТАПІВ ЗА РЕЗУЛЬТАТАМИ ЗМАГАНЬ UA30CTF

Державна служба спеціального зв'язку та захисту інформації України протягом 28–29 квітня провела конкурс райтапів за результатами всеукраїнських онлайн-змагань із кібербезпеки UA30CTF. Переможцем стала команда Knotty Kitten. Тепер, за бажання, команди можуть публікувати свої райтапи на будь-яких платформах.
Райтап – це розповідь у довільному форматі, в якій учасники змагань діляться інформацією про те, як вони успішно впоралися з конкретними завданнями під час CTF.

ВІД ПОЧАТКУ РОКУ ЗРОСЛА КІЛЬКІСТЬ КІБЕРАТАК НА КОМЕРЦІЙНИЙ СЕКТОР: СТАТИСТИКА

Від початку 2023 року Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Держспецзв'язку, в ручному режимі опрацювала понад 700 кіберінцидентів та кібератак: 151 з них сталася протягом квітня.
Урядові організації та місцеві органи влади, за даними CERT- UA, залишаються в центрі уваги ворожих хакерів. Проте протягом березня-квітня експерти також фіксували зростання кількості кібератак на комерційні організації: майже вдвічі порівняно із січнем-лютим 2023 року.
Фішинг залишається улюбленою тактикою російських хакерів. Їхні фішингові кампанії добре сплановані та мають масовий характер. Цей вид атак загрожує не тільки працівникам цільових організацій (держслужбовцям, працівникам підприємств критичної інфраструктури), а й кожному громадянину. За допомогою фішингу російські спецслужби намагаються зібрати про українців усю можливу інформацію, в їхньому фокусі – персональні дані.

ЗЛОВМИСНИКИ ВИКОРИСТОВУЮТЬ ЛЕГІТИМНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ДЕСТРУКТИВНИХ АТАК НА УКРАЇНСЬКІ ДЕРЖОРГАНИ – АНАЛІЗ

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA дослідила кібератаку, імовірно асоційовану з угрупуванням Sandworm. Для виведення з ладу серверного обладнання, автоматизованих робочих місць користувачів та систем зберігання даних зловмисники використали у тому числі легітимне програмне забезпечення.
Отримавши несанкціонований доступ до інформаційно-комунікаційної системи об'єкта атаки, для виведення з ладу ЕОМ, що функціонують під управлінням операційної системи (ОС) Windows, застосовано RoarBat - BAT-скрипт. Скрипт здійснює рекурсивний пошук файлів за визначеним переліком розширень для їх подальшого архівування за допомогою легітимної програми WinRAR з опцією «-df». Ця опція передбачає видалення вихідного файлу та подальше видалення створених архівів. Запуск згаданого скрипту здійснено за допомогою запланованого завдання, яке, за попередньою інформацією, було створено та централізовано розповсюджено засобами групової політики (GPO).
Виведення з ладу ЕОМ під управленням ОС Linux здійснено за допомогою BASH-скрипта, що, серед іншого, забезпечував використанням штатної утиліти «dd» для перезапису файлів нульовими байтами.
CERT-UA зазначає, що реалізації зловмисного задуму в цій та подібних атаках сприяють відсутність багатофакторної автентифікації при здійсненні віддалених підключень до VPN, а також відсутність сегментації мережі та фільтрації вхідних, вихідних та міжсегментних інформаційних потоків. Загальна інформація щодо атаки та індикатори кіберзагроз доступні за посиланням: https://cert.gov.ua/article/4501891

ДЕРЖСПЕЦЗВ'ЯЗКУ ПРОВЕЛА ДРУГІ НАВЧАННЯ ІЗ КІБЕРЗАХИСТУ ДЛЯ ДЕРЖСЛУЖБОВЦІВ КАТЕГОРІЇ «А»

