НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

УКРАЇНСЬКА ФУНДАЦІЯ БЕЗПЕКОВИХ СТУДІЙ

CYBER DIGEST

Огляд подій в сфері кібербезпеки,
вересень 2024

Ця публікація стала можливою завдяки підтримці, наданій Агентством США з міжнародного розвитку, згідно з умовами гранту Української фундації безпекових студій в рамках Проєкту USAID "Кібербезпека критично важливої інфраструктури України".

ЗМІСТ

ОСНОВНІ ТЕНДЕНЦІЇ

США продовжують обмежувати вплив Китаю та росії на свої інформаційні системи й протидіяти кібершпигунству. У вересні були прийняті рішення та розпочаті обговорення, які можуть суттєво вплинути на кібербезпеку в країні. Зокрема, це стосується обмеження використання кранів китайського виробництва у портах і китайських та російських технологій в автомобілях. Паралельно, зростають зусилля з підвищення власної кібербезпеки: запускається грантова програма для індіанських поселень, вводиться модель кіберзрілості CMMC 2.0 для військових підрядників, оновлюються вимоги до кібербезпеки для федеральних установ тощо. Однак, рівень готовності залишається недостатнім. Багато експертів вказують, що Міністерство сільського господарства США (USDA) ще не готове захищати харчовий і сільськогосподарський сектори від кібератак, попри зростання цифрових загроз.

Кібербезпека президентських виборів у США є головний пріоритет для відповідних органів. Китай, Іран і росія посилюють тиск на виборчий процес, поширюючи дезінформацію, фейкові новини та підбурюючи до радикалізму. За даними Microsoft, найбільш активним у втручанні є Китай. Іран і росія також продовжують свої традиційні дії, але цього разу іранські хакери були особливо активні, проводячи довготривалі операції з викрадення даних учасників виборів, атакуючи кампанію Дональда Трампа і намагаючись поширити викрадену інформацію. У відповідь на це Міністерство юстиції США висунуло звинувачення трьом іранцям. Крім того, Агенція з кібербезпеки та інфраструктурної безпеки (CISA) контролює безпеку виборів на всіх етапах, надаючи консультації та розповсюджуючи рекомендації для забезпечення кібер- і фізичної безпеки.

У вересні сталось одразу декілька помітних кіберінцидентів пов'язаних з витоками даних. Зокрема, були розкриті особисті дані всіх нідерландських поліцейських. Кібербезпекова компанія Proton виявила на DarkWeb персональні дані близько 3000 співробітників Конгресу США, а Microchip Technology підтвердила викрадення інформації під час атаки з використанням програм-вимагачів. Хоча ці інциденти зачепили багатьох людей, реакції компаній на такі ситуації різняться. Наприклад, Федеральна комісія зв'язку США (FCC) змусила T-Mobile витратити 31,5 мільйона доларів на покращення кібербезпеки після систематичних витоків даних протягом трьох років. Водночас індійська компанія Star Health подала до суду на Telegram за те, що платформа не протидіяла спробам поширення викрадених даних її клієнтів.

Попри те, що світ обговорює майбутнє кібербезпеки з фокусом на штучному інтелекті та квантових технологіях, експерти також наголошують на іншій важливій проблемі – використанні застарілих технологій як у державному, так і в приватному секторах. Корпорація MITRE підготувала документ, в якому звертає увагу на те, що деякі федеральні системи, яким понад 60 років, все ще використовуються, що є небезпечним у довгостроковій перспективі, оскільки фахівців, які можуть їх обслуговувати, стає дедалі менше. Експерти SANS Institute також вказують на цю проблему, зазначаючи, що експлуатація застарілих систем на застарілих мовах програмування входить до п'ятірки найбільших загроз для кібербезпеки в майбутньому.

Об'єкти критичної інфраструктури залишаються головною мішенню для хакерів. Хоча їхні зусилля спрямовані на доступ до операційних технологій (OT), підтверджених успішних атак поки що небагато. Наприклад, хакерська група Red Devil з Ізраїлю заявила про кібератаку на OT інфраструктуру в Лівані, але багато експертів сумніваються в правдивості цієї інформації. Хакери продовжують атакувати IT-інфраструктуру організацій традиційними методами, такими як фішинг (у 2023 році 80% об'єктів критичної інфраструктури зіштовхнулися з цією проблемою) і атаки програмами-вимагачами (зокрема, у вересні було атаковано одну із систем водопостачання). Кіберфахівці регулярно наголошують на вразливостях у промислових системах, але реальних кроків для їх усунення все ще небагато. Наприклад, Bitsight виявив щонайменше 7 критичних вразливостей у системах автоматичного вимірювання (ATG), які використовуються в великих резервуарах, що дозволяють отримати повний доступ до адміністрування пристроїв.

Україна продовжує активно розширювати свою мережу міжнародних партнерств. У вересні до IT-коаліції приєдналася Іспанія, ставши 13-м партнером у цій сфері. Японія оголосила про плани допомогти Міністерству оборони України в цифровізації, а Держспецзв'язку України підписала Меморандум про взаєморозуміння з Державною комісією з питань захисту інформації Болгарії. Міжнародна співпраця вже приносить результати: за підтримки партнерів Україна запускає спільні проєкти у сфері кібербезпеки. Це включає інформаційні кампанії з кібергігієни, адаптацію інструментів кібердіагностики (як-от CSET), та впровадження автоматизованих систем для моніторингу реалізації Стратегії кібербезпеки України (CyberTracker). Ці зусилля доповнюються роботою над застосуванням міжнародного гуманітарного права під час війни. Національний координаційний центр кібербезпеки разом із партнерами обговорює такі питання, як статус комбатантів у «кібервійні», міжнародний досвід щодо застосування міжнародного гуманітарного права до проведення кібероперацій, правовий аналіз кібератак, що відбувались під час російсько-української війни тощо.

Україна активно впроваджує нові заходи кібербезпеки. Так, 19 вересня рішенням НКЦК при РНБО України було обмежено використання Telegram в державних органах, військових структурах та на об'єктах критичної інфраструктури. Заплановано створення першого в Україні центру обміну інформацією про кіберзагрози (ISAC) у сфері телекомунікацій, що має допомогти в боротьбі з кібератаками в одному з найбільш вразливих секторів. А також започатковано національну ініціативу щодо сприяння посиленню ролі жінок у кібербезпеці та забезпечення гендерної рівності. Безпекові органи, такі як СБУ та БЕБ, протидіють ворожим ботофермам, які поширюють дезінформацію, а також групам, що використовують платіжні системи для фінансування ворожих агентів. Нещодавно вдалося припинити діяльність однієї з таких груп, яка передала російським агентам десятки мільйонів гривень.

У вересні Держспецзв'язку опублікувала свій черговий звіт «російські кібероперації H1'2024». У ньому йдеться, що в першій половині 2024 року російські хакери зосередили атаки на об'єктах, пов'язаних із військовими операціями та постачальниками критичних послуг, намагаючись якомога довше залишатися непоміченими в системах. Звіт також вказує на нову тенденцію: зловмисники активно використовують месенджери та інші комунікаційні засоби, видаючи себе за знайомих жертви. Вони надсилають шкідливі файли, маскуючи їх під документи або відео, що стосуються військової тематики.

Кіберпростір залишається полем глобального протистояння. В США все більше уваги приділяють загрозам з боку Китаю, які становлять небезпеку для американської інфраструктури. У вересні стало відомо, що китайська хакерська група Salt Typhoon зламала кілька інтернет-провайдерів у США, а на кранах, які працюють в портах, виявили приховані бекдори, встановлені без відома користувачів. Ці питання обговорюються в Конгресі. Китай також займається кібершпигунством. За даними компанії TrendMicro, група TIDRONE проводить атаки проти Тайваню, а для шпигування за армією США та Тайванем китайські хакери створили великий ботнет з IoT-пристроїв. Пекін активно розширює свою діяльність і в Південно-Східній Азії. Інше угруповання, Flax Typhoon, вдалося знешкодити американським правоохоронцям, які конфіскували тисячі скомпрометованих пристроїв під їхнім контролем.

росія продовжує атакувати європейських партнерів України, особливо тих, хто надає допомогу Україні. До цих атак долучаються й білоруські хакери. Латвія повідомила про нову хвилю кібератак на урядові та критично важливі інфраструктурні сайти, а Польща виявила мережу російських і білоруських хакерів, які планували атаки на її мережі. Німецька розвідка звинуватила російське гру в атаках на країни НАТО та ЄС. США також продовжують притягувати російських хакерів до відповідальності, висунувши звинувачення п'яти членам підрозділу 29155 гру та одному цивільному за атаки на Україну на початку 2022 року. У відповідь на загрози, Microsoft відключає російські компанії від своїх хмарних сервісів. Активні дії в кіберпросторі демонструють також північнокорейські хакери, які атакують навіть росію.

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

БІЛИЙ ДІМ НАГОЛОШУЄ НА СКЛАДНІЙ ПРОБЛЕМІ БЕЗПЕКИ МАРШРУТИЗАЦІЇ ІНТЕРНЕТ-ТРАФІКУ

3 вересня Управління кібербезпеки Білого дому опублікувало нові рекомендації для мережевих операторів, щоб посилити захист протоколу прикордонного шлюзу (BGP), який відповідає за маршрутизацію інтернет-трафіку. Це рішення спрямоване на розв'язання давньої проблеми, оскільки BGP не забезпечує достатнього захисту від кіберзагроз, таких як крадіжка криптовалюти та поширення шкідливого програмного забезпечення. Рекомендації передбачають впровадження інфраструктури відкритих ключів ресурсів (RPKI), а також технологій, як-от Route Origin Validation (ROV) і Route Origin Authorization (ROA), для кращого захисту маршрутної інформації. Ці заходи є частиною ширшої ініціативи з підвищення безпеки в Інтернеті, і очікується, що понад 60% федеральних мереж впровадять їх до кінця року.

CISA ПРЕДСТАВИЛА ПЛАН ОПЕРАТИВНОГО УЗГОДЖЕННЯ КІБЕРБЕЗПЕКИ ДЛЯ ФЕДЕРАЛЬНОГО СЕКТОРУ

16 вересня CISA опублікувала План оперативного узгодження кібербезпеки для федерального сектору (FOCAL), щоб надати федеральним відомствам чітке бачення ключових кібербезпекових пріоритетів. План має допомогти їм краще координувати свої зусилля в забезпеченні кібербезпеки, впроваджуючи основні практики. План визначає п'ять пріоритетів: управління активами, управління вразливістю, захищена архітектура, управління ризиками в ланцюгу постачання (C-SCRM) та виявлення і реагування на інциденти.

USCYBERCOM ОПРИЛЮДНИЛО ДОРОЖНЮ КАРТУ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРОПЕРАЦІЯХ

10 вересня заступник директора з питань планування та політики Кіберкомандування США Майкл Кларк представив план інтеграції штучного інтелекту у військові кібероперації. Дорожня карта включає понад 100 заходів у різних напрямках, серед яких зміцнення співпраці з промисловістю та розробка нових технологій на основі ШІ. Ініціативу планують реалізувати поетапно, починаючи з понад 60 пілотних проєктів.

