НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

УКРАЇНСЬКА ФУНДАЦІЯ БЕЗПЕКОВИХ СТУДІЙ

CYBER DIGEST

Огляд подій в сфері кібербезпеки,
червень 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 концентрується на освітній складовій, визнаючи значну нестачу кіберфахівців у всіх секторах економіки (наразі існує близько 500 тисяч незаповнених вакансій). Офіс національного кібердиректора США (ONCD) активно просуває імплементацію Національної стратегії кіберосвіти та робочої сили, проводячи дискусії з учасниками ринку. В цих дискусіях все частіше лунає думка концептуально відмовитись при винаймі кіберфахівців від вимоги наявності у них вищої освіти та зробити ставку виключно на підтверджену кваліфікацію. Це має допомогти та Міністерству оборони США, яке зараз має близько 27 тисяч кібервакансій, які не може заповнити через бюрократичні проблеми.

Сектор операційних технологій (ОТ) намагається адаптуватись до нової реальності підвищених кіберзагроз для цієї унікальної сфери. США занепокоєно низькими стандартами кібербезпеки саме для ОТ технологій, від яких залежать критичні послуги економіки. Уряд намагається вдатись до додаткового регулювання, однак власники промислових об'єктів вказують на системні проблеми з процесом регулювання, яке є здебільшого фрагментарним та суперечливим щодо секторальних стандартів. Також власники промислових компаній вказують на специфічність ОТ як технологічних рішень, які складно і дорого модернізувати. Однак малоймовірно, що ці аргументи будуть мати ефект – в багатьох промислових організаціях не дотримуються навіть найпростіших стандартів кібербезпеки (як то заміна стандартних паролів), що ставить під загрозу функціонування критичної інфраструктури.

Україна вдосконалює та впроваджує державні політики у сфері кібербезпеки та новітніх технологій. Мінцифра презентувала Білу книгу щодо регулювання штучного інтелекту в Україні. Цей крок допоможе компаніям підготуватися до запровадження законодавчого регулювання у цій сфері, а державі – інтегруватися до ЄС. Кабінет Міністрів України схвалив завдання Національної програми інформатизації. З метою автоматизації моніторингу виконання Стратегії кібербезпеки України, НКЦК презентував новий інструмент – CyberTracker. Державна служба спеціального зв'язку та захисту інформації затвердила вимоги до аудиторів інформаційної безпеки на ОКІ та порядок їх атестації, в той час, як перший в Україні розпочав сертифікацію спеціалістів Кваліфікаційний центр інформаційних технологій та кібербезпеки.

Україна активно інтегрується до європейського та євроатлантичного простору у сфері кібербезпеки, адже побудова кіберстійкості та надання відсічі рф є спільним завданням України та країн ЄС. У червні Національний координаційний центр кібербезпеки став партнером Paris Cyber Summit, Україна вперше взяла участь у європейських кібернавчаннях Cyber Europe. Українська інноваційна платформа Brave1, НАТО та Defense Innovation Unit Міністерства оборони США вперше провели Форум оборонних інноваторів НАТО-Україна, де, серед іншого, обговорювали перспективи інвестування в український defense tech, плани співпраці в оборонно-технологічній сфері.

У червні відбулась атака ransomware на компанію Synnovis, яка спеціалізується на клінічних дослідженнях і є ключовим партнером Національної служби здоров'я Великобританії. Зловмисники, яких підозрюють у належності до російського угрупування Qilin, вимагали викуп у розмірі 50 мільйонів доларів. Однак активна реакція правоохоронних органів призвела до зменшення їхньої активності. Сектор охорони здоров'я залишається однією з улюблених цілей хакерів, особливо в умовах, коли використовуються програми-вимагачі, як от ransomware Knight, через слабкі системи захисту та великий обсяг персональних даних. На цьому фоні продовжується активна дискусія щодо необхідності повної заборони виплат викупу зловмисникам. Однак частина стейкхолдерів висловлює обурення, стурбована можливими наслідками таких обмежень на їхню діяльність у разі кібератак. Зловмисники, своєю чергою, все частіше застосовують нестандартні методи тиску, включаючи фізичний вплив на потенційних жертв, як це було у випадку з групою UNC3944.

Штучний інтелект стає постійним елементом безпекових дискусій. В травні 2024 року це було ключовою темою конференції RSAC 2024, а в червні CISA вже провела перші командно-штабні навчання щодо загроз від ШІ. Дослідники з аналітичного центру CSIS демонструють як ШІ може впливати на процес прийняття рішень у сфері національної безпеки. Вже згадана CISA також занепокоєна тим, як ШІ може вплинути на зростання кіберзагроз в хімічному та біологічному сектору. Одночасно з цим, урядові структури США шукають шляхи як застосувати ШІ для більшої безпеки – зокрема зараз це питання опрацьовується Міноборони США в частині передачі ШІ можливостей реагування на кібератаки.

Не можна не відзначити зростаючу активність російських хакерів проти країн-партнерів України. Лише у червні вони здійснили кілька значних атак. Зокрема, було атаковано сайт іспанської компанії, яка займається ремонтом танків Leopard для України. Також були зафіксовані втручання в супутникові ефіри, що призводило до переривань і навіть трансляції російських військових відео на дитячому телеканалі. російські хакери постійно шукають нові інструменти доступу до своїх жертв, наприклад, атакували компанію TeamViewer. Особливе занепокоєння викликає бажання та готовність російських хакерів втручатися у виборчі процеси в США та Європі. Водночас проукраїнські хакери завдають значні удари у відповідь. Низка російських енергетичних компаній, IT-компаній та державних установ постраждали від трояна Decoy Dog. Було порушено роботу супермаркетів по всій росії, а група Sticky Werewolf здійснила атаки на російську фармацевтичну компанію та науково-дослідний інститут, що займається мікробіологією та розробкою вакцин. Крім того, була здійснена масштабна атака на великі російські банки, що зробило їхні послуги недоступними для деяких користувачів.

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

ENISA НАБУЛА ПОВНОВАЖЕНЬ ОРГАНУ НУМЕРАЦІЇ ЗАГАЛЬНИХ ВРАЗЛИВОСТЕЙ (CVE)

12 червня ENISA повідомила, що офіційно набула повноважень як органу нумерації загальних вразливостей (CVE) і ще активніше буде надавати підтримку мережі CSIRT та реалізації програми відповідального розкриття вразливостей. Тепер ENISA має право призначати ідентифікатори CVE і публікувати записи CVE для вразливостей, виявлених CSIRT Європейського Союзу або повідомлених їм. Крім того, згідно з NIS2, ENISA розробляє та підтримує Європейську базу даних про вразливості (EUVD).

БІЛИЙ ДІМ ПРОВІВ ДИСКУСІЮ ЩОДО СТРАТЕГІЇ РОЗВИТКУ ПОТЕНЦІАЛУ ВИРОБНИЧИХ КІБЕРСИЛ З ПРЕДСТАВНИКАМИ 12 ГАЛУЗЕЙ

На початку червня Офіс національного кібердиректора (ONCD) організував 3-годинну дискусію щодо створення сильної робочої сили з кібербезпеки. У сесії взяли участь представники понад 30 державних і приватних організацій, що охоплюють 12 галузей.

Основні висновки дискусії:

- кожній організації (включно з МСБ) потрібні стратегії залучення кіберфахівців;
- всюди де це можливо потрібно забезпечити найм працівників на основі кваліфікації, а не вимог наявності освітнього рівня;
- майбутнім фахівцям потрібні реальні майданчики для тестування своїх знань (наприклад SOCи локального рівня);
- потрібні чіткі та зрозумілі моделі розвитку професіоналів в межах організацій;
- підготовка якісних кіберкадрів є питанням національної безпеки.

CISA ПРОВЕЛА ПЕРШІ КОМАНДНО-ШТАБНІ НАВЧАННЯ (TTX) ПО ШІ

13 червня CISA разом з іншими федеральними установами та партнерами з приватного сектора провели TTX, спрямований на ефективну та скоординовану реакцію щодо інцидентів безпеки штучного інтелекту. TTX зібрав понад 50 експертів зі ШІ. Захід відбувся у приміщенні заводу Microsoft Corp у Рестоні, штат Вірджинія. Чотиригодинні навчання проводилися під керівництвом JCDC – у завданнях було змодельовано кіберінцидент за участю системи з підтримкою ШІ. Учасники відпрацьовували механізми оперативного співробітництва і протоколи обміну інформацією для реагування на інциденти між представленими організаціями.