З метою підвищити знання представників державного сектору у сфері кіберзахисту та надати практичні навички, які допоможуть інституціям бути ефективними у побудові та управлінні кіберзахистом, Держспецзв'язку вдруге провела освітній курс для держслужбовців категорії «А».
Програма освітнього курсу орієнтована на керівників, які мають стати лідерами змін у своїх установах у галузі кіберзахисту. Знаннями зі службовцями ділилися провідні українські фахівці: представники суб'єктів кібербезпеки України – Держспецзв'язку, СБУ, Кіберполіції, а також Національного координаційного центру кібербезпеки при РНБО України, фахівці Урядової команди реагування на комп'ютерні надзвичайні події CERT-UA, Державного центру кіберзахисту і фахівці з кібербезпеки із бізнесу, які були залучені до взаємодії в межах державно-приватного партнерства.
«Сьогодні весь світ об'єднує зусилля для протидії російській агресії у кіберпросторі. Так само важливо, щоб ми об'єднували зусилля всередині країни: ділилися знаннями та експертизою, взаємодіяли під час протидії кіберзагрозам. Такі освітні програми допомагають експертам із кібербезпеки та кіберзахисту країни поширювати найкращі практики тоді, коли країна цього найбільше потребує, і будувати мости для взаємодії в забезпеченні кіберзахисту держави», – підкреслив заступник Голови Держспецзв'язку Олександр Потій.

СБУ ЛІКВІДУВАЛА ПОТУЖНИЙ ПРОКСІ-ЦЕНТР У ПОЛТАВІ, ЧЕРЕЗ ЯКИЙ РФ ПРОВОДИЛА СПЕЦІАЛЬНІ ІНФОРМАЦІЙНІ ОПЕРАЦІЇ В ІНТЕРНЕТІ

Кіберфахівці Служби безпеки спільно з БЕБ заблокували у Полтаві потужний проксі-центр, який агресор використовував для підривної діяльності проти України. У результаті комплексних заходів затримано організаторів незаконної діяльності. Ними виявились двоє мешканців Полтавської та Харківської областей.
Ділки налагодили підпільний проксі-центр, який працював як VPN-сервіс. Він дозволяв абонентам з будь-якої країни видавати себе за користувачів українського мобільного Інтернету. Вартість такої «підписки» становила майже 2,5 тис. грн на місяць. За оперативною інформацією, фігуранти щодня отримували сотні «замовлень», а гроші одержували через заборонені платіжні системи.
Серед «постійних» клієнтів були громадяни рф, які через послуги проксі-центру намагалися приховати власні IP-адреси для доступу до популярних соцмереж. При цьому сервери ворожого «осередку» знаходились на території країни-агресора. Це дозволяло російським спецслужбам отримувати віддалений доступ до українського інтернет-простору, а також поширювати кремлівські наративи та фейкову інформацію про ситуацію на фронті нібито від імені українських громадян.
Тривають слідчі дії для встановлення всіх обставин злочину і притягнення винних до відповідальності.

КІБЕРПОЛІЦЕЙСЬКІ ВИКРИЛИ ЖИТЕЛЯ ЧЕРНІВЦІВ У РОЗРОБЦІ ТА ЗБУТІ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Фігурант розробив програму для віддаленого керування даними на серверах потерпілих. Свою розробку він продавав на форумах і надалі з її використанням хакери здійснювали атаки на різні компанії та установи. Підозрюваному може загрожувати до п'яти років позбавлення волі.
Чоловік розробив програму за типом Obfuscated Web Backdoor для шифрування програмного коду та модифіковане шкідливе забезпечення для віддаленого контролю над вебресурсами. Таким чином розробка фігуранта дозволяла приховати шкідливе програмне забезпечення на ураженому ресурсі та залишати контроль над ним непомітним для власника. Шкідливу програму він продавав на тематичних форумах. Надалі розробку використовували інші хакери для атак іноземних кампаній та подальшого скоєння кіберзлочинів.
Паралельно фігурант застосовував іншу програму, яка штучно підвищувала рейтинг та пошукову видачу вебсторінки в обхід правил використання та просування вебресурсів пошукових систем.

СБУ ЛІКВІДУВАЛА МЕРЕЖУ БОТОФЕРМ З АУДИТОРІЄЮ МАЙЖЕ 200 ТИСЯЧ КОРИСТУВАЧІВ: ПРАЦЮВАЛИ НА РОЗХИТУВАННЯ ОБСТАНОВКИ В УКРАЇНІ

Кіберфахівці Служби безпеки викрили міжрегіональну мережу ботоферм, які поширювали дезінформацію для розхитування суспільно-політичної ситуації в Україні. Насамперед зловмисники намагались дискредитувати діяльність вищого військово-політичного керівництва нашої держави в умовах війни. Також вони розповсюджували хибні повідомлення про теракти в українських містах та «мінування» об'єктів з масовим скупченням людей.
Для «розгону» фейків створили анонімні акаунти у соцмережах Фейсбук, Інстаграм і Твіттер із загальною аудиторією у майже 200 тис. користувачів. У результаті багатоетапної спецоперації у різних регіонах України знешкоджено 9 ботоферм і викрито їхніх організаторів. Апаратно-програмні комплекси для «вирощування» ботів фігуранти встановили у власних помешканнях або в офісних приміщеннях.
Триває розслідування для встановлення всіх обставин злочину і притягнення винних до відповідальності.