МІНІСТЕРСТВО ОБОРОНИ США ГОТУЄТЬСЯ ДО ВПРОВАДЖЕННЯ CMMC 2.0 ДЛЯ СВОЇХ ПІДРЯДНИКІВ

З першого кварталу 2025 року Міністерство оборони США почне включати вимоги щодо CMMC 2.0 у всі контракти з підрядниками. CMMC 2.0 – це оновлена модель кіберзрілості, розроблена Міноборони на основі стандартів NIST 171 та 172. На відміну від попередньої версії, кількість рівнів зрілості скорочено з 5 до 3, але додано нову вимогу: рівні 2 та 3 повинні бути підтверджені незалежними аудиторами.

США ВИДІЛЯЮТЬ 18,2 МЛН ДОЛАРІВ НА ПОСИЛЕННЯ КІБЕРБЕЗПЕКИ ІНДІАНСЬКИХ СПІЛЬНОТ

11 вересня стало відомо, що уряд США через Міністерство внутрішньої безпеки (DHS) виділив 18,2 мільйона доларів у рамках програми грантів Tribal Cybersecurity для підвищення кібербезпеки серед індіанських племен. Ці кошти будуть використані на оцінку ризиків, впровадження рішень з кібербезпеки, посилення захисту, навчання та підвищення обізнаності. Виділена сума становить близько третини від загального обсягу запитів на покращення кібербезпеки, які DHS отримало від індіанських спільнот з жовтня 2023 року.

ЗАКОНОДАВЦІ США ЗАЯВЛЯЮТЬ, ЩО КИТАЙСЬКІ КРАНИ МОЖУТЬ СТАНОВИТИ ЗАГРОЗУ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ ПОРТІВ

13 вересня Спеціальний комітет з питань Комуністичної партії Китаю та Комітет Палати представників з питань внутрішньої безпеки оприлюднили звіт про залежність США від китайських кранів у морських портах. Звіт зосереджений на компанії Shanghai Zhenhua Heavy Industries (ZPMC), яка забезпечує близько 80% транспортних перевезень та портових кранів, що використовуються в США.

Законодавців турбує, що ZPMC належить компанії, яку Міністерство оборони США вважає «Китайською комуністичною військовою компанією» і яка бере участь у мілітаризації Південнокитайського моря. Крім того, ZPMC виробляє і збирає своє обладнання в Китаї, постачаючи в США готову продукцію.

У відповідь на звіт Американська асоціація портових адміністрацій (AAPA) заявила, що на цей момент немає відомостей про порушення безпеки, пов'язані з портовим обладнанням.

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ ІНДІЇ ПЛАНУЄ ПІДГОТОВКУ П'ЯТИ ТИСЯЧ НОВИХ КІБЕРПОЛІЦЕЙСЬКИХ

11 вересня Міністерство внутрішніх справ Індії оголосило про плани підготувати за п'ять років спеціальний підрозділ з 5000 «кіберкомандос» для боротьби з кіберзлочинністю. Це одна з чотирьох великих ініціатив, які представив міністр Аміт Шах. Інші заходи включають створення Центру боротьби з кібершахрайством (CFMC), платформи Samanvay для координації дій правоохоронних органів і обміну даними, а також національного реєстру підозрюваних у кіберзлочинах, де будуть зберігатися дані про осіб, причетних до кібер- та фінансових шахрайств онлайн.

ВЕЛИКОБРИТАНІЯ ВІДНЕСЛА ЦЕНТРИ ОБРОБКИ ДАНИХ ДО КРИТИЧНОЇ НАЦІОНАЛЬНОЇ ІНФРАСТРУКТУРИ

12 вересня уряд Великої Британії офіційно визнав центри обробки даних частиною «Критичної національної інфраструктури», підкресливши їхню важливість для економіки поряд з енергетикою та водопостачанням. Цей статус дозволяє надавати додаткову державну підтримку під час надзвичайних ситуацій, щоб захистити важливі дані, такі як інформація про здоров'я та фінанси, від кібератак та інших загроз. Цей крок має на меті підвищити довіру до Великої Британії як центру для інвестицій у сферу обробки даних. Уже заплановано інвестиції в розмірі 3,75 мільярда фунтів стерлінгів у найбільший центр обробки даних у Європі, який збудують у Хартфордширі.

США ПЛАНУЮТЬ ЗАБОРОНИТИ КИТАЙСЬКІ ТА РОСІЙСЬКІ АВТОМОБІЛЬНІ ТЕХНОЛОГІЇ

23 вересня Міністерство торгівлі США оголосило про плани заборонити використання технологій підключених транспортних засобів з китайських і російських джерел. Бюро промисловості та безпеки (BIS) заявило, що готує рішення про заборону імпорту і продажу обладнання або програмного забезпечення для систем зв'язку транспортних засобів (VCS) та автоматизованих систем водіння (ADS), якщо вони пов'язані з виробниками з Китаю чи росії. Ці заходи спрямовані на захист від можливого використання таких технологій для шпигунства з боку урядів Китаю та росії.

США ВИСУНУЛИ ЗВИНУВАЧЕННЯ ТРЬОМ ІРАНЦЯМ ЗА КІБЕРАТАКУ НА ПРЕЗИДЕНТСЬКУ КАМПАНІЮ ДОНАЛЬДА ТРАМПА

27 вересня Міністерство юстиції США висунуло звинувачення трьом іранцям у причетності до масштабної хакерської кампанії, під час якої вони, ймовірно, викрали велику кількість даних з президентської кампанії Дональда Трампа 2024 року і передали цю інформацію в ЗМІ. Усі троє звинувачених є членами Корпусу вартових ісламської революції Ірану. Їм також інкримінують злам облікових записів чинних і колишніх урядовців США, журналістів, неурядових організацій та осіб, пов'язаних з політичними кампаніями в країні.

ГУБЕРНАТОР КАЛІФОРНІЇ ПІДПИСАВ ЗАКОНИ, ЩО ЗАБОРОНЯЮТЬ ВИКОРИСТАННЯ ВИБОРЧИХ ДИПФЕЙКІВ, СТВОРЕНИХ ЗА ДОПОМОГОЮ ШІ

18 вересня губернатор Каліфорнії Гевін Ньюсом підписав три законопроєкти, які регулюють використання штучного інтелекту в політичній рекламі напередодні виборів 2024 року. Один з законів забороняє створення та поширення дипфейків, згенерованих штучним інтелектом, які пов'язані з виборами, протягом 120 днів до та 60 днів після дня виборів. Це дозволяє судам зупиняти їх розповсюдження і накладати штрафи.

Інший закон вимагає від виборчих штабів розкривати використання зміненого штучним інтелектом контенту в рекламі, а соціальні мережі повинні видаляти оманливі матеріали, створені за допомогою ШІ.

НОВИЙ УРЯД ПОРТУГАЛІЇ ЗБЕРЕЖЕ ЗАБОРОНУ НА ВИКОРИСТАННЯ КИТАЙСЬКОГО ОБЛАДНАННЯ ДЛЯ МЕРЕЖ 5G

10 вересня стало відомо, що новий уряд Португалії планує зберегти заборону, введену попередньою адміністрацією, щодо використання китайського 5G обладнання телекомунікаційними компаніями у своїх мережах. У травні 2023 року Рада з кібербезпеки Португалії (CSSC) заборонила використання китайського обладнання для високошвидкісних мобільних мереж 5G.

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

10 КРАЇН ОПУБЛІКУВАЛИ СПІЛЬНЕ ДОСЛІДЖЕННЯ ПРО ДІЯЛЬНІСТЬ РОСІЙСЬКИХ ХАКЕРІВ З ВІЙСЬКОВОЇ ЧАСТИНИ 29155 ГРУ

5 вересня десять країн, включаючи українські СБУ та CERT-UA, оприлюднили спільне дослідження про діяльність російських хакерів з в/ч 29155 гру рф. У звіті розкрито конкретні тактики та цілі цієї групи, а також інструменти, які вони використовують для атак на об'єкти критичної інфраструктури в різних країнах. Документ також містить рекомендації для організацій щодо пом'якшення наслідків таких атак.

АВСТРАЛІЯ НАПРАВИЛА ЕКСПЕРТНІ ГРУПИ НА ФІДЖІ ПІСЛЯ АТАК НА ФОРУМ ТИХООКЕАНСЬКИХ ОСТРОВІВ, ЗДІЙСНЕНИХ КИТАЙСЬКИМИ ХАКЕРАМИ

12 вересня ABC News повідомило, що цього року австралійський уряд направив кіберспеціалістів на Фіджі після масштабної кібератаки на мережі Секретаріату Форуму тихоокеанських островів, здійсненої хакерами, пов'язаними з Китаєм. За даними джерел, метою атаки було зібрати інформацію про діяльність Секретаріату.

США РАЗОМ ІЗ ЧОТИРМА СОЮЗНИКАМИ ОПРИЛЮДНИЛИ ПОПЕРЕДЖЕННЯ ПРО ЗАГРОЗИ ВІД КИТАЙСЬКИХ ХАКЕРІВ, СПРЯМОВАНІ НА IOT СИСТЕМИ

18 вересня три безпекові органи США разом із чотирма країнами-союзниками оприлюднили звіт про діяльність китайського хакерського угруповання, яке націлене на злам маршрутизаторів і пристроїв IoT для створення ботнетів. У попередженні міститься інформація про інфраструктуру ботнету, країни з розташованими скомпрометованими пристроями, а також рекомендації щодо захисту та усунення цієї загрози.

ПІВДЕННА КОРЕЯ ПРОВЕЛА ТТХ ЗА СЦЕНАРІЄМ МОЖЛИВОГО МІЖДЕРЖАВНОГО КОНФЛІКТУ В ІНДО-ТИХООКЕАНСЬКОМУ РЕГІОНІ

10-12 вересня у Південній Кореї відбулися навчання APEX 2024, організовані Національною розвідувальною службою Республіки Корея спільно з Науково-дослідним інститутом національної безпеки, Міністерством національної оборони (Командуванням кібероперацій), Міністерством науки та ІКТ, Інститутом фінансової безпеки, Інститутом стратегії національної безпеки та Центром передового досвіду спільного кіберзахисту НАТО. Основним сценарієм була кібервійна в умовах гіпотетичного міждержавного конфлікту в Індо-Тихоокеанському регіоні. У навчаннях взяли участь 21 країна з НАТО та Індо-Тихоокеанського регіону.

ЦЕНТР ПЕРЕДОВОГО ДОСВІДУ НАТО ОНОВИВ СВІЙ ОНЛАЙН ІНСТРУМЕНТ CYBER LAW TOOLKIT

У вересні Центр передового досвіду НАТО (CCDCOE) оновив свій онлайн-ресурс Cyber Law Toolkit, присвячений міжнародному праву та кіберопераціям. Оновлення включає нові сценарії, описи реальних кіберінцидентів та національні позиції деяких країн щодо кіберподій. Зокрема, додано правовий аналіз кібератак на системи водопостачання в США, операцій проти місії НАТО в Туреччині та Сирії, а також витоку даних у Міжнародному кримінальному суді. На цей час ресурс містить понад 32 гіпотетичних сценарії та описує 72 кіберінциденти, засновані на реальних подіях, разом із докладним правовим аналізом.

АНБ РОЗШИРЮЄ ГЛОБАЛЬНІ ПАРТНЕРСТВА ДЛЯ ПРОТИДІЇ КІБЕРЗАГРОЗАМ З БОКУ КИТАЮ

Агентство національної безпеки США (АНБ) активно співпрацює з міжнародними партнерами, зокрема з Австралійським управлінням сигналів, щоб протистояти використанню вразливостей програмного забезпечення та дезінформації, створеної штучним інтелектом. Це стало особливо важливим під час виборів у Тайвані у 2023 році, коли дезінформація намагалася вплинути на результати голосування.