ВІДБУЛИСЬ ЗАГАЛЬНОЄВРОПЕЙСЬКІ КІБЕРНАВЧАННЯ CYBER EUROPE 2024

19-20 червня ENISA провела дводенні кібернавчання Cyber Europe. Сценарії зосередився на кіберзагрозах енергетичній інфраструктурі ЄС, які були викликані геополітичною напруженістю між Європейським Союзом та вигаданою іноземною державою. Ввідні передбачали активну пропаганду супротивника, яка впливала на громадську думку, і діяльність APT- груп, що була спрямована на енергетичний сектор. Щоб запобігти широкомасштабній атаці, яка руйнує європейську економіку та дестабілізує політичну рівновагу, учасники повинні були швидко скоординувати свої дії та відповідь. У навчаннях взяли участь 30 національних агенцій з кібербезпеки, інші державні установи країн-членів, а також понад 1000 профільних експертів.

МІНІСТЕРСТВО ОБОРОНИ США ПРИЙНЯЛО СТРАТЕГІЮ РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

25 червня Пентагон оприлюднив прийняту ним Стратегію досягнення IT-інтеграції та сумісності. Мета стратегії – створити сумісну, інтегровану цифрову платформу в межах Міноборони. Для цього її виконавці зосередяться на декількох напрямках:

- модернізація інформаційних мереж відповідно до вимог місії МО;
- оптимізація управління IT для підвищення ефективності надання можливостей і забезпечення економії коштів;
- культивація першокласної цифрової робочої сили, готової використовувати новітні технології.

Найближчим часом має бути розроблено та ухвалено план реалізації цієї Стратегії.

МІНОБОРОНИ США НАМАГАЄТЬСЯ ЗАЛУЧИТИ ТИСЯЧІ IT-ФАХІВЦІВ, АЛЕ СТИКАЄТЬСЯ З НЕГНУЧКІСТЮ СИСТЕМИ НАЙМУ

У матеріалі від 26 червня «Знайдіть спосіб утримати кіберпрофесіоналів, каже кадровий гуру Пентагону» висвітлюється проблема Міністерства оборони США з набором десятків тисяч необхідних IT-фахівців. Попри наявність 27 000 вакансій в системі міністерства, їх заповнення стикається з низкою труднощів. Однією з основних проблем є відсутність гнучкості в оплаті праці: досвідчені фахівці можуть отримувати лише трохи більше, ніж новачки, що демотивує висококласних спеціалістів. Іншою проблемою є вимога до фахівців мати вищу освіту.

Головний директор відділу ресурсів і аналізу Міноборони США, Марк Горак, вважає, що цю ситуацію потрібно змінювати. Існує велика кількість молодих кіберталантів, які не мають і, можливо, не матимуть вищої освіти, але їхні навички є вкрай необхідними для армії США.

ПОЛЬЩА ІНВЕСТУЄ 760 МІЛЬЙОНІВ ДОЛАРІВ У КІБЕРЗАХИСТ ЧЕРЕЗ ПОСИЛЕННЯ РОСІЙСЬКОГО ТИСКУ

За словами міністра цифрових технологій країни Кшиштофа Гавковського, Польща збирається витратити майже 760 мільйонів доларів на посилення захисту від триваючих кібератак з росії. Під час прес-конференції 3 червня Гавковський сказав, що Польща знаходиться «на передовій кіберборотьби з росією». Нова програма Cyber Shield, яка коштуватиме уряду три мільярди злотих, спрямована на підвищення стійкості критичної інфраструктури країни та державних служб, додав він.

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

СТІЙКОСТІ НЕДОСТАТНЬО, НАТО МАЄ БУТИ «ПРОАКТИВНИМ» ДЛЯ КІБЕРЗАХИСТУ

Під час виступу на CyCon в Таллінні , керівник відділу кібер- та гібридної політики НАТО Крістіан-Марк Ліфлендер підкреслив: «Союзники по НАТО повинні надати своїм збройним силам можливість зайняти проактивну позицію у кіберпросторі для захисту від кібератак, які можуть перешкодити розгортанню сил під час конфліктів». Цей підхід, що отримав підтримку під час його виступу на Міжнародній конференції з кіберконфліктів, має на меті вийти за межі простої стійкості, яка не стала ефективною у стримуванні супротивників, особливо в умовах активізації російської кіберактивності.

Ліфлендер наголосив на необхідності інтеграції військових зусиль у кіберстратегію НАТО для спільного управління ризиками та запобігання перебоям у критично важливому матеріально-технічному забезпеченні, узгоджуючи зі стратегічною концепцією НАТО, яка визнає кіберпростір сферою постійного протистояння. Ця проактивна позиція розглядається як важлива для формування поведінки супротивника та забезпечення оперативної готовності, що підкреслює необхідність узгоджених дій між членами НАТО, оскільки тривають переговори щодо створення нового кіберцентру в Бельгії.

CISCO СТВОРИТЬ ЦЕНТР КІБЕРБЕЗПЕКИ НА ТАЙВАНІ

Американський виробник мережевого обладнання Cisco заявив 17 червня, що створить центр кібербезпеки в Тайвані та співпрацюватиме з урядом, щоб навчити більше фахівців для роботи в урядовому кібербезпековому секторі.

ANSSI ПРИЄДНАЛАСЬ ДО ТИХООКЕАНСЬКОЇ ОПЕРАТИВНОЇ МЕРЕЖІ КІБЕРБЕЗПЕКИ PACSON

20 червня Французьке агентство кібербезпеки (ANSSI) повідомило, що приєдналось до Тихоокеанської оперативної мережі кібербезпеки PaCSON, яка об'єднує 16 країн тихоокеанського регіону. Мережа заохочує обмін найкращими практиками, обмін інформацією та розвиток можливостей реагування на інциденти. Країнами-членами є: Австралія, Острови Кука, Фіджі, Кірібаті, Маршаллові Острови, Науру, Нова Зеландія, Ніуе, Палау, Папуа-Нова Гвінея, Самоа, Соломонові Острови, Токелау, Тонга, Тувалу та Вануату.

DHS СПІВПРАЦЮЄ З ІНДОНЕЗІЄЮ ДЛЯ ЗМІЦНЕННЯ МОРСЬКОЇ КІБЕРБЕЗПЕКИ В ІНДО-ТИХООКЕАНСЬКОМУ РЕГІОНІ

21 червня видання Industrial Cyber повідомило, що Міністерство внутрішньої безпеки США (DHS) посилює морську кібербезпеку в Індійсько-Тихоокеанському регіоні через партнерство з Індонезією за підтримки інших органів США. Ця співпраця спрямована на зміцнення заходів кібербезпеки, захист критичної морської інфраструктури та підвищення стійкості міжнародної морської транспортної системи. Зусилля включають цілеспрямовані обговорення реагування на інциденти, обмін інформацією та майбутнє двостороннє співробітництво, а також спільні навчання та семінари, проведені з владою Індонезії для покращення кібербезпеки та можливостей реагування на інциденти.

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

ПІВНІЧНА КОРЕЯ ПІДРОБИЛА ЗАСТОСУНОК КОМПАНІЇ GOOGLE, ЩОБ ВИКРАДАТИ ДАНІ ГРОМАДЯН ПІВДЕННОЇ КОРЕЇ

28 червня американська компанія Zscaler, що займається хмарною безпекою, заявила, що викрила кібератаку Північної Кореї із застосуванням підробленого розширення Chrome під назвою TRANSLATEXT. Фальшивий застосунок маскувався під легітимний додаток Chrome для перекладу текстів. Після його встановлення на комп'ютері жертви, зловмисники отримували доступ до адреси електронної пошти та паролів, могли робити знімки екрана та викрадати фрагменти особистих даних у жертв. Швидше за все за атакою стоїть північнокорейська хакерська група Kimsuky.