НАЦПОЛІЦІЯ СПІЛЬНО З ФБР ЛІКВІДУВАЛА МЕРЕЖУ СЕРВІСІВ ДЛЯ ОБМІНУ КРИПТОВАЛЮТИ, ЗДОБУТОЇ ЗЛОЧИННИМ ШЛЯХОМ

Сервіси надавали можливість кіберзлочинцям легалізувати активи, здобуті як «викупи» від атак вірусами-шифрувальниками. Ліквідували мережу в ході міжнародної поліцейської операції.
Працівники Департаменту кіберполіції спільно з Головним слідчим управлінням Нацполіції, Офісом Генерального прокурора України та у співпраці з ФБР Сполучених штатів Америки провели багаторівневу міжнародну операцію з ліквідації дев'яти сервісів обміну віртуальних активів.
Вебресурси пропонували користувачам анонімний обмін криптовалют. Такі послуги надавалися для сприяння легалізації та відмивання грошей, здобутих протиправним шляхом. Через біржі зловмисники проводили активи, отримані в результаті атак шкідливим програмним забезпеченням та онлайн-шахрайства. Рекламування послуг з обміну здійснювалося на закритих хакерських форумах.
За результатами операції правоохоронці заблокували інфраструктуру мережі, котра розміщувалася на серверах Сполучених Штатів Америки, країнах Європи та в Україні. Доменні імена вилучено. Наразі працівники поліції встановлюють причетних до злочинної діяльності.

СБУ ЗАТРИМАЛА У КИЄВІ ДВОХ «ПРИВАТНИХ ДЕТЕКТИВІВ», ЯКІ ТОРГУВАЛИ КОНФІДЕНЦІЙНОЮ ІНФОРМАЦІЄЮ ІЗ ДЕРЖАВНИХ БАЗ ДАНИХ

Кіберфахівці Служби безпеки нейтралізували у Києві злочинну діяльність приватного детективного агентства, яке продавало інформацію із закритих баз даних держаних установ. Незаконну діяльність організував колишній слідчий одного зі столичних райвідділів міліції, який відмовився проходити атестацію у лави поліції й у 2015 році звільнився з правоохоронного органу. Згодом він спільно зі своїм знайомим створив приватне детективне агентство.
Під виглядом легального бізнесу вони збирали для своїх клієнтів конфіденційну інформацію про інших громадян, у тому числі діставали дані, які зберігаються у державних реєстрах. Для цього «в темну» використовували власні «старі» зв'язки серед чиновників та представників правоохоронних органів. Вартість «досьє» на одну людину сягала від 800 до 2,6 тис. дол. Сума залежала від обсягу персональних даних і терміновості «замовлення».
Так, наприклад, до «розгорнутих анкет» окрім паспортних даних громадян входила інформація про номери їхніх телефонів і автомобілів, а також відомості про перетин кордону та вчинення адмінправопорушень.
Тривають слідчі дії для притягнення до відповідальності всіх осіб, причетних до злочину. Також перевіряється інформація щодо можливого продажу конфіденційної інформації до рф.