АНБ працює з понад 1,000 державними та приватними організаціями, щоб боротися з новими кіберзагрозами, особливо з боку Китаю, який використовує штучний інтелект для дестабілізації ситуації у світі. Завдяки Центру співпраці у сфері кібербезпеки, створеному у 2020 році, АНБ швидше виявляє загрози та обмінюється важливою інформацією з партнерами через захищені канали.

Також АНБ створило Центр безпеки штучного інтелекту, який захищає технології ШІ та встановлює глобальні стандарти для їх використання. Це допоможе зробити ці технології більш безпечними та етичними.

СТРИМУВАННЯ В КІБЕРПРОСТОРІ Є МОЖЛИВИМ І «НЕВІДКЛАДНИМ» ЧЕРЕЗ ЗРОСТАЮЧУ ЗАГРОЗУ ГІБРИДНИХ АТАК – НАТАНІЕЛЬ ФІК

В інтерв'ю для CyberScoop, посол США з питань кібербезпеки Натаніель Фік підкреслив важливість стримування в кіберпросторі, заявивши, що кібератаки, такі як напади з боку росії та Китаю, потребують дотримання глобальних норм для запобігання подальшій ескалації. Він зазначив, що кіберзагрози, як і традиційна війна, є наслідком людських рішень і повинні розглядатися через цей контекст, закликаючи поширювати традиційні підходи на цифровий простір.

Фік позитивно оцінив створення свого бюро, яке зосереджується на нових технологіях і кіберзахисті, а також підкреслив зусилля США щодо підтримки таких країн, як Коста-Рика та Молдова, у протистоянні російському кібервпливу. Він також закликав до розширення іноземної допомоги для зміцнення кіберзахисту союзників США.

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

ОСОБИСТІ ДАНІ ПОНАД 3000 СПІВРОБІТНИКІВ КОНГРЕСУ ОПИНИЛИСЯ У ВІДКРИТОМУ ДОСТУПІ В DARK WEB

24 вересня стало відомо, що тисячі облікових записів та особистих даних співробітників Конгресу США опинилися на Dark Web. Співробітники безпекової компанії Proton виявили ці дані під час розслідування розкритих акаунтів державних службовців. За інформацією компанії, більшість даних надійшли з кількох джерел, включаючи соціальні мережі, сайти знайомств та сайти для дорослих. Виявилось, що багато співробітників Конгресу використовували свої офіційні поштові адреси та паролі для реєстрації на цих ресурсах.

ПІД ЧАС КІБЕРАТАКИ БУЛИ ВИКРАДЕНІ ДАНІ ВСІХ ПОЛІЦЕЙСЬКИХ НІДЕРЛАНДІВ

27 вересня стало відомо, що під час кібератаки були викрадені імена всіх нідерландських поліцейських. Міністр юстиції Нідерландів підтвердив цю інформацію і повідомив нідерландській пресі, що уряд наразі оцінює можливі ризики для офіцерів під прикриттям.

КІБЕРАТАКА ПОРУШИЛА РОБОТУ АГЕНТСТВА, ВІДПОВІДАЛЬНОГО ЗА ТРАНСПОРТНУ МЕРЕЖУ ЛОНДОНА

3 вересня Transport for London (TfL), відповідальний за транспорт у Лондоні, повідомило про кібербезпековий інцидент, який вплинув на його внутрішні системи. Попри це, дані клієнтів і послуги залишилися неушкодженими. Персоналу порадили працювати з дому, а Національний центр кібербезпеки допомагає в розслідуванні.

ІРАН ВИПЛАТИВ МІЛЬЙОННИЙ ВИКУП, ЩОБ ЗУПИНИТИ МАСШТАБНУ КІБЕРАТАКУ НА БАНКИ

4 вересня видання Politico повідомило, що у серпні 2023 року сталася значна кібератака на банківську систему Ірану, яка змусила його режим виплатити викуп понад 3 мільйони доларів хакерській групі IRLeaks. Зловмисники погрожували оприлюднити конфіденційні фінансові дані з 20 іранських банків, включаючи дані рахунків мільйонів громадян. Під час атаки використовувалися уразливості в фінансовій інфраструктурі Ірану через компанію Tosan, яка постачає цифрові послуги для банківського сектору. Хоча уряд Ірану не визнав інцидент публічно, він підкреслив крихкість банківської системи країни, яка вже перебуває під значним тиском.

ІНФРАСТРУКТУРА ШПИГУНСЬКОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ PREDATOR ВІДНОВИЛА СВОЮ АКТИВНІСТЬ ПІСЛЯ ВИКРИТТЯ ТА ЗАПРОВАДЖЕНИХ САНКЦІЙ

Згідно зі звітом Insikt Group, після санкцій США шпигунське програмне забезпечення Intellexa Predator здавалося, що занепало, але нещодавно знову з'явилося завдяки модифікаціям інфраструктури, які дозволяють уникати виявлення. Клієнти в таких країнах, як Демократична Республіка Конго та Ангола, продовжують використовувати Predator, що створює серйозні ризики для конфіденційності високопоставлених осіб. Удосконалені заходи анонімності ускладнюють відстеження користувачів, хоча дотримання найкращих практик з кібербезпеки, таких як регулярні оновлення та управління мобільними пристроями, може допомогти зменшити ризики. Зусилля щодо глобального регулювання залишаються важливими у цій сфері, оскільки шпигунське програмне забезпечення продовжує розвиватися.

MICROCHIP TECHNOLOGY ПІДТВЕРДИЛА ВИКРАДЕННЯ ОСОБИСТОЇ ІНФОРМАЦІЇ ВНАСЛІДОК АТАКИ ПРОГРАМОЮ-ВИМАГАЧЕМ

5 вересня американська компанія Microchip Technology, яка постачає напівпровідники, підтвердила атаку програм-вимагачів, під час якої було викрадено особисті та бізнес-дані. Група Play взяла на себе відповідальність за цю атаку і почала розповсюджувати вкрадені дані після невдалої спроби вимагати викуп. Microchip повідомила про злам до Комісії з цінних паперів і бірж США, зазначивши, що була зламана контактна інформація співробітників і деякі зашифровані паролі, але дані клієнтів і постачальників не постраждали. Хоча критичні IT-системи вже відновлено, повний вплив атаки все ще досліджується.

HALLIBURTON ПІДТВЕРДИЛА ВИКРАДЕННЯ ДАНИХ В РЕЗУЛЬТАТІ КІБЕРАТАКИ

Велика американська нафтова компанія Halliburton підтвердила, що під час серпневої кібератаки програм-вимагачів у неї було викрадено корпоративні дані. Хакери порушили роботу окремих IT-систем і отримали доступ до конфіденційної інформації. Хоча Halliburton прямо не визнає спробу вимагання, уряд США пов'язує цю атаку з бандою програм-вимагачів RansomHub. Компанія активувала план реагування на кіберінциденти, залучивши зовнішніх експертів і правоохоронні органи для розслідування та усунення порушень. Цей інцидент показує, що нафтова та газова промисловість залишаються мішенню для атак програм-вимагачів, подібно до гучного інциденту Colonial Pipeline у 2021 році.

ЗЛАМ MOVEIT ПРИЗВІВ ДО ВИТОКУ ДАНИХ МАЙЖЕ ТРЬОХ МІЛЬЙОНІВ КОРИСТУВАЧІВ WISCONSIN MEDICARE

6 вересня видання The Record повідомило, що під час кіберзлочинної кампанії, яка вразила популярний сервіс передачі файлів MOVEit минулого року, була зламана конфіденційна інформація близько 3,1 мільйона осіб з кількох штатів. Центри Medicare і медичної допомоги (CMS), федеральне агентство, відповідальне за програму Medicare, а також Wisconsin Physicians Service Insurance Corporation (WPS), почали інформувати людей, чия особиста інформація стала доступною після того, як хакери використали вразливість у програмному забезпеченні MOVEit.

НОВА АТАКА PIXHELL ВИКОРИСТОВУЄ ШУМ РК-ЕКРАНУ ДЛЯ ВИЛУЧЕННЯ ДАНИХ ІЗ КОМП'ЮТЕРІВ, ЩО НЕ ПІДКЛЮЧЕНІ ДО МЕРЕЖІ

Згідно з нещодавно опублікованим дослідженням Offensive Cyber Research Lab на кафедрі розробки програмного забезпечення та інформаційних систем Університету Бен-Гуріона, шум РК-екрану можна використовувати для отримання даних з комп'ютерів, які не підключені до мережі. Шкідливий код використовує звук, що створюється котушками та конденсаторами, щоб контролювати частоти, які виходять з екрана. Акустичні сигнали можуть кодувати та передавати конфіденційну інформацію.

НОВА ГРУПА RAAS ВЕРБУЄ ЗЛОЧИННИХ СОЮЗНИКІВ

Підрозділ 42 компанії Palo Alto Networks опублікував звіт про нове програмне забезпечення RaaS під назвою Repellent Scorpius, яке з'явилося в травні 2024 року. Ця група розповсюджує рансомвер Cicada3301 та здійснює атаки з подвійним вимаганням, спочатку викрадаючи дані, а потім розгортаючи програму-вимагач. Дослідники зазначили, що Unit 42 має докази того, що оператори Repellent Scorpius створили партнерську програму RaaS, яка включає панель керування для афілійованих осіб і сторінки для виплати викупу жертвам. Вони також активно залучають брокерів початкового доступу (IAB) та мережевих зловмисників на російськомовних кіберзлочинних форумах.

СЛУЖБА ШВИДКОЇ ДОПОМОГИ ACADIAN ПОВІДОМИЛА ПРО ВИТІК ДАНИХ, ЯКИЙ ЗАЧЕПИВ МАЙЖЕ ТРИ МІЛЬЙОНИ ОСІБ

Служба швидкої допомоги Acadian Ambulance Service з Луїзіани повідомила про витік даних, який може торкнутися майже 3 мільйонів осіб. Компанія, заснована в 1971 році, надає екстрену та неекстрену медичну допомогу в Луїзіані, Міссісіпі, Теннессі та Техасі. Порушення безпеки сталося в червні 2024 року і пов'язане з атакою програм-вимагачів від групи Daixin, яка стверджує, що викрала та опублікувала конфіденційну інформацію про пацієнтів на своєму сайті в даркнеті.

FORTINET ПІДТВЕРДИЛА ВИТІК ДАНИХ ПІСЛЯ ТОГО, ЯК ХАКЕРИ ЗАЯВИЛИ ПРО ВИКРАДЕННЯ 440 ГБ ФАЙЛІВ

12 вересня видання Bleeping Computer повідомило, що кібербезпекова компанія Fortinet підтвердила витік даних після заяви злочинного угруповання Fortibitch, яке стверджує, що вкрало 440 ГБ файлів з її сервера Microsoft SharePoint. Хакери намагалися вимагати гроші у Fortinet, але компанія відмовилася платити. Витік торкнувся менш як 0,3% клієнтів Fortinet, включаючи невелику кількість даних, що зберігалися на сторонньому хмарному диску. Хоча компанія не розкрила точний зміст даних або кількість постраждалих клієнтів, вона запевнила, що не було злочинної діяльності щодо клієнтів, і її корпоративна мережа залишилася безпечною.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

ІНДІЙСЬКА КОМПАНІЯ STAR HEALTH ПОДАЛА ДО СУДУ НА TELEGRAM ЧЕРЕЗ ПОШИРЕННЯ ВИТОКУ ДАНИХ КОМПАНІЇ

26 вересня індійська компанія у сфері охорони здоров'я з капіталізацією в 4 мільярди доларів повідомила, що подає до суду на Telegram. Причина – компанія не припинила роботу чат-бота хакера, який використовував його для поширення вкрадених особистих даних і медичних висновків страхувальників. Компанія вже зверталася до Telegram з проханням зупинити діяльність чат-бота, але не досягла успіху. Хакер створив два чат-боти для розповсюдження даних Star Health. Один з них пропонував документи у форматі PDF, а інший дозволяв користувачам запитувати до 20 зразків з 31,2 мільйона наборів даних, надаючи такі деталі, як номер полісу, ім'я та навіть індекс маси тіла.