NSA НАДАЛО ПОРАДИ ЩОДО БЕЗПЕЧНОГО ВИКОРИСТАННЯ МОБІЛЬНИХ ТЕЛЕФОНІВ

1 червня NSA поширило свої рекомендації щодо заходів безпеки, які доцільно вживати всім користувачам мобільних телефонів, аби зменшити загрози їх зараження вірусами чи спрямованим атакам хакерів. До таких порад відноситься: щонайменше раз на тиждень повністю виключати та включати телефон; використовувати не 4, а 6 значні коди блокування екрана; завжди відключати сервіси, якими не користуєшся в цей момент (наприклад, Bluetooth).

РЕБРЕНДОВАНА RANSOMWARE KNIGHT АТАКУЄ УСТАНОВИ ОХОРОНИ ЗДОРОВ'Я ТА БІЗНЕС У ВСЬОМУ СВІТІ

Аналіз штаму програм-вимагачів під назвою RansomHub показав, що він є оновленою та перейменованою версією програми-вимагача Knight, яка сама походить від іншої програми-вимагача, відомої як Cyclops. ПЗ Knight (воно ж Cyclops 2.0) вперше з'явилося в травні 2023 року, використовуючи подвійну тактику вимагання для крадіжки та шифрування даних жертв з метою отримання фінансової вигоди. Він працює на багатьох платформах, включаючи Windows, Linux, macOS, ESXi та Android.

Цю операцію RaaS було закрито наприкінці лютого 2024 року, коли її вихідний код було виставлено на продаж, що підвищило ймовірність того, що вона могла перейти до іншого учасника, який згодом вирішив оновити та перезапустити його під брендом RansomHub.

НІМЕЦЬКИЙ ХДС ЗАЗНАВ ВЕЛИКОЇ КІБЕРАТАКИ

2 червня Християнсько-демократичний союз Німеччини (ХДС) зазнав значної кібератаки, яка змусила партію тимчасово закрити частину своєї IT-інфраструктури. Влада розслідує напад, підозрюючи високопрофесійного актора, але не уточнює масштаб чи виконавців атаки. Міністерство внутрішніх справ Німеччини планує попередити всі партії Бундестагу та вже посилило заходи захисту від цифрових загроз. Політично вмотивовані кібератаки зросли перед виборами в ЄС, часто пов'язані з російськими державними акторами.

ХАКЕР ВИВІВ З ЛАДУ 600 ТИСЯЧ МАРШРУТИЗАТОРІВ ВСЬОГО ЗА 72 ГОДИНИ

Дослідники безпеки з Black Lotus Labs у Lumen Technologies опублікували звіт, у якому детально описано деактивацію сотень тисяч маршрутизаторів у жовтні 2023 року за 72 години. Невідомий хакер зміг зламати понад 600 000 маршрутизаторів інтернет-провайдера Windstream за допомогою шкідливого оновлення ПЗ. Маршрутизатори постійно світилися червоним, перестали працювати та не перезавантажувалися. Вони назавжди вийшли з ладу, і їх довелося замінити. Дослідники вважають, що атака була ініційована за допомогою трояна віддаленого доступу Chalubo. Мотив нападу досі незрозумілий, і жодна держава не була причетна до інциденту.

RANSOMHUB ВЗЯЛА ВІДПОВІДАЛЬНІСТЬ ЗА КІБЕРАТАКУ НА ТЕЛЕКОМУНІКАЦІЙНОГО ГІГАНТА FRONTIER

Відповідальність за квітневу кібератаку на велику телекомунікаційну компанію Frontier взяла група ransomware, яка набирає обертів. 2 червня RansomHub згадала Frontier Communications на сайті, через який вона зливає дані, заявивши, що володіє конфіденційною інформацією понад двох мільйонів людей. Сама ж Frontier Communications повідомила регуляторам, що було викрадено імена та номера соціального страхування 751,895 жителя США.

Швидкий розвиток RansomHub викликає тривогу. З моменту появи на початку цього року рансомвер банда швидко взяла на себе відповідальність за резонансні атаки, включаючи кіберінциденти з Frontier Communications і Change Healthcare. Згідно з дослідженням Symantec, програма-вимагач, як послуга (RaaS) RansomHub, ймовірно, є оновленою та перейменованою версією старішої програми-вимагача Knight.

ТИХООКЕАНСЬКИЙ ОСТРІВ, ПОВ'ЯЗАНИЙ ІЗ ТАЙВАНЕМ, ЗЛАМАЛИ. ЧИ БУЛИ ЦІ ДІЇ ПОЛІТИЧНО МОТИВОВАНИМИ?

2 червня New York Times повідомила, що щойно США фіналізували плани надання Палау, групі з приблизно 350 невеликих островів у Тихому океані, сотні мільйонів доларів допомоги протягом двох десятиліть, острівна держава постраждала від кібератаки, під час якої було викрадено понад 20 000 документів уряду. Палау є однією з небагатьох країн у світі, які визнають Тайвань як незалежну демократію, що змусило лідерів Палау сказати, що напад був організований Китаєм як попередження. Китай відкинув це звинувачення, адже немає доказів причетності Пекіна. Натомість група програм-вимагачів під назвою DragonForce взяла на себе відповідальність за атаку, заявивши, що вона планувала її заради фінансової вигоди. Незалежно від того, яка група стояла за атакою, злом небезпечний для США, оскільки хакери можуть скористатися витоком інформації. Це може дозволити зловмисникам адаптувати складніші фішингові атаки. Викрадені документи можуть становити ризик для інших країн, оскільки вони включають дипломатичні контакти з такими країнами, як США, Японія та Ізраїль.

КІБЕРАТАКА НА МЕДИЧНУ ІНФРАСТРУКТУРУ ЛОНДОНА ПРИЗВЕЛА ДО СКАСУВАННЯ МЕДИЧНИХ ПРОЦЕДУР

На початку червня атака рансомвер вразила великі лікарні Лондона. Це призвело до перенесення понад 800 запланованих операцій і 700 амбулаторних приймань. Особливо атака вплинула на переливання крові. Серед постраждалих – служби первинної медичної допомоги в кількох районах Лондона. Лікарні оголосили про «критичний інцидент», але невідкладна допомога продовжила працювати попри збої. Національна служба здоров'я Великобританії працює з Національним центром кібербезпеки, щоб вирішити цю ситуацію. Цей інцидент стався після недавніх атак програм-вимагачів на інші об'єкти Національної служби здоров'я.

Згодом Кіаран Мартін, колишній керівник Національного центру кібербезпеки Великобританії сказав BBC Radio 4: «Ми вважаємо, що це російська група кіберзлочинців, які називаються Qilin. Вони просто шукають грошей. Навряд чи вони знали, що спричинили такі серйозні збої в первинній медичній допомозі, коли вирушили атакувати компанію». Спочатку Qilin вимагав 50 млн доларів викупу, однак після публічного розголосу і залучення правоохоронних органів Великобританії до вирішення ситуації вимога зникла.

КИТАЙСЬКІ ХАКЕРИ ЗЛАМАЛИ 20 ТИСЯЧ СИСТЕМ FORTIGATE ПО ВСЬОМУ СВІТУ

11 червня Служба військової розвідки та безпеки Нідерландів (MIVD) виявила, що китайська кампанія кібершпигунства, розкрита на початку цього року, має набагато гірші наслідки, ніж вважалося спочатку. Китайські хакери скористалися критичною вразливістю FortiOS/FortiProxy (CVE-2022-42475), щоб розгорнути зловмисне ПЗ на вразливих пристроях Fortigate, заразивши 14 000 систем і націлившись на західні уряди, міжнародні організації та компанії оборонної промисловості. Зловмисне ПЗ, яке використовувалося в кампанії політичного шпигунства, також було виявлено в мережі Міністерства оборони Нідерландів, але його було локалізовано через сегментацію мережі. MIVD виявив, що принаймні 20 000 систем FortiGate було зламано в усьому світі, а складне шкідливе ПЗ Coathanger, яке ухиляється від виявлення та витримує оновлення, передбачає постійний доступ до багатьох систем. Ця кампанія схожа на попередні атаки китайських хакерів на невиправлені пристрої SonicWall.

CDK GLOBAL СТИКНУЛАСЬ З АТАКОЮ ЧЕРЕЗ ЛАНЦЮЖОК ПОСТАЧАННЯ

19 червня компанія CDK Global, яка постачає програмне забезпечення для тисяч автодилерів, зазнала кібератаки, що була реалізована через вразливість в одного із її підрядників (атака через ланцюжок постачання). Компанії довелось вимкнути всі свої системи з метою мінімізації наслідків. CDK Global працює з 15 000 дилерськими центрами, переважно у США та Канаді.