НАЦПОЛІЦІЯ ЛІКВІДУВАЛА МАСШТАБНУ ШАХРАЙСЬКУ СХЕМУ: ЇЇ УЧАСНИКИ ПРИВЛАСНИЛИ ГРОШІ З РАХУНКІВ ПОНАД 10 ТИСЯЧ ГРОМАДЯН

Для припинення розгалуженої злочинної мережі та проведення слідчих дій у 20 регіонах держави проведено спецоперацію, у якій брали участь понад 500 співробітників Національної поліції. У результаті викрили 56 зловмисників: вони розсилали фішингові посилання для отримання даних про банківські картки громадян. У такий спосіб фігуранти отримали доступ до рахунків, із яких привласнили близько 15 мільйонів гривень.
Під час розслідування поліцейські встановили 11 спільнот: зловмисники об'єднувалися на закритих тематичних каналах і форумах. Адміністратори таких спільнот розміщували оголошення з приводу «підробітку»: охочі мали створювати і розсилати фішингові посилання, які дуже схожі на посилання офіційних ресурсів, для отримання даних банківських карток громадян. Фішинг маскували різними способами: від пропозицій оформлення грошових виплат до продажу різних товарів, здебільшого - побутової техніки.
За попередніми даними, від протиправної діяльності постраждали понад 10 тисяч громадян. На цей час відомо, що фігуранти привласнили 15 мільйонів гривень, однак остаточна сума збитків буде встановлена під час розслідування.
Працівники поліції ідентифікували 56 причетних до шахрайства осіб, а відтак провели обшуки за місцями проживання фігурантів у 20 областях України.
Слідчі розслідують кримінальні провадження за ч. 3, 4 ст. 190 (Шахрайство) Кримінального кодексу України. Готуються матеріали для оголошення підозри зловмисникам.

У ЛЬВОВІ ПРАВООХОРОНЦІ ВИКРИЛИ ЗЛОЧИННУ ОРГАНІЗАЦІЮ, УЧАСНИКИ ЯКОЇ ПРИВЛАСНИЛИ БЛИЗЬКО 6 МЛН ГРИВЕНЬ ЗА ДОПОМОГОЮ ФІШИНГУ

Зловмисники створювали та розсилали фішингові посилання під виглядом оформлення соціальних виплат. У такий спосіб вони отримали доступ до рахунків понад 1500 осіб і надалі привласнили їхні гроші. Фігурантів затримано, їм повідомлено про підозру.
Зловмисники розсилали фішингові посилання через соціальні мережі та месенджери під приводом оформлення грошової допомоги від Президента України, ООН, UNICEF та інших організацій. Інтерфейс шахрайських сайтів був подібним до офіційних урядових ресурсів і сайтів банківських установ.
За попередніми даними, учасники угруповання отримали доступ до онлайн-банкінгу близько 1500 осіб. Загальна сума збитків становить 6 мільйонів гривень.
Слідчі оголосили фігурантам підозри у вчинені шахрайства, створені та участі у злочинній організації – ч. 4 ст. 190, ч. 1, 2 ст. 255. Також трьом учасникам групи оголошено підозри за фактом несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж – ч. 5 ст. 361 Кримінального кодексу України.

ЗЛОВМИСНИКИ РОЗПОЧАЛИ ЧЕРГОВУ КАМПАНІЮ АТАК ІЗ ВИКОРИСТАННЯМ ЕЛЕКТРОННИХ ЛИСТІВ НА ТЕМУ «РАХУНКІВ» – АНАЛІЗ

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA виявила та дослідила факт чергової кампанії з розповсюдження хакерським угрупуванням UAC-0006 електронних листів на тему «рахунків». Зловмисники розсилають листи з вкладенням у вигляді ZIP або RAR-архіву, що містить шкідливу програму SmokeLoader. Для надсилання застосовують легітимні скомпрометовані електронні поштові скриньки.
У CERT-UA відзначають низку змін у тактиках, техніках і процедурах UAC-0006:

- використання кількох ланцюгів ураження;
- розповсюджуваний зразок SmokeLoader містить 26 URL-адрес сервера управління бот-мережею (переважна більшість доменів не зареєстрована);
- виявлення шкідливої програми Cobalt Strike Beacon може свідчити про розширення переліку використовуваного угрупуванням інструментарію.

Для реєстрації доменних імен та розміщення серверів управління бот-мережею зловмисники використовують російських реєстраторів доменних імен та провайдерів: @reg.ru, @nic.ru, @iqhost.ru, @macloud.ru, @cloudx.ru, які сприяють реалізації зловмисного задуму. Як нагадують у CERT-UA, для запуску JavaScript-завантажувача, який забезпечує доставлення і запуск SmokeLoader, використовується Windows Script Host (wscript.exe, cscript.exe); у зв'язку з чим, з метою зменшення поверхні атаки, рекомендується обмежити можливість використання цієї технології на ЕОМ. Загальна інформація щодо атаки та індикатори кіберзагроз доступні за посиланням: https://cert.gov.ua/article/4555802