CLEARVIEW AI ОШТРАФУВАЛИ НА €30,5 МЛН ЗА НЕЗАКОННЕ СТВОРЕННЯ БАЗИ ДАНИХ ДЛЯ РОЗПІЗНАВАННЯ ОБЛИЧ

Управління із захисту даних Нідерландів (Dutch DPA) наклало штраф у розмірі 30,5 млн євро (33,7 млн доларів) на компанію Clearview AI, яка займається технологією розпізнавання облич, за порушення Загального регламенту захисту даних (GDPR) у Європейському Союзі. DPA вважає, що компанія створила «незаконну базу даних» з мільярдами фотографій облич, у тому числі громадян Нідерландів. Голова DPA Нідерландів Алеїд Вольфсен заявив: «Розпізнавання облич – це надзвичайно нав'язлива технологія, яку не можна застосовувати до будь-кого у світі без належних підстав».

CISA ОРГАНІЗАЦІЯМ СЛІД ПРИДІЛЯТИ БІЛЬШЕ УВАГИ СТРАТЕГІЯМ ГЛИБОКОГО ЗАХИСТУ – КЛЮЧОВИЙ ВИСНОВОК ПІСЛЯ ОПЕРАЦІЇ «ЧЕРВОНОЇ КОМАНДИ» CISA

20 вересня автор видання SecurityIntelligence Джош Надо детально проаналізував результати операції CISA SILENTSHIELD – «червоний командний» тест, проведений CISA на початку 2023 року проти федеральних цивільних органів виконавчої влади (FCEB). Про результати цієї операції CISA повідомила лише в липні 2024 року.

Під час тесту «червона команда» успішно отримала доступ до підключених мереж і систем організацій, скориставшись відомою вразливістю, яка не була виправлена на відповідних серверах. Вони змогли не лише пересуватися мережею, але й отримати доступ до захищеної інформації.

Основні висновки CISA щодо захисту у федеральних відомствах вказують на недостатній контроль для запобігання та виявлення зловмисної активності в мережі, нездатність ефективно збирати, зберігати та аналізувати мережеві журнали, погану внутрішню комунікацію між захисниками мережі через децентралізовану структуру та невміння виявити злом за допомогою нових TTP, які використовувала «червона команда».

ЛАБОРАТОРІЯ КАСПЕРСЬКОГО ВІДДАЛЕНО ВИДАЛИЛА СВОЇ ПРОДУКТИ З КОМП'ЮТЕРІВ КОРИСТУВАЧІВ ТА ВСТАНОВИЛА ІНШИЙ АНТИВІРУС

24 вересня з'явилась інформація про неоднозначні дії Лабораторії Касперського щодо своїх американських споживачів. У зв'язку із забороною продуктів Лабораторії Касперського в США, розробник антивірусного програмного забезпечення вдався до суперечливого кроку: віддалено видалив своє програмне забезпечення з комп'ютерів легальних користувачів і встановив замість нього антивірус UltraAV від Pango Group. Більшість користувачів були здивовані тим, що антивірусне програмне забезпечення може без їх відома видаляти та встановлювати програми на їхніх персональних комп'ютерах.

RANSOMWARE RUNSOMHUB ВИКОРИСТОВУЄ ІНСТРУМЕНТ EDRKILLSHIFTER ДЛЯ ОБХОДУ EDR

У своєму аналітичному матеріалі від 20 вересня кіберфахівці компанії Proofpoint досліджують ransomware під назвою RunsomHUB, яке використовує група Water Bakunawa. Ця група відрізняється тим, що застосовує різні методи для обходу захисту EDR та антивірусних систем. Одним з таких методів є EDRKillShifter – шкідливе програмне забезпечення, яке інтегроване в ланцюг атак хакерської групи. EDRKillShifter створено для використання вразливих драйверів, що підриває ефективність рішень EDR. Крім того, EDRKillShifter демонструє вдалі механізми стійкості, забезпечуючи свою постійну присутність у системі, навіть після виявлення та усунення початкових компрометацій.

GOOGLE CHROME ПЕРЕХОДИТЬ НА ML-KEM ДЛЯ ПОСТКВАНТОВОГО КРИПТОГРАФІЧНОГО ЗАХИСТУ

Компанія Google оголосила, що перейде з криптографії KYBER на ML-KEM у своєму веббраузері Chrome. Це рішення є частиною зусиль щодо захисту від ризиків, які можуть виникнути через криптографічно відповідні квантові комп'ютери (CRQC).

Очікується, що зміни набудуть чинності у версії Chrome 131, яка має вийти на початку листопада 2024 року. Google підкреслює, що два гібридні підходи постквантового обміну ключами є несумісними, що спонукало компанію відмовитися від KYBER.

5. КРИТИЧНА ІНФРАСТРУКТУРА

АГЕНЦІЯ З УПРАВЛІННЯ ПОВІТРЯНИМ РУХОМ НІМЕЧЧИНИ ПІДТВЕРДИЛА КІБЕРАТАКУ, ЗАЗНАЧИВШИ, ЩО ВОНА НЕ СПРИЧИНИЛА ЗБОЇВ У РОБОТІ

2 вересня німецька державна компанія Deutsche Flugsicherung, яка відповідає за управління повітряним рухом у країні, підтвердила, що зазнала кібератаки. Природа нападу наразі невідома. Представник прес-служби компанії повідомив, що інцидент торкнувся адміністративної IT-інфраструктури, але робота з управління авіарухом не зазнала збоїв.

КИТАЙСЬКІ ШПИГУНИ ПРОТЯГОМ МІСЯЦЯ ПЕРЕБУВАЛИ В МЕРЕЖІ АЕРОКОСМІЧНОЇ ІНЖЕНЕРНОЇ ФІРМИ ЧЕРЕЗ ВИКОРИСТАННЯ ЗАСТАРІЛИХ IT-СИСТЕМ

18 вересня директор з досліджень безпеки Binary Defense Джон Дваєр повідомив, що їм вдалося виявити китайських шпигунів у мережі однієї глобальної аерокосмічної інженерної компанії. Зловмисники використали облікові дані «за замовчуванням» порталу адміністратора на серверах IBM AIX, які компанія майже не використовувала, але які були підключені до її мережі. Зловмисники провели близько місяця в мережі, шукаючи можливості для крадіжки більше інформації. Атакована компанія виготовляє компоненти для державних і приватних аерокосмічних організацій, а також для інших критичних секторів, включаючи нафту і газ.

АМЕРИКАНСЬКА FCC ЗМУСИЛА T-MOBILE ІНВЕСТУВАТИ 31,5 МЛН ДОЛАРІВ У ПОКРАЩЕННЯ КІБЕРБЕЗПЕКИ КОМПАНІЇ

30 вересня Федеральна комісія зв'язку США (FCC) повідомила, що досягла мирової угоди з T-Mobile на суму 31,5 мільйона доларів, щоб завершити розслідування щодо значних витоків даних в компанії протягом останніх трьох років. Ці витоки вплинули на десятки мільйонів споживачів у США.

T-Mobile заплатить 15,75 мільйона доларів цивільного штрафу і витратить ще 15,75 мільйона доларів протягом двох років на покращення своєї кібербезпеки. У FCC заявили, що у 2021, 2022 та 2023 роках T-Mobile зазнала витоків даних, які вплинули на мільйони клієнтів. Зокрема, у 2021 році витік торкнувся 76,6 мільйона споживачів у США, а у 2023 році – 37 мільйонів користувачів.

КІБЕРФАХІВЦІ СТАВЛЯТЬ ПІД СУМНІВ ЗАЯВИ ПРОІЗРАЇЛЬСЬКИХ ХАКЕРІВ ПРО УСПІШНУ КІБЕРАТАКУ НА ОТ СИСТЕМИ ВОДОПОСТАЧАННЯ ЛІВАНУ

У середині вересня проізраїльське хакерське угрупування Red Devil заявило про успішну кібератаку на системи водопостачання Лівану. Зловмисники стверджували, що взяли під контроль систему SCADA, пов'язану з 14 об'єктами водопостачання в південному Лівані та Бейруті. Завдяки цьому їм вдалось змінити рівень хлору в системі водопостачання.

Однак незалежні кіберфахівці вказують на відсутність переконливих доказів цієї акції та її ефективності. Вони схиляються до думки, що ця заява є частиною ширшої інформаційно-психологічної операції, що проводиться силами оборони Ізраїлю.

У США ЧЕРГОВА СИСТЕМА ВОДОПОСТАЧАННЯ ПОСТРАЖДАЛА ВІД КІБЕРІНЦИДЕНТУ

22 вересня водоочисні споруди міста Арканзас (штат Канзас) змушені були перейти на ручне управління через інцидент кібербезпеки. Місцеве керівництво повідомило, що процес водопостачання не постраждав і інцидент не спричинив перебоїв у роботі служби.

Деталі інциденту наразі не розголошуються, але дослідники безпеки зазначають, що перехід на ручні операції вказує на те, що системи були вимкнені для стримування атаки, що є типовою реакцією на інциденти, пов'язані з ransomware.

СИСТЕМИ АВТОМАТИЧНОГО ВИМІРЮВАННЯ (ATG) У ЦИСТЕРНАХ ЗАЛИШАЮТЬСЯ ВРАЗЛИВИМИ ДО КІБЕРАТАК, ЗГІДНО З ДОСЛІДЖЕННЯМ BITSIGHT

Ще у 2015 році дослідники кібербезпеки показали, що системи автоматичного вимірювання (ATG) можуть бути піддані кібератакам. Свіже дослідження, проведене компанією Bitsight і опубліковане 24 вересня, підтвердило, що ситуація мало змінилася.

У дослідженні було проаналізовано шість систем ATG (Maglink LX і LX4, OPW SiteSentinel, Proteus OEL8000, Alisonic Sibylla та Franklin TS-550) від п'яти різних постачальників, і виявлено 10 вразливостей у безпеці, з яких 7 є «критичними».

Ці вразливості дозволяють отримати повні права адміністратора програми пристрою, а деякі з них надають повний доступ до операційної системи. Системи ATG використовуються в великих резервуарах на багатьох OKI для моніторингу таких параметрів, як об'єм, тиск і температура.

АМЕРИКАНСЬКИЙ РЕГУЛЯТОР РИНКУ ЦІННИХ ПАПЕРІВ ОПУБЛІКУВАВ НОВІ РЕКОМЕНДАЦІЇ З КІБЕРБЕЗПЕКИ

На початку січня 2024 року регуляторний орган фінансової індустрії FINRA опублікував рекомендації щодо кібербезпеки, в яких висвітлюються нові ризики від третіх сторін, що впливають на його членів і організації, які надають фінансові послуги.