SYMANTEC ПОВ'ЯЗАЛА КІБЕРНАПАД НА АЗІЙСЬКІ ТЕЛЕКОМУНІКАЦІЙНІ КОМПАНІЇ З КИТАЙСЬКИМИ ДЕРЖАВНИМИ ХАКЕРАМИ

Згідно зі звітом, опублікованим компанією Symantec 20 червня, протягом багатьох років, починаючи з 2021, а іноді та раніше, телекомунікаційні компанії в одній неназваній азійській країні були мішенню кіберінструментів, пов'язаних із китайськими шпигунськими групами. Звіт містить детальний опис використовуваних інструментів.

ІНДОНЕЗІЙСЬКИЙ НАЦІОНАЛЬНИЙ ЦЕНТР ОБРОБКИ ДАНИХ ПОСТРАЖДАВ ВІД КІБЕРАТАКИ, ЩО ПОРУШИЛО РОБОТУ УРЯДОВИХ СЛУЖБ

13 червня Національний центр обробки даних Індонезії піддався кібератаці ransomware. Це призвело до перебоїв у наданні державних послуг, вплинувши на роботу аеропортів і поромів країни, а також системи перевірки паспортів. Зловмисники вимагали виплату викупу у вісім мільйонів доларів. Кібератака торкнулася близько 200 державних установ як національного, так і регіонального рівнів. Слід зазначити, що Національний центр обробки даних, який зазнав атаки, є тимчасовим об'єктом, призначеним для використання лише до завершення будівництва центру високого рівня безпеки в Сікаранзі, Західна Ява, який зараз будується. Цей об'єкт матиме рейтинг Tier IV і буде найбезпечнішим у країні, коли він буде працювати. 28 червня президент Індонезії Джоко Відодо наказав провести аудит державних центрів обробки даних після того, як офіційні особи заявили, що для основної маси даних, постраждалих від нещодавньої кібератаки ransomware, не створено резервні копії.

ЯПОНСЬКЕ КОСМІЧНЕ АГЕНТСТВО ЗАЗНАЛО КІЛЬКОХ КІБЕРАТАК, АЛЕ ОФІЦІЙНІ ОСОБИ КАЖУТЬ, ЩО КОНФІДЕНЦІЙНІ ДАНІ НЕ ВИКРАЛИ

24 червня видання Security Week повідомило, що японське космічне агентство JAXA зіткнулося з кількома кібератаками з кінця минулого року. Головний секретар кабінету міністрів Йосімаса Хаясі підтвердив інциденти, зазначивши, що JAXA розслідувала порушення та вимкнула постраждалі мережі. Витоків секретних даних не було, і Японія прагне посилити свої можливості кіберзахисту. Міністр оборони Мінору Кіхара та міністр освіти Масахіто Моріяма повідомили про відсутність збитків від атак. JAXA співпрацює з урядовою командою з кібербезпеки для впровадження профілактичних заходів, продовжуючи успішні космічні місії, включаючи висадку на Місяць і запуск супутників.

НОВІ ПІВНІЧНОКОРЕЙСЬКІ ХАКЕРИ АТАКУВАЛИ АЕРОКОСМІЧНУ ТА ОБОРОННУ КОМПАНІЮ

24 червня видання Cybersecurity News повідомило, що дослідники безпеки виявили складну нову кампанію зловмисного ПЗ, ймовірно пов'язану з північнокорейськими хакерами, націлену на аерокосмічні та оборонні компанії через раніше незадокументований бекдор. Дослідники назвали кампанію Niki. Як приманку її виконавці використовують описи вакансій, щоб здійснити багатоетапну атаку, яка в кінцевому підсумку встановлює потужний бекдор в системи жертви. Бекдор надає зловмисникам віддалений доступ і можливість виконувати команди, завантажувати додаткові корисні дані та вилучати конфіденційні дані.

ЗЛОВМИСНЕ ПЗ VALLEYRAT, ПОВ'ЯЗАНЕ З КИТАЄМ, ПОВЕРТАЄТЬСЯ РАЗОМ З ПЕРЕДОВОЮ ТАКТИКОЮ КРАДІЖКИ ДАНИХ

Дослідники з кібербезпеки виявили оновлену версію шкідливого ПЗ під назвою ValleyRAT, яке поширюється в рамках нової кампанії.
«В останній версії ValleyRAT представив нові команди, такі як створення скріншотів, фільтрація процесів, примусове завершення роботи та очищення журналів подій Windows», – повідомили дослідники Zscaler ThreatLabz Мухаммед Ірфан В. А. та Маніша Рамчаран Праджапаті. Раніше ValleyRAT був задокументований QiAnXin і Proofpoint у 2023 році через фішингову кампанію, націлену на китайськомовних користувачів і японські організації, які поширювали різні сімейства зловмисного ПЗ, наприклад Purple Fox і варіант трояна Gh0st RAT, відомий як Sainbox RAT (він же FatalRAT).

ХАКЕР ОТРИМАВ ДОСТУП ДО ВНУТРІШНЬОГО ІНСТРУМЕНТУ TILE, ЯКИЙ НАДАЄ ПОЛІЦЕЙСЬКИМ ДАНІ ПРО МІСЦЕПЕРЕБУВАННЯ

404 Media повідомило, що хакер зламав платформу підтримки клієнтів, яка використовується компанією Tile, що відстежує місцеперебування, і отримав доступ до даних клієнтів, включаючи імена, адреси, адреси електронної пошти та номери телефонів. Материнська компанія Tile Life360 повідомила, що злочинець спробував вимагати гроші від компанії після крадіжки даних. Компанія додала, що порушення «не включає більш конфіденційну інформацію, таку як номери кредитних карток, паролі або облікові дані для входу, дані про місцеперебування або державні ідентифікаційні номери, оскільки платформа підтримки клієнтів Tile не містила цих типів інформації.

НАЙБІЛЬША ХОРВАТСЬКА ЛІКАРНЯ ЗАЗНАЛА КІБЕРАТАКИ

Університетський лікарняний центр Загреба (KBC Zagreb) зазнав кібератаки, починаючи з вечора 26 червня, що призвело до відключення його інформаційної системи. Хоча всі служби залишались в робочому стані, приймання пацієнтів відбувалось повільніше через неможливість надрукувати медичні звіти, вимагаючи рукописні документи. Служби екстреної допомоги та медичні лабораторії працювали у штатному режимі, доказів витоку даних пацієнтів поки що немає. Незрозуміло чи ця атака була пов'язана з програмним забезпеченням-вимагачем або вона пов'язана з недавніми DDoS-атаками на хорватські урядові та фінансові установи проросійської хакерської групи NoName057(16). Експерти відзначають зростання кількості DDoS-атак на інфраструктуру Хорватії, підкреслюючи необхідність надійного захисту, який регулярно перевіряється.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

NSA ВИПУСТИЛА НОВІ НАСТАНОВИ ЩОДО ПОБУДОВИ СИСТЕМ НА ПРИНЦИПАХ ZERO TRUST

1 червня NSA оприлюднила Інформаційний лист з кібербезпеки (CSI) «Підвищення рівня зрілості Zero Trust в рамках видимості та аналітики». CSI пояснює, як інтегрувати ключові можливості Visibility and Analytics Pillar у структуру Zero Trust. Рекомендовано наступні дії:

- реєструвати всі релевантні дії;
- централізувати інформацію про безпеку та керування подіями;
- регулярно використовувати аналітику безпеки та ризиків;
- проводити аналітику поведінки користувачів;
- інтегрувати розвідку про загрози;
- автоматизувати динамічні політики.

ЧИ Є ДОЦІЛЬНОЮ ПОВНА ЗАБОРОНА НА ПЛАТЕЖІ ЗА RANSOMWARE?

У статті від 10 червня «Чи є доцільною повна заборона на платежі за ransomware?» проводиться огляд поточного стану дискусії в США щодо планів уряду повністю заборонити виплати хакерам, що вдаються до ransomware. Автор статті наводить аргументи обох сторін – як противників такої заборони, так і прихильників. Основним аргументом противників є те, що не всі організації технічно готові до захисту своїх систем від таких атак. Відповідно заборона виплат може зробити для таких організацій в принципі неможливою подальшу діяльність. А якщо це стосується таких секторів як освіта, охорона здоров'я чи промислові системи, то це може створити несподівані виклики суспільній стабільності. На противагу цьому противники жорсткого підходу вказують на те, що протягом останніх років кількість атак ransomware зменшується, в тому числі через те, що жертви відмовляються платити.