8. ПЕРША СВІТОВА КІБЕРВІЙНА

ОБМЕЖЕННЯ ЗДАТНОСТІ РОСІЇ ПІДТРИМУВАТИ СВОЇ ВІЙСЬКОВІ АМБІЦІЇ В УКРАЇНІ МАЄ БУТИ ОДНИМ ІЗ ЗАВДАНЬ ТРАНСАТЛАНТИЧНОГО ПАРТНЕРСТВА – ДОСЛІДЖЕННЯ BELFER CENTER

У травні 2023 року експерти Belfer Center for Science and International Affairs, Harvard Kennedy School опублікували дослідження «Відповідь на російські та китайські кіберзагрози». У дослідженні всебічно розглядається ситуація із кіберзагрозами для трансатлантичної спільноти і виходить з двох ключових викликів перед яким постають демократичні держави: необхідність стримування можливостей росії у досягненні їх цілей в Україні та необхідність захисту партнерів по спільності від китайської кіберактивності.
Серед рекомендацій звіту є заклик до ЄС та США створити міжнародний орган під егідою Бюро кіберпростору та цифрової політики Державного департаменту США для посилення підтримки України. З іншого боку, українському уряду рекомендується краще координувати хактивістів, вказуючи на неприпустимість проведення контратак.

КІБЕРУРОКИ УКРАЇНИ: ГОТУЙТЕСЯ ДО ТРИВАЛОГО КОНФЛІКТУ, А НЕ ДО НОКАУТУ ОДНИМ УДАРОМ

У статті Breaking Defense опублікованій 1 травня Сідні Фрідберг молодший (Sydney Freedberg Jr.) стверджує, що широко поширений страх перед «кібер-11 вересня» або «кібер-Перл-Харбором», тобто рішучою, паралізуючою, блискавичною атакою в кіберпросторі, виявився необґрунтованим.
«Кілька незалежних експертів заявили, що стратегічний урок для США полягає в тому, що тривалий кіберконфлікт є більш вірогідною моделлю для майбутніх війн, ніж раптова смерть на кшталт «кібер-Перл-Харбор» або «кібер 9/11», прогнозована офіційними особами США більше десятиліття». Хоча кібероперації були і, ймовірно, залишатимуться важливою частиною майбутніх війн, вони навряд чи стануть вирішальними для перемоги у війнах, а також не принесуть значних переваг на оперативному рівні.

САЙТИ МЕРІЙ НИЗКИ МІСТ У ФРАНЦІЇ ЗАЗНАЛИ ПРОРОСІЙСЬКИХ КІБЕРАТАК

4 травня «Європейська правда» цитувала французьке Le Figaro про те, що напередодні сайти мерій багатьох міст Франції зазнали кібератак, з'явилися проросійські повідомлення. Постраждали щонайменше 30 міст по всій країні. Серед атакованих сайтів – сайт мерії міста Брі-сюр-Марн (департамент Валь-де-Марн), на якому з'явилася порожня сторінка з написом: «Поважайте росію! Інакше ми продовжимо воювати з вами». На момент публікації не було відомо, хто стоїть за атакою.

САЙТ СЕНАТУ ФРАНЦІЇ АТАКУВАЛИ РОСІЙСЬКІ ХАКЕРИ

Укрінформ із посиланням на The Guardian повідомив 5 травня, що російські хакери відключили сайт французького сенату. Угрупування NoName взяло на себе відповідальність за атаку, заявивши в Telegram, що причиною атаки стало те, що «Франція працює з Україною над новим пакетом допомоги, який може включати зброю».

РОСІЯ АТАКУЄ ЦИВІЛЬНУ ІНФРАСТРУКТУРУ В КІБЕРПРОСТОРІ ТАК САМО, ЯК І НА ЗЕМЛІ – CERT-UA

Речник Держспецзв'язку Володимир Кондрашов повідомив, що урядова група реагування на надзвичайні ситуації в кіберпросторі CERT-UA відстежує діяльність понад 80 хакерських угруповань, більшість з яких походять з російської федерації, а 90% їхніх членів – російські військові. Він наголосив, що в кіберпросторі рф використовує ту ж тактику, що й на звичайному полі бою, тобто намагається атакувати цивільну інфраструктуру.