Рекомендації FINRA зосереджені на попередженні кібератак через ланцюги постачання та підготовці організацій до таких атак. Вони включають більш прискіпливий моніторинг постачальників, впровадження багатофакторної аутентифікації (MFA) в організаціях і акцент на виправленні вразливостей з високим ризиком.

НЕВСТАНОВЛЕНИЙ АКТОР НАЦІЛИВСЯ НА ТРАНСПОРТНІ ТА ЛОГІСТИЧНІ КОМПАНІЇ ПІВНІЧНОЇ АМЕРИКИ

24 вересня кіберфахівці компанії Proofpoint оприлюднили інформацію про те, що їм вдалося виявити невідомого зловмисника, який за допомогою зламаних облікових записів і соціальної інженерії націлився на транспортні та логістичні компанії Північної Америки. За попередніми даними, зловмисники прагнули отримати доступ до спеціалізованого програмного забезпечення, яке використовується для управління транспортом і операціями автопарку.

80% ОРГАНІЗАЦІЙ КРИТИЧНОЇ ІНФРАСТРУКТУРИ СТИКАЮТЬСЯ ЗІ ЗЛАМАМИ ЕЛЕКТРОННОЇ ПОШТИ

17 вересня компанія OPSWAT оприлюднила результати свого дослідження безпеки електронної пошти в організаціях критичної інфраструктури (OKI). За отриманими даними, 80% організацій стикалися зі зламами електронної пошти протягом останніх 12 місяців. На кожні 1000 співробітників організації щороку припадає 5,7 випадків успішних фішингових атак та 5,6 випадків компрометації облікового запису.

НА САЙТІ АВТОВИРОБНИКА KIA ВИЯВИЛИ ВРАЗЛИВІСТЬ, ЯКА ДОЗВОЛЯЛА ВІДДАЛЕНО КЕРУВАТИ ДЕЯКИМИ ФУНКЦІЯМИ АВТОМОБІЛІВ

26 вересня дослідники безпеки опублікували результати аналізу вебсайту автовиробника KIA. Вони виявили, що одна з вразливостей на цьому сайті дозволяла віддалено керувати деякими функціями мільйонів автомобілів компанії. Ця уразливість давала змогу дистанційно керувати ключовими функціями, використовуючи лише номерний знак автомобіля. Згідно з звітом, дослідники змогли відстежувати місцезнаходження автомобіля, відімкнути його двері, подати звуковий сигнал і запустити двигун. На деяких моделях KIA вони навіть могли активувати камеру на відстані. Вразливість вже була виправлена виробником.

CISA ОПРИЛЮДНИЛА СПИСКИ КОНТРОЛІВ ДЛЯ ОЦІНКИ ГОТОВНОСТІ ДО ФІЗИЧНОЇ ТА КІБЕРБЕЗПЕКИ ПІД ЧАС ВИБОРІВ

9 вересня CISA опублікувала на своєму сайті два Списки контролів для перевірки готовності виборчого процесу до фізичних і кіберзагроз. Ці списки містять ряд запитань, які допоможуть відповідальним за виборчий процес підготуватися до потенційних інцидентів кібербезпеки та фізичної безпеки, які можуть вплинути на виборчу інфраструктуру. Список контролів фізичної безпеки складається з 15 блоків, які містять 34 контрольних питання, а Список контролів кібербезпеки включає 14 блоків і 27 контрольних питань.

6. АНАЛІТИЧНІ ОЦІНКИ

ЕКСПЕРТИ ПІДТРИМУЮТЬ ЗАПУСК CISA НОВОГО ПОРТАЛУ ДЛЯ ЗВІТУВАННЯ ПРО КІБЕРІНЦИДЕНТИ, АЛЕ ВИСЛОВЛЮЮТЬ СУМНІВИ ЩОДО ЙОГО ЕФЕКТИВНОСТІ

Наприкінці серпня CISA запустила портал для добровільного звітування про кіберінциденти. Портал «Security Magazine» зібрав думки експертів щодо цієї ініціативи. Більшість опитаних висловили підтримку цій ініціативі, вважаючи її кроком у правильному напрямку. Однак вони також висловили сумніви щодо її ефективності. Експерти вказують, що інформація з порталу може стати бажаним трофеєм для хакерів, а це може зменшити бажання потенційних учасників ділитися своїми чутливими даними через загрози репутації та можливі юридичні наслідки у випадку витоку інформації.

П'ЯТЬ КІБЕРЗАГРОЗ, ЯКІ СТАНУТЬ ТРЕНДОВИМИ НА ДУМКУ ФАХІВЦІВ SANS INSTITUTE

У вересні 2024 року було опубліковано звіт SANS про актуальні кіберзагрози. Фахівці SANS виділили 5 кіберзагроз, які або вже набирають популярність, або стануть такими найближчим часом:

- спроби здирництва у дітей через створення сексуального контенту з ними за допомогою методів штучного інтелекту;
- використання генеративного ШІ для маніпуляцій громадською думкою;
- гіперприскорення життєвих циклів експлуатації ПЗ через використання ШІ, зокрема, здатність зловмисників автоматизувати свої атаки;
- експлуатація вразливостей ПЗ, написаного за допомогою застарілих мов програмування, через брак фахівців, які можуть їх оновлювати;
- ширше використання deepfakes для ускладнення перевірки особистості користувача.

КІЛЬКІСТЬ ЖІНОК У СФЕРІ КІБЕРБЕЗПЕКИ ЗРОСТАЄ, АЛЕ ЇХНІЙ ВІДСОТОК ЗАЛИШАЄТЬСЯ НЕВЕЛИКИМ – ДОСЛІДЖЕННЯ ISC2 CYBERSECURITY WORKFORCE STUDY

5 вересня авторка видання SecurityIntelligence Дженіфер Грегорі проаналізувала дослідження «Women in Cyber», проведене організацією ISC2. Вона зазначила, що, хоча рівень середньої зарплати чоловіків і жінок у цій сфері все ще не рівний, позитивна тенденція полягає в тому, що все більше молодих жінок обирають кар'єру в кібербезпеці. Зокрема, відсоток жінок віком до 30 років у сфері кібербезпеки становить 26%, тоді як серед жінок віком від 39 до 44 років цей показник складає лише 16%.

СПРОБИ КИТАЮ ВПЛИНУТИ НА АМЕРИКАНСЬКІ ВИБОРИ СТАЛИ ЗНАЧНО АКТИВНІШИМИ ПОРІВНЯНО З ПОПЕРЕДНІМИ ПЕРІОДАМИ – ПРЕЗИДЕНТ MICROSOFT БРЕД СМІТ

18 вересня президент корпорації Microsoft Бред Сміт дав свідчення перед Спеціальним комітетом Сенату США з розвідки під час слухань на тему «Захист виборів у США від противників національних держав». Він вказав на зусилля росії, КНР та Ірану в їхніх спробах вплинути на виборчий процес у США.

Один з результатів дослідницької діяльності Microsoft – виявлення значного розширення діяльності китайських хакерів у їхніх спробах вплинути на вибори. Це включає як вкидання підбурюючого контенту (фото, відео), так і кібератаки на організації, які беруть участь у виборчому процесі.

У контексті цих слухань інші оглядачі зазначили, що глибоке розуміння проблеми з боку уряду є важливим, але недостатнім, якщо не буде виділено необхідних коштів для подолання вказаних загроз. Це стає проблемою, оскільки багато штатів вказують на недофінансування з боку федерального бюджету для захисту виборчого процесу.

У 45% ВИПАДКІВ ЗЛОВМИСНИКИ ВИКРАДАЮТЬ ДАНІ ПРОТЯГОМ МЕНШЕ НІЖ 24 ГОДИНИ ПІСЛЯ ЗЛАМУ — ЗВІТ UNIT 42

26 вересня кібербезпековий підрозділ Palo Alto Networks Unit 42 опублікував звіт про кіберінциденти у 2024 році. Автори звіту відзначають нову тенденцію: зростання швидкості, з якою зловмисники отримують доступ до даних і викрадають їх. У 45% випадків зловмисники витрачають менше 24 годин після зламу для викрадення даних, а в деяких випадках їм вдалося викачати терабайти інформації всього за кілька годин. Для порівняння, у 2023 році на це йшло кілька днів. Це підвищує вимоги до кіберзахисників щодо швидкості виявлення та реагування на такі атаки.

MITRE РОЗРОБИЛА НАБІР З 8 РЕКОМЕНДАЦІЙ ДЛЯ НОВОЇ АДМІНІСТРАЦІЇ ПРЕЗИДЕНТА США ЩОДО ЗАМІНИ ЗАСТАРІЛИХ IT-СИСТЕМ

У своєму матеріалі від 5 вересня корпорація MITRE надала ряд рекомендацій для майбутньої Адміністрації Президента США щодо проблеми застарілих і архаїчних систем у федеральних відомствах. Експерти MITRE зазначають, що деякі федеральні системи, які досі експлуатуються, були створені понад 60 років тому і становлять небезпеку в довгостроковій перспективі.

Щорічно на підтримку IT у федеральних установах витрачається близько 100 мільйонів доларів, але лише невелика частина цих коштів йде на заміну застарілих систем. Рекомендації включають конкретні кроки, які можуть вжити Офіс управління та бюджетування, Конгрес і індустрія для зміни ситуації. Це може включати інвентаризацію таких систем, пріоритизацію їх заміни, моніторинг процесу заміни та прийняття необхідних нормативних змін.

СЕРТИФІКАЦІЯ НАВИЧОК КІБЕРБЕЗПЕКИ ВАЖЛИВА ДЛЯ ЗАБЕЗПЕЧЕННЯ ЄС КВАЛІФІКОВАНОЮ РОБОЧОЮ СИЛОЮ

27 вересня ENISA у співпраці з Угорщиною провела 3-тю Європейську конференцію з навичок кібербезпеки. Захід зібрав понад 200 провідних експертів, політиків і професіоналів, які працюють у сфері кібербезпеки з усієї Європи. Однією з ключових тем конференції було усунення постійно зростаючої нестачі експертів з кібербезпеки в Європі. У цьому контексті було підкреслено важливість сертифікації навичок кібербезпеки, особливо з огляду на дотримання законодавства ЄС.

ШІСТЬ КЛЮЧОВИХ ТЕНДЕНЦІЙ НА ГЛОБАЛЬНОМУ РИНКУ ШПИГУНСЬКОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ – ЗВІТ DFRLAB

Звіт DFRLab щодо ринку шпигунського програмного забезпечення містить інформацію про 435 компаній у 42 країнах на світовому ринку шпигунського ПЗ. На основі цього деталізованого, хоча й неповного набору даних, виявлено шість основних тенденцій:

- концентрація організацій у трьох основних юрисдикціях: Ізраїль, Італія та Індія;
- серійне підприємництво між кількома постачальниками;
- партнерство між виробниками шпигунського програмного забезпечення та постачальниками обладнання для спостереження;
- регулярна зміна ідентичності постачальників;
- стратегічна зміна юрисдикції;
- транскордонні потоки капіталу, що підживлюють цей ринок.

УРЯД США НЕ ГОТОВИЙ ДО КІБЕРЗАГРОЗ У ПРОДОВОЛЬЧОМУ ТА СІЛЬСЬКОГОСПОДАРСЬКОМУ СЕКТОРАХ

У вересні видання The Record повідомило, що Міністерство сільського господарства США (USDA) не готове захищати харчовий і сільськогосподарський сектори від кібератак, попри зростання цифрових загроз. Експерти та політики попереджають, що робота міністерства, якою керує невеликий і недостатньо фінансований відділ, не є ефективною. Це робить сектор вразливим до потенційних катастроф, таких як перебої в постачанні або маніпуляції з даними.