ВПЛИВ ШІ НА УПРАВЛІННЯ НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ БУДЕ ЗРОСТАТИ, АЛЕ ДЕЯКІ КЛАСИЧНІ СТРАТЕГІЇ ЗАЛИШАТЬСЯ АКТУАЛЬНИМИ – НОВИЙ ЗВІТ CSIS

10 червня експерти CSIS оприлюднили свою доповідь «Алгоритмічна стабільність: як ШІ може сформувати майбутнє стримування». Це дослідження базується на серії симуляцій кризи (war game), аналізуючи, як AI/ML сформує майбутнє стримування. Три ключових висновки дослідження:

- держави інтегруватимуть ШІ і машинне навчання (ML) у процес управління національною безпекою аби отримати переваги в прийнятті рішень перед конкурентами;
- нова технологія змінить характер, але не природу державного управління та стратегування у цій сфері (держави, як і раніше, поєднуватимуть дипломатію, економічний примус і кампанії впливу з погрозами військової сили, щоб дати сигнал суперникам і заспокоїти союзників);
- інформація про можливості AI/ML (своїх та ворожих) впливатиме на те, як держави керуватимуть ескалацією. Прогалини в розвідувальних даних щодо алгоритмів супротивника збільшують ймовірність ескалації, але лише тоді, коли держави перетнуть рубікон і борються нижче ядерного порогу.

ЗЛОВМИСНИКИ З UNC3944 ВДАЮТЬСЯ ДО ФІЗИЧНИХ ПОГРОЗ ТЕХНІЧНИМ ФАХІВЦЯМ АБИ ОТРИМАТИ ДАНІ ДЛЯ ЗЛАМУ СИСТЕМ – РОЗСЛІДУВАННЯ MANDIANT

17 червня кібербезпекова компанія Mandiant оприлюднила своє дослідження щодо діяльності зловмисної групи UNC3944. За даними Mandiant, злочинне угруповання (яке раніше покладалось на ransomware) наразі більше сконцентрувалось на інструментах соціальної інженерії. Відмінністю від інших схожих груп є тактика нагнітання страху, щоб отримати доступ до облікових даних жертви. Це містить в собі погрози доксінгу особистої інформації (збір та подальше публічне поширення чутливої персональної інформації), фізичні шкоди жертвам та їхнім родинам, а також поширення компрометуючих матеріалів. Відомо про спроби зловмисників атакувати інструмент управління гібридною хмарою vSphere від VMware та Azure від Microsoft. Метою обох заходів було отримання можливості UC3944 для створення віртуальних машини всередині організації та використання їх для своїх протиправних дій.

НАЦІОНАЛЬНИЙ НАУКОВИЙ ФОНД США ПРОПОНУЄ ПРОВОДИТИ ТТХ ЩОДО МОЖЛИВИХ КІБЕРЗАГРОЗ У КОСМОСІ

17 червня Національний науковий фонд США оприлюднив доповідь про можливі кібератаки в космосі. У звіті описано кілька можливих сценаріїв таких кібератак, зокрема проведення DDoS-атаки, відключення електронних дверей у місячному поселенні, захоплення мешканців в середині фізичної структури тощо. Дослідники Фонду сподіваються, що запропоновані ними сценарії стануть основою для проведення ТТХ відповідальними державними структурами та їх підрядниками.

CCDCOE ОПУБЛІКУВАВ ПОЗИЦІЙНИЙ ДОКУМЕНТ ЩОДО КІБЕРДИПЛОМАТІЇ

14 червня Центр передового досвіду НАТО з кібербезпеки (CCDCOE) опублікував позиційний документ щодо кібердипломатії. В документі проводиться огляд процесу розвитку кібердипломатії, її визначення, та як вона застосовується у зв'язку з критичними питаннями кібербезпеки та кіберзахисту. У документі робиться висновок про необхідність адаптації урядів до реалій кібердипломатії, а також про підвищення важливості ролі кібердипломатів під час війни.

МІНІСТЕРСТВО ВНУТРІШНЬОЇ БЕЗПЕКИ США, ДЕТАЛЬНО ОПИСАЛО, ЯК ШІ МОЖЕ ПОСИЛИТИ БІОЛОГІЧНІ ТА ХІМІЧНІ ЗАГРОЗИ

У звіті Міністерства внутрішньої безпеки наголошується, що хоча ШІ може допомогти зловмисникам у розробці хімічної, біологічної, радіологічної та ядерної зброї, він також може допомогти захисникам у пом'якшенні цих загроз. У звіті, підготовленому згідно з указом від 2023 року, підкреслюється ризик, який створюють інструменти ШІ в поєднанні з поточними прогалинами в нормах біологічної та хімічної безпеки США. Він рекомендує створити настанови щодо захисту конфіденційних даних, посилити нагляд за доступом до віддаленої лабораторії та розробити федеральні настанови щодо використання ШІ в біологічних і хімічних дослідженнях. Звіт також закликає до консенсусу між регуляторними органами щодо управління технологіями ШІ, просування культури відповідальності в природничих науках та вивчення потенціалу ШІ у виявленні загроз і реагуванні на них.

5. КРИТИЧНА ІНФРАСТРУКТУРА

ПРЕДСТАВНИКИ ОКІ, ЩО МАЮТЬ СПРАВУ З ОТ, ЗАНЕПОКОЄНІ ФРАГМЕНТАРНІСТЮ АМЕРИКАНСЬКОЇ НОРМАТИВНОЇ БАЗИ З КІБЕРБЕЗПЕКИ

ONCD, прагнучи поліпшити нормативне регулювання сфери кібербезпеки для OKI, стикнувся з консолідованою позицією тих представників OKI, які безпосередньо пов'язані з OT. Останні вказують на те, що наявні спроби держави встановлювати все нові регуляторні вимоги до безпеки OT мають фрагментарний характер, не враховують об'єктивну специфіку OT (часто це технології створені на замовлення, а також створені дуже давно і в них не передбачено можливості засобів кіберзахисту), вимагаються від компаній технічних вимог, які насправді не ведуть до поліпшення кібербезпеки, а також суперечать галузевим вимогам та стандартам. Також представники OKI вказують на брак підтримки регуляторів в процесі впровадження нових вимог, що значно ускладнює цей процес.

RAND CORPORATION ПІДГОТУВАЛА КОМПЛЕКСНИЙ ЗВІТ ЩОДО БЕЗПЕКИ У СЕМИ СЕКТОРАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ США

11 червня RAND опублікувала звіт про загрози та небезпеки для критичної інфраструктури США, концентруючись на кібернетичних, фізичних, вікових та екологічних загрозах для кожного сектора. Серед висновків:

- критична інфраструктура США тісно інтегрована між собою, що може призвести до важких каскадних ефектів у випадку вдалої атаки;
- деякі сектори недостатньо вкладають у безпеку своїх процесів, що ставить під загрозу безпеку громадян;
- об'єкти критичної інфраструктури не хочуть ділитись інформацією про свої системи та їх стан, побоюючись репутаційних викликів та посилаючись на об'єктивні юридичні обмеження (в тому числі щодо конкурентної боротьби).

NSA ПОПЕРЕДЖАЄ ПРО ЗРОСТАННЯ КІЛЬКОСТІ КІБЕРАТАК НА ВІЙСЬКОВО-ПРОМИСЛОВИЙ СЕКТОР США

25 червня під час форуму TechNet Cyber керівник NSA Тімоті Хо звернув увагу на помітну тенденцію зловмисних груп з Китаю та росії до атак на американський військово-промисловий сектор. За різними оцінками мова йде про 160 000 компаній (американських та іноземних), у яких працює 9% робочої сили США. Міністерство оборони зі свого боку вважає, що найкращою стратегією захисту стане впровадження Zero Trust та автоматизація (на базі ШІ) процесу кіберзахисту. Водночас навіть в межах Міністерства оборони США існує думка, що Міноборони не достатньо швидко рухається до Zero Trust – новий керівник Офісу управління портфелем Zero Trust (знаходиться у підпорядкуванні CISO MO США) заявив, що буде домагатись надання йому більш серйозних повноважень для того, аби чинити тиск на власну організацію з метою швидшого впровадження Zero Trust.