ЩОБ ОТРИМАТИ ГРОШІ ТА УВАГУ: KILLNET, ОЧЕВИДНО, ЗНОВУ РЕОРГАНІЗУЄТЬСЯ

У звіті, опублікованому 4 травня, кібербезпекова компанія Flashpoint заявила, що російська хакерська група KillNet продовжує розвиватись. Flashpoint повідомляє, що група все ще прагне отримати прибуток: «Flashpoint неодноразово зазначав, що попри всі свої націоналістичні витівки, Killnet залишається переважно фінансово вмотивованою групою, яка користується перевагами російської прокремлівської медіа-екосистеми для просування своїх DDoS-сервісів за наймом. Killnet співпрацює з кількома власниками ботнетів і партнерським угрупованням Deanon Club, з метою таргетування ринків даркнету, орієнтованих на наркотики».
KillNet не продемонструвала значного зростання складності чи ефективності методів, які вона використовувала, така залежність від простих інструментів викликала глузування з боку інших гравців кібер underground. «Killnet все ще дуже висміюють на провідних російськомовних форумах», – пише Flashpoint.

CERT-UA ПОПЕРЕДЖАЄ ПРО АТАКИ ШКІДЛИВИХ ПРОГРАМ SMOKELOADER І ROARBAT НА УКРАЇНУ

Як 8 травня повідомило The Hacker News, за даними CERT-UA, в Україні триває фішингова кампанія з використанням приманок, пов'язаних із рахунками. Вона використовується для розповсюдження зловмисного програмного забезпечення SmokeLoader у вигляді багатомовного файлу.
За даними агентства, електронні листи були надіслані з використанням скомпрометованих облікових записів і мають у додатку ZIP-архів, який насправді є багатомовним файлом, що містить документ-приманку та файл JavaScript.
Потім код JavaScript використовується для запуску виконуваного файлу, який прокладає шлях для виконання зловмисного ПЗ SmokeLoader. SmokeLoader, вперше виявлений у 2011 році, є завантажувачем, основною метою якого є завантаження даних або встановлення більш прихованого чи ефективнішого шкідливого програмного забезпечення в заражені системи.
CERT-UA приписує цю діяльність зловмиснику під назвою UAC-0006 і описує її як фінансово мотивовану операцію, спрямовану на викрадення облікових даних і здійснення несанкціонованих грошових переказів.

ПОВ'ЯЗАНЕ З КРЕМЛЕМ ШПИГУНСЬКЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ SNAKE ЛІКВІДОВАНО – МІН'ЮСТ США

9 травня американські та міжнародні правоохоронні органи оголосили, що вони успішно видалили імплантат шкідливого програмного забезпечення під назвою Snake, яке протягом двох десятиліть використовувалося відомою хакерською групою Turla, пов'язаною з російським фсб.
«Ми вважаємо, що це їхній основний інструмент шпигунства», – сказав високопоставлений чиновник ФБР журналістам, зазначивши, що його використовували проти НАТО та інших країн для викрадення конфіденційної інформації
Керівник Mandiant Intelligence Analysis у Google Cloud Джон Хултквіст вважає, що збій у роботі хакерів Turla буде тимчасовим. Водночас він наголосив, що важливо послабити розвідувальні можливості під час війни, особливо, коли він приймає рішення щодо можливого відступу.

КОРПОРАЦІЯ MICROSOFT ВИПУСТИЛА НОВИЙ ПАТЧ ДЛЯ ВИПРАВЛЕНОЇ ПРОБЛЕМИ З OUTLOOK, ЯКУ ВИКОРИСТОВУВАЛИ РОСІЙСЬКІ ХАКЕРИ

10 травня Microsoft випустила новий патч для вразливості в Outlook, яку спочатку виправили в березні, але пізніше з'ясувалося, що вона містила уразливість, якою могли скористатись російські хакери для атак на європейські урядові, транспортні, енергетичні та військові організації.
Про вразливість Microsoft повідомили представники української команди реагування CERT-UA, але пізніше дослідники Akamai знайшли спосіб обійти виправлення, дозволяючи зловмисникам використовувати вразливість, щоб змусити клієнт Outlook під'єднатись до сервера, контрольованого зловмисником. Це називається експлойтом без кліків(zero-click vulnerability).