Автоматизація в сільському господарстві збільшила кіберризики, а атака на м'ясопереробну компанію JBS у 2021 році через програму-вимагач показала ці вразливості. Критики вказують на те, що Міністерство сільського господарства США не приділяє достатньо уваги кібербезпеці, і, хоча певний прогрес був досягнутий, необхідні суттєві покращення.

NCA ВЕЛИКОБРИТАНІЇ СТИКАЄТЬСЯ З СЕРЙОЗНИМИ ВИКЛИКАМИ ЧЕРЕЗ МАСОВІ ЗВІЛЬНЕННЯ ТА ПОТРЕБУЄ ТЕРМІНОВИХ РЕФОРМ

Національне агентство боротьби зі злочинністю Великобританії (NCA) зіткнулося з серйозними проблемами через масові звільнення досвідчених співробітників, що призвело до втрати «п'ятої частини» його кіберспроможностей. Звіт Spotlight on Corruption вказує на проблеми з оплатою праці, що змушує агентство витрачати більше коштів на тимчасових працівників та консультантів.

Автори звіту закликають уряд терміново реформувати NCA, оскільки це важливо для захисту Великобританії від кіберзагроз. Хоча агентство досягло певних успіхів у боротьбі з кіберзлочинністю, нестача ресурсів заважає ефективній роботі. Уряд пообіцяв продовжити інвестувати в NCA для зміцнення його можливостей у протидії злочинності.

МАЙЖЕ ПОЛОВИНА ІНЦИДЕНТІВ ВІДБУВАЄТЬСЯ У ПІСЛЯРОБОЧИЙ ЧАС – ЗВІТ ARCTIC WOLF SECURITY

Звіт Arctic Wolf Security Operations Report за 2024 рік, який аналізує понад 250 трильйонів безпекових інцидентів, підкреслює важливість цілодобового моніторингу безпеки. Майже половина інцидентів безпеки відбувається в неробочий час. У звіті також зазначено, що збільшення кількості інструментів безпеки перевантажує команди, причому найчастіше сповіщення пов'язані з управлінням ідентифікацією. Технологічні компанії мають найслабший рівень безпеки, тоді як банківська справа та охорона здоров'я демонструють кращий стан.

Головними мішенями для кібератак залишаються провідні бізнес-програми, особливо від Microsoft. Звіт наголошує на необхідності впровадження передових заходів безпеки для підвищення стійкості організацій проти сучасних загроз.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

НКЦК ОБМЕЖИВ ВИКОРИСТАННЯ TELEGRAM В ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ, ВІЙСЬКОВИХ ФОРМУВАННЯХ, НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

На засіданні Національного координаційного центру кібербезпеки (НКЦК) 19 вересня було прийнято рішення про заборону використання месенджера Telegram на службових пристроях державних органів, військових формувань та критичних інфраструктур. Причина – Telegram активно використовується ворогом для кібератак, розповсюдження фішингу та шкідливого програмного забезпечення, встановлення геолокації користувачів, корегування ракетних ударів тощо.

З метою мінімізації цих загроз було прийнято рішення щодо заборони встановлення та використання Telegram на службових пристроях працівників органів державної влади, військовослужбовців, працівників сектору безпеки і оборони, а також підприємств – операторів критичної інфраструктури. Виняток становитимуть лише ті особи, для яких використання цього месенджера є частиною службових обов'язків.

ІСПАНІЯ ДОЛУЧИЛАСЯ ДО ІТ-КОАЛІЦІЇ

Іспанія приєдналася до ІТ-коаліції, підписавши Декларацію про наміри під час зустрічі Контактної групи з оборони України у форматі «Рамштайн». Це вже 13-та країна-партнер, яка підтримує Україну у сфері ІТ, зв'язку та кібербезпеки. Заступниця міністра оборони Катерина Черногоренко подякувала Іспанії за підтримку та зазначила, що дедалі більше країн допомагають Україні стати технологічно сильнішою. ІТ-коаліція під керівництвом Естонії та Люксембургу вже зібрала понад 70 млн євро на підтримку українського війська.

УКРАЇНА ПОСІЛА 5-ТЕ МІСЦЕ ЗА ІНДЕКСОМ ОНЛАЙН-СЕРВІСІВ У ГЛОБАЛЬНОМУ РЕЙТИНГУ ООН

Україна досягла значного прогресу в цифровізації державних послуг, піднявшись з 102-го місця у 2018 році на 5-те в рейтингу Online Service Index. Цей індекс оцінює, наскільки добре країна надає державні послуги через інтернет, зокрема зручність сайтів і можливість отримувати послуги онлайн.

Online Service Index є частиною E-Government Development Index (EGDI), який розробляється ООН і вимірює загальну ефективність використання цифрових технологій урядами для надання послуг громадянам. В цьому рейтингу Україна також показала прогрес, піднявшись з 82-го місця у 2018 році на 30-те у 2023 році.

В УКРАЇНІ БУДЕ СТВОРЕНО ЦЕНТР ОБМІНУ ІНФОРМАЦІЄЮ ПРО КІБЕРЗАГРОЗИ (ISAC)

На засіданні НКЦК було підтримано ініціативу створити центр обміну інформацією про кіберзагрози за європейською моделлю ISAC. Компанії сектору телекомунікацій постійно зазнають кібератак з боку російських хакерів. З метою покращення взаємодії у реагуванні на такі загрози учасники підтримали ініціативу щодо створення у галузі центру обміну та аналізу інформацією про кіберзагрози з використанням кращих європейських практик, зокрема за моделлю ISAC.

ЖІНКИ В КІБЕРБЕЗПЕЦІ ТА ПЛАТФОРМА CYBERTRACKER: НКЦК ЗАПУСКАЄ ІНІЦІАТИВИ ДЛЯ РОЗВИТКУ СФЕРИ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Національний координаційний центр кібербезпеки на засіданні 19 вересня оголосив про започаткування національної ініціативи, спрямованих на розвиток сфери кібербезпеки в державі. Серед них – започаткування національної ініціативи щодо сприяння посиленню ролі жінок у кібербезпеці та забезпечення гендерної рівності, а також упровадження автоматизованої платформи з моніторингу реалізації Стратегії кібербезпеки України (Cyber-Tracker), що дозволить покращити стратегічне планування у цій сфері. Також окремі питання, спрямовані на зміцнення національної кіберстійкості, було розглянуто у закритому режимі.

ДЕРЖСПЕЦЗВ'ЯЗКУ ПРЕЗЕНТУВАЛА ІНСТРУМЕНТ ОЦІНКИ КІБЕРБЕЗПЕКИ CSET

Фахівці Держспецзв'язку провели презентацію та практичне заняття з використання інструменту CSET (Cybersecurity Evaluation Tool) для оцінки кібербезпеки, адаптованого до українських потреб у співпраці з Агентством з кібербезпеки та безпеки інфраструктури Сполучених Штатів (CISA). Застосунок допоможе спеціалістам органів державної влади та операторам критичної інфраструктури у проведенні оцінок кібербезпеки, виявленні вразливих місць та визначенні необхідних заходів для покращення стану кібербезпеки як IT систем, так і систем автоматизованого управління». Адаптація даного продукту та його презентація відбулися за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України».

НКЦК ПРОВІВ ВОРКШОП ЩОДО ЗАСТОСУВАННЯ МІЖНАРОДНОГО ГУМАНІТАРНОГО ПРАВА ДО ПРОВЕДЕННЯ КІБЕРОПЕРАЦІЙ

Метою заходу було створення єдиного підходу до правового регулювання кібероперацій, які можуть бути застосовані в умовах війни, забезпечення дотримання принципів гуманітарного права, а також підготовки рекомендацій щодо позиції України на міжнародній арені.

Заступник Секретаря РНБО України Сергій Демедюк наголосив, що росія є країною-агресором, яка розпочала неспровоковану та невиправдану війну проти України, у тому числі в кіберпросторі. «Всі її атаки є грубим порушенням принципів та норм міжнародного права. Натомість Україна має законне право на самозахист, яке гарантується Статутом ООН. Це – ключова відмінність, про яку необхідно пам'ятати під час правової оцінки кібервійни між Україною та рф, що триває».

НКЦК ЗАПУСТИВ ПРОГРАМУ СТРАТЕГІЧНОГО ЛІДЕРСТВА 2.0 ДЛЯ УПРАВЛІНЦІВ У СФЕРІ КІБЕРБЕЗПЕКИ

6 вересня розпочалося навчання другого набору програми «Стратегічне лідерство для управлінців у кібербезпеці SJC-2024». Програму організував Національний координаційний центр кібербезпеки (НКЦК) разом із Global Cyber Cooperative Center. Ця програма допомагає підвищити професійний рівень керівників з державного та приватного секторів, а також політиків, які ухвалюють важливі рішення у сфері кібербезпеки. Програма SOPHOS.JOINT.CYBER розроблена за участі міжнародних експертів і включає чотири модулі, що фокусуються на стратегічному лідерстві та прийнятті рішень для зміцнення кіберзахисту України. Цього року у програмі беруть участь 50 фахівців із кібербезпеки.

УКРАЇНСЬКІ ВІЙСЬКОВІ ВИЯВЛЯЮТЬ 12 ТИСЯЧ ЦІЛЕЙ ЩОТИЖНЯ ЗАВДЯКИ ШТУЧНОМУ ІНТЕЛЕКТУ – КАТЕРИНА ЧЕРНОГОРЕНКО

Сили оборони щотижня автоматично виявляють 12 тисяч одиниць ворожої техніки за допомогою платформи штучного інтелекту Avengers, розробленої Центром інновацій Міноборони України. Платформа автоматично аналізує відео з дронів і камер, що дозволяє операторам швидше та ефективніше приймати рішення. Avengers інтегрована у бойову систему DELTA. Центр інновацій продовжує навчати ШІ-модель платформи Avengers на нових даних. Це дозволяє удосконалювати якість розпізнавання різноманітної ворожої техніки, навіть у складних умовах.

ГОЛОВА НАЦПОЛІЦІЇ ІВАН ВИГІВСЬКИЙ ВИСТУПИВ У ЄВРОПОЛІ З ТЕМОЮ ПРО ГІБРИДНІ ЗАГРОЗИ ТА КІБЕРАТАКИ РОСІЇ

Голова Нацполіції України Іван Вигівський виступив на Європейському з'їзді керівників поліції в Європолі з темою про гібридні загрози та кібератаки росії проти України. Він наголосив на зростанні кібератак з початком вторгнення та поділився досвідом українських правоохоронців у боротьбі з цими викликами. Під час асамблеї Вигівський також провів двосторонні зустрічі із представниками Угорщини, Німеччини, США, Румунії, Великої Британії, Італії та Іспанії, де сторони обговорили подальшу співпрацю.

УКРАЇНА ТА ЯПОНІЯ ПОСИЛЮЮТЬ СПІВПРАЦЮ В МЕЖАХ ІТ-КОАЛІЦІЇ

Заступниця міністра оборони Катерина Черногоренко зустрілась з Надзвичайним і Повноважним Послом Японії в Україні паном Мацудою Кунінорі та його командою в Києві. Вони обговорили подальшу співпрацю щодо впровадження проєктів в межах коаліції, а також цифрову трансформацію війська та системи Резерв+, Армія+ і DELTA. Черногоренко подякувала Японії за підтримку та зазначила, що сторони домовилися продовжувати роботу над поточними ініціативами і шукати нові можливості для співпраці.