НЕВІДОМІ ЗЛОВМИСНИКИ ОТРИМАЛИ ДОСТУП ДО ІНСТРУМЕНТУ CSAT РОЗРОБЛЕНОГО І ПІДТРИМУВАНОГО CISA

25 червня CISA звернулась до всіх користувачів Chemical Security Assessment Tool (CSAT) з проханням посилити свої заходи безпеки через виявлений несанкціонований доступ до цього інструменту. CSAT – це спеціальний інструмент, що використовується підприємствами (близько 300), де зберігаються специфічні хімічні речовини, у кількостях, що дорівнюють або перевищують певний поріг. Ці хімікати з яких можуть бути виготовлені вибухівка та зброя. Зловмисники використали вразливість в Ivanti Connect Secure аби отримати доступ до цього інструменту, однак наразі у CISA немає підтверджень, що зловмисникам вдалось отримати якісь дані з системи. Крім того, всі дані в системі зашифровані.

«ПАРОЛІ ЗА ЗАМОВЧУВАННЯМ» СТАНОВЛЯТЬ ЗНАЧНУ ЧАСТИНУ КІБЕРРИЗИКІВ ДЛЯ ICS/OT

Стаття «Поширеність і вплив уразливості пароля в ICS/OT» від 13 червня зосереджується на проблемі неефективної політики щодо паролів в секторах (зокрема, коли заводські паролі не змінюються кінцевими користувачами чи паролі взагалі «зашиті» в деяких системах), які багато працюють з OT. Зокрема показано, як протягом останнього року використання «паролів за замовчуванням» призвело до декількох серйозних інцидентів (в тому числі у сфері водопостачання США). Експерти вказують на об'єктивну специфіку OT, що особливо ускладнює там правильну парольну політику. Наприклад, OT продукти часто створювались для довгострокової, ізольованої роботи. Відповідно там не передбачалась зміна паролів і взагалі кібербезпека даних, які там функціонують. В багатьох випадках для виробників OT продуктів кібербезпека залишається поза пріоритетом діяльності, хоча навіть обов'язкова вимога виробника до кінцевого користувача змінити базовий пароль могла б істотно поліпшити кібербезпеку в цих секторах.

6. АНАЛІТИЧНІ ОЦІНКИ

В США ВСЕ ЩЕ НЕ ЗАПОВНЕНО 500 ТИСЯЧ ВАКАНСІЙ КІБЕРФАХІВЦІВ – ОФІС НАЦІОНАЛЬНОГО КІБЕРДИРЕКТОРА США

25 червня помічник національного кібердиректора США Сієу Мо опублікував матеріал, в якому вказує на позитивні зрушення у сфері підготовки кадрів для сфери кібербезпеки, яких вдалось домогтись завдяки реалізації Національної стратегії кіберосвіти та робочої сили. Водночас він підкреслює, що в США все ще залишається 500 тисяч незаповнених вакансій у сфері кібербезпеки, що робить США вразливою перед кібератаками.

MITRE ПІДГОТУВАЛА РЕКОМЕНДАЦІЇ НОВОМУ ПРЕЗИДЕНТУ США ЩОДО ПРІОРИТЕТІВ У КІБЕРБЕЗПЕКОВІЙ ПОЛІТИЦІ

6 червня MITRE Corporation оприлюднила набір стратегічних рекомендацій для майбутнього президента США щодо державної політики у сфері кібербезпеки. MITRE концентрується на чотирьох ключових рекомендаціях:

- посилити заходи із захисту критичної інфраструктури;
- повністю перевести федеральний уряд на Zero Trust та SBOM;
- інтенсивніше готуватись до ери квантових обчислень;
- уточнити та зміцнити ролі;
- обов'язки ключових кіберстейкхолдерів.

TRELLIX CYBERTHREAT REPORT ЗА ПЕРШЕ ПІВРІЧЧЯ 2024 РОКУ

11 червня кібербезпекова компанія Trellix оприлюднила свій звіт про стан з кіберзагрозами у першій половині 2024 року. В ньому підкреслюється шість основних тенденцій:

- Китай і росія збільшують кількість атак (68,3% усіх виявлених кібератак пов'язано з Китаєм);
- зростання кількості випадків шахрайства на тему американських виборів;
- зміни в екосистемі програм-вимагачів (найбільші загрози – сектору транспорту та судноплавства, поява самозванців, що видають себе за LockBit);
- активне застосування шкідливого ПЗ Terminator для обходу EDR (на думку експертів поява інструменту пов'язана з російсько-українською війною);
- використання GenAI кіберзлочинцями.

ЛИШЕ ПРИБЛИЗНО 5% АТАК НА MFA КОРИСТУВАЧІВ Є ВДАЛИМИ – ДАНІ CISCO TALOS

18 червня експерти Cisco Talos оприлюднили результати свого поглибленого дослідження щодо зростаючих кібератак зловмисників проти систем MFA. Основний акцент дослідження – на атаках типу push spray (надсилання фальшивих push повідомлень як частини процесу ідентифікації користувачів MFA). Дослідивши 15 тисяч таких атак за період з червня 2023 року по травень 2024 року, дослідники прийшли до висновку, що лише 5% таких атак досягають успіху. Водночас ті п'ять відсотків користувачів, які все ж натискають на фальшиве повідомлення роблять це здебільшого буквально з 3-5 спроби зловмисника, і лише в окремих випадках зловмисникам довелось надсилати до 60 таких повідомлень аби досягти результату.

ДЕТАЛІЗАЦІЯ ПРОГНОЗУ ЗАГРОЗ ВІД SAAS 2024 РОКУ

На початку 2024 року компанія Wing Security опублікувала звіт про стан безпеки SaaS, розповідаючи про нові загрози та найкращі практики в області SaaS. В середині року, кілька передбачень звіту про загрози SaaS вже виявилися точними. У статті компанія переглядає свої прогнози з початку року, демонструє реальні приклади цих загроз у дії та пропонує практичні поради та найкращі практики, які допоможуть запобігти подібним інцидентам у майбутньому.

КІБЕРЗАГРОЗИ СЕКТОРУ ПРОФЕСІЙНИХ ПОСЛУГ У НОВОМУ ЗВІТІ TRUSTWAVE SPIDERLABS

26 червня компанія Trustwave оприлюднила дослідження «Ландшафт професійних послуг за 2024 рік» (до таких послуг вони віднесли консалтингові, бізнес-консалтингові, управлінські, бухгалтерські та юридичні послуги). Основні висновки:

- ransomware – ключова загроза (у 2023 році щонайменше 142 компанії з цієї категорії стали жертвами злочинців, і атак стає більше, адже саме ці компанії часто мають ресурси для виплати викупів);
- кіберзлочинці все частіше націлюються на перевірених сторонніх постачальників, яких використовують професійні послуги та юридичні фірми;
- перехід на нові технології (в тому числі хмарні) не завжди відбувається із дотриманням всіх правил, а отже збільшує поверхню атак для компаній.

ЕЛЕКТРИКА ТА НАПРУГА: ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ВІЙСЬКОВОЇ ЕЛЕКТРИФІКАЦІЇ

Оскільки західні збройні сили, зокрема США, Німеччини, Франції, Великобританії та Австралії, переходять на електромобілі у рамках стратегій декарбонізації та модернізації, вони стикаються зі значними проблемами кібербезпеки. Зростаюча комп'ютеризація та зв'язок між транспортними засобами та зарядною інфраструктурою створюють нові вразливості, якими зловмисники можуть скористатися для збору розвідувальних даних або зриву операцій.
Ці загрози варіюються від злому бортових систем до компрометації зарядних станцій, що потенційно може призвести до шпигунства, знерухомлення транспортних засобів або дестабілізації електромереж. Щоб пом'якшити ці ризики, військові повинні прийняти надійні заходи кібербезпеки, включаючи принципи безпеки за проєктом, червоне об'єднання та шифрування даних, а також забезпечити кіберстійкість за допомогою комплексного навчання та планування на випадок непередбачених ситуацій.