РОЗВИТОК КІБЕРОПЕРАЦІЙ ТА МОЖЛИВОСТЕЙ – ДОПОВІДЬ CSIS

18 травня експерти Center for Strategic and International Studies (CSIS) опублікували звіт про досвід України у протидії російській кіберагресії. Дослідження зосереджується на факторах, які допомогли Україні ефективно боротися з російськими кіберзусиллями, а також висвітлює кілька висновків, які західний світ повинен зробити з цього протистояння.
Одним із ключових висновків є те, що Україна успішно продемонструвала концепцію кіберстійкості. Крім того, вирішальним є побудова міцних відносин із союзниками та партнерами для обміну розвідданими, технологіями та тактикою. Залучення ресурсів і підтримки приватного сектору та громадянського суспільства також забезпечує унікальні переваги.
Однак експерти застерігають не покладатися виключно на досвід України, оскільки не можна гарантувати, що ворожі хакери в інших конфліктах будуть такими ж некомпетентними та непідготовленими, як у цій кібервійні. При цьому український кейс спровокував ширшу дискусію щодо застосовуваності норм міжнародного права стосовно кіберконфліктів.

CERT-UA ІДЕНТИФІКУЄ ЙМОВІРНУ КАМПАНІЮ РОСІЙСЬКОГО КІБЕРШПИГУНСТВА

22 травня CERT-UA повідомив, що російським кібершпигунам, ймовірно, вдалося скомпрометувати облікові записи посольства Таджикистану. Зловмисники, яких в Україні відстежують як UAC-0063, використовували ці облікові записи у фішинговій кампанії, призначеній для встановлення кейлоггерів (LOGPIE), бекдорів (CHERRYSPY) і викрадачів файлів (STILLARCH або DownEx) на цільових пристроях.
«Встановлено, що 18 квітня 2023 року та 20 квітня 2023 року, – пише CERT-UA, – на електронну адресу відомства надсилалися електронні листи, ймовірно, з офіційної скриньки посольства Таджикистану в Україні (ймовірно, внаслідок злому останнього), перший містив вкладення у вигляді документа з макросом, а другий – посилання на той самий документ». За даними CERT-UA, кампанія торкнулася не лише цілей в Україні, а й організацій в Монголії, Казахстані, Киргизстані, Ізраїлі та Індії. Bank Info Security пише, що ця кампанія має певну схожість з минулими операціями російського гру Fancy Bear.

ІРЛАНДІЯ РОЗГЛЯДАЄ КІБЕРДОПОМОГУ УКРАЇНІ ЯК ВНЕСОК У КОЛЕКТИВНУ БЕЗПЕКУ

23 травня Irish Times повідомило, що Ірландія надає Україні «значну» підтримку в галузі кібербезпеки під час війни з росією. Дублін розглядає цю допомогу як внесок у колективну безпеку.

9. РІЗНЕ

ЄС І США ПОПЕРЕДЖАЮТЬ МАЛАЙЗІЮ ПРО ЗАГРОЗУ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ ВІД ЗАЯВКИ HUAWEI НА УЧАСТЬ У РОЗБУДОВІ 5G – FT

2 травня видання US News з посиланням на Financial Times повідомило, що Європейський Союз і США попередили Малайзію про ризики для національної безпеки та іноземних інвестицій, оскільки вона завершує перевірку розгортання 5G, що дозволяє китайській Huawei Technologies Co Ltd подати заявку на участь у розбудові її телекомунікаційної інфраструктури.
Представники ЄС і США в Малайзії надіслали листа уряду у квітні після того, як він вирішив переглянути рішення про присудження Ericsson тендер на 11 мільярдів ринггітів (2,5 мільярда доларів) на будівництво державної мережі 5G. До того уряд Малайзії ігнорував попередження США про загрози національній безпеці.

ДОСЛІДНИКИ КАЖУТЬ, ЩО ВОНИ ВПЕРШЕ ЗНАЙШЛИ ШПИГУНСЬКЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ЯКЕ ВИКОРИСТОВУЄТЬСЯ НА ВІЙНІ

25 травня TechCrunch повідомив, що дослідники з питань безпеки та організації, що займаються цифровими правами, вважають, що уряд Азербайджану використав шпигунське програмне забезпечення, створене NSO Group, для нападу на урядовця, журналістів, активістів та уповноваженого з прав людини у Вірменії в рамках конфлікту в Нагорному Карабаху.
Кібератака може бути першими відомим випадком використання комерційного шпигунського програмного забезпечення у військових діях – повідомляє організація, що займається питаннями цифрових прав Access Now, яка розслідувала деякі випадки.