ДЕРЖСПЕЦЗВ'ЯЗКУ ПОСИЛЮЄ СПІВПРАЦЮ З МІЖНАРОДНИМИ ПАРТНЕРАМИ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ ЗА СТАНДАРТАМИ NATO

Держспецзв'язку України та Державна комісія з питань захисту інформації Болгарії підписали Меморандум про взаєморозуміння у сфері захисту інформації з обмеженим доступом за стандартами NATO. Співпраця охоплюватиме обмін досвідом у сфері захисту інформації з обмеженим доступом за стандартами NATO, акредитації з безпеки інформаційно-комунікаційних систем, де обробляється така інформація, реалізації національної політики у сфері захисту інформації з обмеженим доступом та розвитку спроможностей національних безпекових акредитаційних органів.

КІБЕРПОЛІЦІЯ УКРАЇНИ ПОСИЛЮЄ МІЖНАРОДНУ СПІВПРАЦЮ ДЛЯ ЗАХИСТУ ДІТЕЙ ОНЛАЙН

У вересні в Гаазі відбулася зустріч «Victim Identification Task-Force (VIDTF) 15», організована Європолом. Представники правоохоронців з 31 країни, зокрема кіберполіція України, допомагали ідентифікувати жертв сексуального насильства над дітьми. Вони аналізували контент і використовували міжнародні бази для встановлення осіб, які виготовляють дитячу порнографію. Отриману інформацію передали правоохоронцям у країнах Європи та Америки. Під час зустрічі також проводилися тренінги, аналізувалися методи розслідування та пошук шляхів покращення співпраці між поліцейськими різних країн.

ДІЯ.ОСВІТА ТА ПРОЄКТ USAID КІБЕРБЕЗПЕКА ЗАПУСТИЛИ ІНФОРМАЦІЙНУ КАМПАНІЮ З КІБЕРГІГІЄНИ

Мета кампанії – підвищити обізнаність українців про онлайн-загрози та навчити основ кібергігієни, важливих для захисту в цифровому світі. У межах інформаційної кампанії анонсовані нові освітні серіали та симулятори, що покривають різні цільові аудиторії — від підлітків до людей елегантного віку:

- Кібергігієна для молоді – пояснює базові правила безпеки в інтернеті;
- Базові знання з кібергігієни – серіал для користувачів мережі елегантного віку, який містить дієві поради про захист мобільних пристроїв та банківських карток, безпечно виконувати онлайн-операції;
- Кібергігієна: як захиститися від фішингу – розповідає про загрози шахрайства в мережі.

Національна кампанія також включає серію соціальної реклами для різних вікових груп. Усі матеріали доступні на платформі Дія.Освіта: https://osvita.diia.gov.ua/cyberhygiene

Серіали «Кібергігієна для молоді» та «Базові знання з кібергігієни» створено з ініціативи Мінцифри Національним координаційним центром кібербезпеки та Національним університетом «Києво-Могилянська академія» за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України».

СБУ ЛІКВІДУВАЛА ДВІ БОТОФЕРМИ, ЯКІ ПРОВОДИЛИ ІНФОРМДИВЕРСІЇ ПРОТИ УКРАЇНИ

СБУ та Національна поліція викрили дві ботоферми в Полтавській і Закарпатській областях, які працювали на російські спецслужби. Організаторами були двоє місцевих ІТ-фахівців, які продавали фейкові акаунти рф. Через ці акаунти росіяни поширювали дезінформацію про Україну та дискредитували Сили оборони.

У Полтавській області викрили місцевого жителя, який на замовлення росії створив майже 15 тисяч анонімних акаунтів у соцмережах та месенджерах. На Закарпатті закрили канал незаконного продажу унікальних IP-адрес до росії, які дозволяли росіянам маскуватися під українців в Інтернеті. Фігурант отримував оплату в криптовалюті через російські платіжні системи. Обом організаторам загрожує до 5 років ув'язнення.

ГУР РОЗПОВІЛО ПРО ЗЛАМ ФЕДЕРАЛЬНОГО ЦЕНТРУ ВИДАЧІ ЦИФРОВИХ ПІДПИСІВ

11 вересня 2024 року українські кіберфахівці з ГУР МО розповіли про проведену разом з активістами BO Team успішну атаку на російський федеральний посвідчувальний центр «Основаніє», який видає електронні підписи. Цей центр обслуговує банки, військові та державні установи, зокрема «вертольоти россии», «Альфа-Банк» та інші. Внаслідок атаки знищено терабайти даних, а також отримано базу даних на 1,5 мільйона електронних підписів. Хакери планують продати ці дані, а кошти передати на потреби українських військових.

СБУ ТА БЕБ ВИКРИЛИ МЕРЕЖУ ПІДПІЛЬНИХ БРОКЕРІВ WEBMONEY, ЯКІ ФІНАНСУВАЛИ РОСІЙСЬКУ АГЕНТУРУ В УКРАЇНІ

СБУ та БЕБ ліквідували мережу підпільних онлайн-сервісів, що використовували заборонену в Україні платіжну систему Webmoney. Частина переказів фінансувала російську агентуру. У 10 регіонах викрито 12 осіб, які незаконно обмінювали електронні кошти, у тому числі з рф, і конвертували їх у валюту або готівку. З початку війни вони провели десятки мільйонів гривень. Усім фігурантам оголошено підозру, вирішується питання щодо додаткової кваліфікації їхніх дій.

НА ДНІПРОПЕТРОВЩИНІ ЗАТРИМАЛИ ХАКЕРА, ЯКИЙ ПРОДАВАВ БАЗИ ДАНИХ ТИСЯЧ КОРИСТУВАЧІВ

Кіберполіція затримала 25-річного жителя Кам'янського, який зламав близько 10 тисяч електронних пошт користувачів і продавав їх дані. Для цього він використовував метод брутфорсу (brute force) — автоматичний підбір паролів за допомогою спеціального програмного забезпечення. Хакер зламував сервери різних вебресурсів, зокрема сайтів знайомств, використовуючи вразливості через SQL-ін'єкції — впровадження шкідливого коду у бази даних сайтів. Отримані паролі дозволяли йому входити до електронних скриньок, які не були захищені двофакторною автентифікацією, і красти персональні дані, включаючи доступ до криптогаманців.

З «відпрацьованих» акаунтів зловмисник формував бази даних для продажу у даркнеті. Кіберполіцейські встановили близько 10 облікових записів фігуранта на різних хакерських форумах, частина з яких адмініструється з рф. Підозрюваному загрожує до 15 років ув'язнення. Він знаходиться під вартою, слідчі перевіряють можливі зв'язки з ворогом та збитки, завдані потерпілим.

CERT-UA ВИЯВИЛА КІБЕРАТАКИ З ВИКОРИСТАННЯМ ПІДРОБЛЕНИХ МОБІЛЬНИХ ЗАСТОСУНКІВ ДЛЯ ВІЙСЬКОВИХ СИСТЕМ

CERT-UA разом із командою MILCERT та фахівцями системи «Очі» виявили дві кібератаки на мобільні пристрої українських військових. Хакери через Signal поширювали посилання на фальшиві застосунки GRISELDA та «Очі», що містили шкідливе ПЗ. Метою атак було викрадення облікових даних та GPS-координат пристроїв. Завдяки швидкій взаємодії між фахівцями кіберзагроза була нейтралізована.

ХАКЕРИ РФ АКТИВІЗУВАЛИ АТАКИ НА УКРАЇНСЬКИХ ВІЙСЬКОВИХ – ДЕРЖСПЕЦЗВ'ЯЗКУ

У першій половині 2024 року хакери рф посилили спроби отримання персональних даних українських військовослужбовців для доступу до військових систем. Про це йдеться в аналітичному звіті Держспецзв'язку «російські кібероперації» Н1'2024. Зловмисники використовують месенджери та інші засоби комунікації, видаючи себе за знайомих жертви. Вони надсилають шкідливі файли, маскуючи їх під документи або відео, пов'язані з військовою діяльністю. Детальний аналіз кіберзагроз та рекомендації щодо захисту від них доступні у звіті за посиланням:

UA: https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=65897&embedded=true&a=bi

EN: https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=65898&embedded=true&a=bi

РОСІЙСЬКІ ХАКЕРИ ЗМІНИЛИ ТАКТИКУ АТАК НА УКРАЇНУ – ДОСЛІДЖЕННЯ ДЕРЖСПЕЦЗВ'ЯЗКУ

У першій половині 2024 року російські хакери змістили акцент своїх атак на об'єкти, тісно пов'язані з військовими операціями та постачальниками критичних послуг, намагаючись максимально довго залишатися непоміченими в системах.

Аналітичний звіт Держспецзв'язку (також опрацьований британським виданням The Register) зазначає, що у 2022 році атаки були спрямовані на знищення IT-інфраструктури та викрадення баз даних, а також кампанії проти медіа та бізнесу. Проте у 2023 році стратегія змінилася: зловмисники зосередилися на прихованому зборі інформації для аналізу ефективності фізичних атак. У 2024 році їхні дії стали ще більш витонченими, з акцентом на тривале проникнення в системи, пов'язані з театром бойових дій і державною діяльністю, використовуючи їх як приховані канали збору розвідувальної інформації.

8. ПЕРША СВІТОВА КІБЕРВІЙНА

КИТАЙСЬКОМОВНА ХАКЕРСЬКА ГРУПА НАЦІЛИЛАСЬ НА РОЗРОБНИКІВ ДРОНІВ У ТАЙВАНІ

6 вересня кібербезпекова компанія TrendMicro опублікувала результати дослідження щодо діяльності групи TIDRONE, китайськомовного хакерського угруповання, яке зосереджене на атаках на безпековий сектор Тайваню. Група намагається отримати доступ до мереж військової промисловості, супутникових систем і виробників дронів. Дослідники вважають, що ця діяльність не є фінансово мотивованою, а більше схожа на кібершпигунську операцію.

КИТАЙ ЗВИНУВАЧУЄ ТАЙВАНЬ У КІБЕРАТАКАХ НА СВОЇ СИСТЕМИ

23 вересня Міністерство національної безпеки Китаю звинуватило хакерську групу Anonymous 64, яку нібито підтримують тайванські військові, у кібератаках на китайські об'єкти. У своїй заяві Китай оприлюднив імена та фотографії трьох тайванців, яких вважає членами групи. Міністерство оборони Тайваню відкинуло ці звинувачення і, своєю чергою, звинуватило Китай у глобальних кібершпигунських операціях.

ХАКТИВІСТИ ВИКОРИСТОВУЮТЬ ВРАЗЛИВІСТЬ WINRAR ДЛЯ АТАК НА РОСІЮ ТА БІЛОРУСЬ

Групу хактивістів, відому як Head Mare, пов'язують з кібератаками на організації, розташовані в росії та Білорусі. Вони використовують сучасні методи для отримання первинного доступу, зокрема, експлуатують уразливість CVE-2023-38831 у WinRAR, яка дозволяє виконувати довільний код через спеціально підготовлений архів.

Head Mare, активна з 2023 року, здійснює атаки на російські організації в контексті російсько-української війни. Група також присутня у мережі X (колишній Twitter), де публікує конфіденційну інформацію та внутрішню документацію своїх цілей, серед яких урядові структури, транспортний сектор, енергетика, виробництво тощо.