ШПИГУНСЬКА ГРУПА SNEAKYCHEF АТАКУЄ ДЕРЖАВНІ УСТАНОВИ ЗА ДОПОМОГОЮ SUGARGH0ST ТА ІНШИХ МЕТОДІВ ЗАРАЖЕННЯ

У звіті, виданому 21 червня, Cisco Talos описує кампанію вірогідно китайського актора-загрози SneakyChef, який використовував SugarGh0st RAT для атак на державні установи в Анголі, Індії, Казахстані, Латвії, Саудівській Аравії та Туркменістані. Зловмисне ПЗ було доставлено через фішингові електронні листи з добре створеними документами-приманками, які видавали себе за різні урядові організації.

СІЛЬСЬКІ ЛІКАРНІ ОСОБЛИВО ВРАЗЛИВІ ДО ПРОГРАМ-ВИМАГАЧІВ – ЗВІТ

Новий звіт аналітичного центру CSC 2.0 попереджає, що сільські лікарні залишаться найбільш вразливими до атак програм-вимагачів, якщо не буде зроблено значні інвестиції в кібербезпеку. Здатність сектору охорони здоров'я США захищатися від майбутніх кібератак значною мірою залежить від федерального фінансування Конгресу. Нещодавні атаки програм-вимагачів, як-от атаки на Ascension і Change Healthcare, порушили обслуговування пацієнтів і підкреслили серйозний вплив на системи охорони здоров'я.

Сільські лікарні, які часто є критично важливими закладами доступу з обмеженими ресурсами, знаходяться під особливою загрозою. У звіті рекомендовано збільшити фінансування для Департаменту охорони здоров'я та соціальних служб, покращити навчання з кібербезпеки та плани на випадок непередбачених обставин для догляду за пацієнтами. Він також пропонує визначити більше організацій охорони здоров'я як «системно важливі» та розв'язати проблему залежності від застарілих комп'ютерних систем. Попри зусилля адміністрації Байдена, атаки програм-вимагачів зростають, причому сектор охорони здоров'я є найбільш цільовим серед секторів критичної інфраструктури.

ДЕВ'ЯТЬ ВИСНОВКІВ ІЗ РОЗСЛІДУВАННЯ ЗБОЇВ У СФЕРІ КІБЕРБЕЗПЕКИ MICROSOFT ВІД PROPUBLICA

Нещодавнє розслідування ProPublica показало, що співробітник Microsoft неодноразово намагався переконати компанію усунути недоліки за роки до злому SolarWinds – і що компанія на кожному кроці відкидала його занепокоєння. Стаття, опублікована журналістами-розслідувачами, містить основні висновки.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

НКЦК ВИСТУПИВ ПАРТНЕРОМ PARIS CYBER SUMMIT

Національний координаційний центр кібербезпеки став партнером Паризького кібербезпекового саміту Paris Cyber Summit, що відбувся 3-5 червня у Франції. Під час заходу обговорювалися останні досягнення та виклики у сфері кібербезпеки, зокрема вплив штучного інтелекту на кіберполітику. Учасники включали урядовців європейських країн, експертів галузі та представників бізнесу.

Керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України, секретар НКЦК Наталія Ткачук у своєму виступі поділилася уроками, які Україна здобула у кібервійні та наголосила на тому, що росія вже розпочала неприховану кіберагресію проти країн ЄС та НАТО. Також відбулася робоча зустріч з Командувачем Французького кіберкомандування генерал-майором Аймеріком Боннемезоном, яка підкреслила важливість двостороннього співробітництва та обміну досвідом між країнами для боротьби з кіберзагрозами, зокрема з боку російської федерації.

УКРАЇНА ВПЕРШЕ ВЗЯЛА УЧАСТЬ У ЄВРОПЕЙСЬКИХ КІБЕРНАВЧАННЯХ CYBER EUROPE

Основною темою навчань стала готовність до масштабних кібератак на енергетичну інфраструктуру ЄС. Дводенна інтенсивна програма, підготовлена ENISA, зібрала понад 1000 найкращих спеціалістів публічного і приватного сектору з 30 країн.

Представники НКЦК разом з американською CISA у цих навчаннях брали участь як спостерігачі. За результатами візиту в Афіни досягнуто домовленості про поглиблення співпраці з ENISA, зокрема долучення України до розробки сценарію, планування та участі у Cyber Europe 2026.

НКЦК ПРЕЗЕНТУВАВ НОВИЙ ІНСТРУМЕНТ ДЛЯ МОНІТОРИНГУ ВИКОНАННЯ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ CYBERTRACKER

Національний координаційний центр кібербезпеки спільно з Міністерством цифрової трансформації України та Держспецзв'язку провів тренінг 13 червня 2024 року для фахівців профільних міністерств, обласних військових адміністрацій та суб'єктів кібербезпеки, які здійснюють моніторинг та звітування виконання Стратегії кібербезпеки України. Захід був присвячений автоматизації моніторингу виконання Стратегії кібербезпеки України за допомогою порталу CyberTracker.

Впровадження порталу дозволить аналізувати вплив активностей Стратегії, інформувати громадськість та міжнародних партнерів про прогрес, а також спростити процедуру звітування щодо виконання Стратегії. Портал розроблено за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України».

МІНЦИФРА ПРЕЗЕНТУВАЛА БІЛУ КНИГУ ЩОДО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УКРАЇНІ

Завдяки документу компанії зможуть зрозуміти, як підготуватися до майбутнього законодавства у сфері ШІ та створювати продукти, безпечні для громадян. Це дозволить українським компаніям ставати більш конкурентоспроможними та виходити на міжнародні ринки. А для держави це можливість інтегруватися до ЄС, синхронізувавши своє законодавство у сфері ШІ з європейським.

Серед інструментів, які держава надасть компаніям, – загальні та секторальні рекомендації для різних сфер і аспектів використання ШІ: від освіти та журналістики до порад з обробки персональних даних. Крім рекомендацій, планується створити добровільні кодекси поведінки, платформу юридичної допомоги для бізнесу, регуляторну пісочницю для тестування високотехнологічних продуктів на відповідність майбутнім вимогам тощо.

BRAVE1, НАТО ТА DEFENSE INNOVATION UNIT УПЕРШЕ В ІСТОРІЇ ПРОВЕЛИ ФОРУМ ОБОРОННИХ ІННОВАТОРІВ НАТО-УКРАЇНА

NATO-Ukraine Defense Innovators Forum – перший спільний захід у сфері оборонних технологій, який організували НАТО, Підрозділ оборонних інновацій Міністерства оборони США (Defense Innovation Unit – DIU), кластер Brave1, Рада Україна — НАТО та Міністерство національної оборони Польщі. Форум об'єднав близько 400 учасників у сфері оборонних технологій та інновацій з понад 15 країн.

Форум містив панельні дискусії, хакатон та зустрічі для розширення контактів розробників з інвесторами. Ключові теми – розвиток оборонних інновацій України та союзників в НАТО, виклики, з якими стикаються розробники обох сторін, перспективи інвестування в український defense tech, плани співпраці в оборонно-технологічній сфері.

НАТАЛІЯ ТКАЧУК: ПОБУДОВА КІБЕРСТІЙКОСТІ ТА НАДАННЯ ВІДСІЧІ АГРЕСОРУ – СПІЛЬНЕ З КРАЇНАМИ ЄС ЗАВДАННЯ

Секретар НКЦК Наталія Ткачук взяла участь у Європейському діалозі з управління Інтернетом (EuroDig), що стартував 17 червня у Вільнюсі. Головною темою заходу було «Баланс інновацій та регулювання». Під час панельної дискусії на тему «Один за всіх, усі за одного: роль співпраці для підвищення кіберстійкості в Європі» учасники обговорили різноманітні аспекти співробітництва для підвищення європейської кіберстійкості.

Секретар НКЦК поділилася прикладами взаємодії України на міжнародному рівні та кейсами державно-приватного партнерства. Вона підкреслила, що росія продовжуватиме кіберагресію як проти України, так і проти країн ЄС. Тому побудова кіберстійкості та надання відсічі агресору є спільним завданням України та країн ЄС.