MICROSOFT ПОЧАВ ВІДКЛЮЧАТИ РОСІЙСЬКІ КОМПАНІЇ ВІД ХМАРНИХ СЕРВІСІВ

Про це повідомила агенція «Укрінформ» з посиланням на російські опозиційні ЗМІ. У серпні компанія «Софтлайн» попередила, що з 2 вересня Microsoft запровадить нові санкції проти російського бізнесу, відрізавши корпоративним клієнтам у рф доступ до деяких хмарних передплат.

ХАКЕРИ, ПОВ'ЯЗАНІ З РОСІЄЮ ТА БІЛОРУССЮ, ВСЕ ЧАСТІШЕ НАЦІЛЮЮТЬСЯ НА ЛАТВІЙСЬКІ ВЕБСАЙТИ

Латвійські офіційні особи, що відповідають за кібербезпеку, повідомили про нову хвилю кібератак, здійснюваних політично мотивованими хакерами з росії та Білорусі на урядові та критично важливі інфраструктурні сайти Латвії. Метою цих атак є порушення доступу до вебсайтів, а не крадіжка чутливої інформації. Атаки активізувалися після оголошення Латвією нового пакета допомоги Україні та зазвичай відбуваються у відповідь на політичні рішення або під час свят. Більшість інцидентів були DDoS атаками, які тимчасово уповільнювали роботу атакованих сайтів.

Латвійські службовці зазначають, що країна добре підготовлена до таких атак, але боротьба ускладнюється через постійну зміну мішеней і технік хакерів. Ці атаки вважаються частиною «гібридної війни», метою якої є створення паніки в суспільстві та підірвання довіри до державних установ.

США ОГОЛОШУЮТЬ ЗВИНУВАЧЕННЯ ТА ВИНАГОРОДИ ЗА ХАКЕРСЬКІ АТАКИ WHISPERGATE РОСІЇ ПРОТИ УКРАЇНИ

Федеральні агентства США оголосили новий обвинувальний акт проти п'яти членів російської військової розвідки (гру) та одного цивільного, які брали участь у кіберкампаніях із використанням шкідливого програмного забезпечення WhisperGate. Обвинувачення висунуто за змову з метою комп'ютерного вторгнення та шахрайства, спрямованого, зокрема, на комп'ютерні системи уряду України перед початком російського вторгнення у 2022 році.

Агентство юстиції звинуватило членів підрозділу 29155 у зломі, викраденні даних та руйнуванні комп'ютерних систем, пов'язаних з урядом України, а також зазначило, що їхні атаки були націлені на критичну інфраструктуру та цивільні установи. США пропонують винагороду до 10 мільйонів доларів за інформацію, що допоможе у справі.

ПОЛЬСЬКІ СПЕЦСЛУЖБИ РОЗКРИЛИ МЕРЕЖУ РОСІЙСЬКИХ І БІЛОРУСЬКИХ КІБЕРДИВЕРСАНТІВ

9 вересня віцепрем'єр-міністр і міністр цифровізації Польщі Кшиштоф Гавковський повідомив, що польські спецслужби викрили мережу російських і білоруських кібердиверсантів. Ці зловмисники планували проникнути в системи державних органів влади та місцевого самоврядування Польщі, щоб викрасти інформацію для подальшого шантажу та ведення кібервійни. Завдяки зусиллям спецслужб вдалося запобігти потенційному паралічу польської влади.

НІМЕЦЬКА РОЗВІДКА ЗВИНУВАЧУЄ РОСІЙСЬКЕ ГРУ В КІБЕРАТАКАХ НА КРАЇНИ НАТО ТА ЄС

9 вересня Al Jazeera повідомила, що внутрішня розвідка Німеччини (BfV) попередила про кібератаки, спрямовані проти країн НАТО та ЄС з боку російської військової розвідки. У спільних настановах з кібербезпеки, виданих разом із ФБР, Агентством кібербезпеки та безпеки інфраструктури США (CISA), АНБ та іншими партнерами, ці атаки приписуються підрозділу 29155 гру, який відомий своєю участю у шпигунстві, диверсіях та дестабілізації західних країн. Цей підрозділ також пов'язаний із вбивствами за кордоном. BfV підкреслила, що міжнародні партнери продовжують зобов'язуватися захищати критичну інфраструктуру, демократію та свободу від таких кіберзагроз.

ХАКЕРИ, ПОВ'ЯЗАНІ З KIMSUKY, ВИКОРИСТОВУЮТЬ СХОЖУ ТАКТИКУ ДЛЯ НАПАДУ НА РОСІЮ ТА ПІВДЕННУ КОРЕЮ

Згідно зі звітом південнокорейської компанії з кібербезпеки Genians, пов'язана з Північною Кореєю хакерська група Konni, яка тісно співпрацює з державною групою Kimsuky, активізує свої кібершпигунські атаки на Південну Корею та росію. Починаючи з 2021 року, Konni націлилася на такі організації, як міністерство закордонних справ росії та південнокорейські підприємства, використовуючи фішингові електронні листи з такими темами, як податки та стипендії, для розповсюдження шкідливого програмного забезпечення.

Хакери застосовують схожу тактику в обох країнах, використовуючи трояни віддаленого доступу (RAT) для контролю заражених систем і підключення їх до серверів, якими керують зловмисники. Діяльність Konni розпочалася у 2014 році і продовжує становити серйозну загрозу. Дослідники припускають, що вивчення подібностей між цими атаками може допомогти службам безпеки краще реагувати на загрози.

ЕКСПЕРТИ ІДЕНТИФІКУВАЛИ ТРИ КИТАЙСЬКИХ КЛАСТЕРИ, ВІДПОВІДАЛЬНІ ЗА КІБЕРАТАКИ В ПІВДЕННО-СХІДНІЙ АЗІЇ

10 вересня видання The Hacker News повідомило, що кібербезпекова фірма Sophos зафіксувала компрометацію додаткових урядових організацій у Південно-Східній Азії трьома китайськими загрозливими кластерами. Це стало частиною відновленої державної операції з кодовою назвою «Crimson Palace», яка свідчить про розширення масштабів шпигунської діяльності Китаю.

ІРАНСЬКА КІБЕРГРУПА OILRIG ЗДІЙСНИЛА СКЛАДНУ АТАКУ НА УРЯД ІРАКУ

Згідно зі звітом компанії Check Point, урядові мережі Іраку стали ціллю кібератак, організованих спонсорованим іранською державою загрозливим актором під назвою Oil-Rig. Ці атаки були спрямовані на важливі іракські організації, такі як офіс прем'єр-міністра та міністерство закордонних справ.

Група OilRig, яка діє щонайменше з 2014 року, відома своїми фішинговими атаками на Близькому Сході. Її метою є встановлення спеціальних бекдорів для крадіжки конфіденційної інформації.

ПОРТОВІ КРАНИ КИТАЙСЬКОГО ВИРОБНИЦТВА В США МІСТЯТЬ БЕКДОРИ З МОДЕМАМИ – ЗВІТ ПАЛАТИ ПРЕДСТАВНИКІВ

Як повідомило видання The Record 12 вересня, розслідування Конгресу США виявило, що Китай встановив технологічні бекдори, зокрема стільникові модеми, у крани «судно-берег», які використовуються в портах США. Ці модеми, без відома портів, були підключені до комп'ютерів Linux на кранах і могли збирати дані про їхнє використання, а також обходити брандмауери, створюючи ризик перебоїв у роботі портів.

У звіті висловлюється занепокоєння щодо впливу Китаю на критично важливу інфраструктуру США, особливо в умовах зростання напруженості навколо Тайваню. У відповідь адміністрація Байдена оголосила про інвестиції в американське виробництво кранів у співпраці з японською компанією Matsui, щоб зменшити залежність від китайського обладнання. Берегова охорона також посилила вимоги щодо кібербезпеки в портах для захисту від таких загроз.

ПІВНІЧНОКОРЕЙСЬКІ ХАКЕРИ АТАКУЮТЬ ЕНЕРГЕТИЧНУ ТА АЕРОКОСМІЧНУ ПРОМИСЛОВІСТЬ ЗА ДОПОМОГОЮ НОВОГО ШПЗ MISTPEN

18 вересня видання The Hacker News, посилаючись на звіт Mandiant, повідомило, що пов'язана з Північною Кореєю кібершпигунська група використовує фішингові приманки, пов'язані з роботою, для атак на енергетичні та аерокосмічні компанії. Зловмисники заражають жертв раніше незадокументованим бекдором під назвою MISTPEN. Активність цієї групи відстежується під назвою UNC2970, яку Mandiant пов'язує з групою TEMP.Hermit, також відомою як Lazarus Group або Diamond Sleet (раніше Zinc).

Ця група займається шпигунською діяльністю принаймні з 2013 року, атакуючи урядові, оборонні, телекомунікаційні та фінансові установи по всьому світу для збору стратегічних розвідувальних даних на користь Північної Кореї. Вона пов'язана з Головним управлінням розвідки (RGB).

КИТАЙСЬКІ ШПИГУНИ СТВОРИЛИ ВЕЛИКИЙ БОТНЕТ З IOT-ПРИСТРОЇВ ДЛЯ АТАК НА АРМІЮ США ТА ТАЙВАНЮ

Як повідомило видання Security Week 18 вересня, дослідники з Lumen Technologies виявили великий ботнет під назвою Raptor Train, що складається з сотень тисяч захоплених пристроїв Інтернету речей (IoT). Імовірно, цей ботнет керується китайською хакерською групою Flax Typhoon і націлений на критично важливі сектори в США та Тайвані, включаючи військові та урядові установи.

Активний з 2020 року, Raptor Train використовує законні програми для маскування та має надійну інфраструктуру управління. Він експлуатує різноманітні пристрої, такі як маршрутизатори та IP-камери, і розгортає важковиявлене зловмисне програмне забезпечення під назвою Nosedive.

Нещодавнє порушення роботи ботнету показало, що в червні 2023 року він контролював понад 60 000 пристроїв, а загалом було скомпрометовано близько 260 000 пристроїв за чотири роки. Ця тривала активність викликає серйозне занепокоєння у фахівців з кібербезпеки в США.

ФБР ОГОЛОСИЛО ПРО ЗНИЩЕННЯ КИТАЙСЬКОЇ КІБЕРШПИГУНСЬКОЇ ГРУПИ FLAX TYPHOON

18 вересня правоохоронні органи США, включно з ФБР, оголосили про нейтралізацію великої китайської хакерської групи «Flax Typhoon». За даними ФБР, цією групою керує китайська компанія під назвою Integrity Technology Group, яка позиціонувала себе як IT-компанія. Однак, насправді вона займалася збором розвідданих і проведенням шпигунських операцій в інтересах китайських урядових служб безпеки.

КИТАЙСЬКІ КІБЕРШПИГУНИ З SALT TYPHOON ПРОНИКЛИ В МЕРЕЖІ АМЕРИКАНСЬКИХ ІНТЕРНЕТ-ПРОВАЙДЕРІВ

25 вересня стало відомо, що китайське кіберугрупування Salt Typhoon, ймовірно, зламало кількох інтернет-провайдерів у США. Хоча офіційних підтверджень цього проникнення та його атрибуції наразі немає, керівництво CISA заявило, що знайомі з цією інформацією, але поки що не можуть надати додаткових деталей.