АНДРІЙ СИБІГА ПРОВІВ ЗУСТРІЧ ІЗ ЗАСТУПНИКОМ СЕКРЕТАРЯ З ПИТАНЬ ІНФОРМАЦІЇ ТА КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ФІЛІППІН ДЖЕФРІ ЯН ДАЄМ

7 червня під час робочого візиту першого заступника міністра закордонних справ України Андрія Сибіги до Республіки Філіппіни відбулася зустріч із заступником секретаря з питань інформації та комунікаційних технологій Філіппін Джефрі Ян Даєм. Сторони обговорили спільні виклики у галузях кібербезпеки та електронного урядування.

Українська сторона поділилася досягненнями у впровадженні цифрових технологій галузі запровадження цифрових технологій в практики державного управління і надання послуг громадянам: платформи Дія, Prozzoro, електронні банківські послуги, запровадження дистанційної освіти. У сфері боротьби з кіберзлочинністю Україна запропонувала укласти меморандум про обмін інформацією між відповідними відомствами. Сторони також обговорили співпрацю в рамках багатосторонніх механізмів взаємодії.

ДЕРЖСПЕЦЗВ'ЯЗКУ ВЗЯЛИ УЧАСТЬ У NICE CONFERENCE & EXPO

Заступник голови Держспецзв'язку Олександр Потій під час виступу на міжнародній конференції NICE Conference & Expo у Далласі (США) зазначив, що впровадження якісних професійних стандартів та ефективного процесу сертифікації кіберфахівців є одними з основних передумов розвитку потужного кадрового потенціалу України.

Захід був присвячений питанням розбудови кадрового потенціалу з кібербезпеки. У ході однієї зі спеціалізованих дискусій в рамках заходу, Олександр Потій також поділився досвідом України у посиленні кіберстійкості, за напрямками, в яких Держспецзв'язку докладає зусиль.

КІБЕРБЕЗПЕКА ТА ПРОТИДІЯ ДЕЗІНФОРМАЦІЇ РФ У СПОРТИВНІЙ СФЕРІ: У КИЄВІ ВІДБУВСЯ НАЦІОНАЛЬНИЙ КЛАСТЕР КІБЕРБЕЗПЕКИ

27 червня 2024 року в Києві відбувся 28-й Національний кластер кібербезпеки на тему «Червона картка кіберзагрозам та фейкам: виклики та рішення для молоді і спорту». Захід організовано НКЦК України спільно з Міністерством молоді та спорту, CRDF Global в Україні за підтримки Держдепартаменту США. У ньому взяли участь понад сто учасників, включаючи представників державного і приватного сектору, спортивних асоціацій, міжнародних організацій та громадськості.

Під час заходу було обговорено питання важливості захисту спортивної сфери від кіберзагроз, особливо в умовах зростаючої цифровізації, та важливість протидії інформаційним операціям з боку рф у спортивному контексті. Окрему увагу було приділено популяризації теми кібербезпеки серед молоді та їхнього залучення до відповідних освітніх програм.

КІБЕРПОЛІЦЕЙСЬКІ ПРОВЕЛИ ЗУСТРІЧІ З УКРАЇНСЬКИМИ ШКОЛЯРАМИ

Поліцейські Запорізької, Чернігівської, Кіровоградської, Волинської та Закарпатської областей розповіли учням про поширені небезпеки в онлайн-середовищі, зокрема про різновиди кібербулінгу, а також пояснили важливість кібергігієни, як дієвого способу захисту від цих негативних явищ. Правоохоронці розповіли дітям про кібербулінг та застерегли від інших форм онлайн-загроз, зокрема кібергрумінгу. Крім цього, поліцейські також розповіли слухачам про проєкт «Брама» та важливість дотримання кібергігієни та захисту персональних даних, особливо в умовах воєнного стану.

УРЯД СХВАЛИВ ЗАВДАННЯ НАЦІОНАЛЬНОЇ ПРОГРАМИ ІНФОРМАТИЗАЦІЇ

Це дасть змогу розбудувати сучасну інформаційну інфраструктуру, впроваджувати цифрові технології, посилити кіберзахист. Зокрема, серед завдань НПІ: впровадження цифрових антикорупційних інструментів, створення сучасної інформаційної інфраструктури, забезпечення ефективного функціонування інформаційної системи правосуддя, інформатизація сфер охорони здоров'я, освіти, науки тощо.

Загалом, глобальне завдання Національної програми інформатизації спрямоване на продовження цифрових трансформаційних процесів у державі та створення цифрової держави загалом. Одним із ключових напрямів НПІ є виконання заходів Державної антикорупційної програми на 2023–2025 роки.

ДЕРЖСПЕЦЗВ'ЯЗКУ ПРЕЗЕНТУВАЛА НОВІ ТЕХНІЧНІ РІШЕННЯ ДЛЯ ЗАХИСТУ ДЕРЖУСТАНОВ ВІД DDOS-АТАК

Держспецзв'язку презентувала представникам державних органів нові технічні рішення для захисту державних установ від DDoS-атак. Під час презентації представники Держспецзв'язку продемонстрували можливості програмної продукції та сервісної підтримки компаній Radware та Akamai Technologies, що розгорнуті в Державному центрі кіберзахисту. Ці рішення забезпечують ефективне виявлення та блокування різних типів кіберзагроз та розширений моніторинг і аналіз трафіку.

ПЕРШИЙ В УКРАЇНІ КВАЛІФІКАЦІЙНИЙ ЦЕНТР ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА КІБЕРБЕЗПЕКИ РОЗПОЧАВ СЕРТИФІКАЦІЮ СПЕЦІАЛІСТІВ

20 червня Державна служба спеціального зв'язку та захисту інформації України відкрила перший Кваліфікаційний центр інформаційних технологій та кібербезпеки. Його мета – впровадження сучасної системи професійної сертифікації кіберспеціалістів, яка дозволить узгодити відповідність знань, навичок та компетенцій фахівців з кібербезпеки із нинішніми потребами ринку в Україні.

Уже зараз фахівці можуть підтвердити свої навички та компетенції у Кваліфікаційному центрі за двома новими професійними стандартами у сфері кібербезпеки – «Розробник безпеки інформаційних систем» та «Адміністратор безпеки мережі та систем». В подальших планах Кваліфікаційного центру ДержНДІ розширення акредитаційного переліку ще на 9 кваліфікацій. Серед них: «Аудитор системи менеджменту інформаційної безпеки», «Фахівець з реагування на інциденти кібербезпеки» тощо.

ДЕРЖСПЕЦЗВ'ЯЗКУ ЗАТВЕРДИЛА ВИМОГИ ДО АУДИТОРІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Державна служба спеціального зв'язку та захисту інформації України затвердила вимоги до аудиторів інформаційної безпеки на об'єктах критичної інфраструктури та порядок їх атестації (переатестації).

Цей наказ розроблений відповідно до постанови Кабінету Міністрів України від 24.03.2023 № 257 «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури». Він встановлює ряд вимог до осіб, які планують отримати право проводити аудит інформаційної безпеки на об'єктах критичної інфраструктури. Повний текст за посиланням: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspec-zv-yazku-vid-30-04-2024-228-pro-zatverdzhennya-vimog-do-auditoriv-informaciinoyi-bezpe-ki-na-ob-yektakh-kritichnoyi-infrastrukturi-ta-poryadku-yikh-atestaciyi-pereatestaciyi.

СБУ ВИКРИЛА БОТОФЕРМИ, ЯКІ ДОПОМАГАЛИ РФ «РОЗГАНЯТИ» ФЕЙКИ КРЕМЛЯ ТА ЗЛАМУВАТИ ТЕЛЕФОНИ УКРАЇНСЬКИХ ВОЇНІВ

Служба безпеки нейтралізувала дві ботоферми, які діяли на Житомирщині та у Дніпрі. Фігуранти допомагали спецслужбам рф зламувати телефони українських захисників та поширювати кремлівську пропаганду.
На Житомирщині викрито зловмисницю, яка реєструвала віртуальні номери та анонімні акаунти в Telegram для російських спецслужб. Вона продала понад 600 мобільних номерів, які використовувалися для зламу телефонів українських військових через фішингові розсилки.

У Дніпрі затримали чоловіка, який зареєстрував майже 15 тисяч фіктивних акаунтів у соцмережах і месенджерах, продаючи їх на форумах даркнету, де основними покупцями були представники рф. За обома фактами тривають розслідування.

ПОЛІЦЕЙСЬКІ ЛІКВІДУВАЛИ ДІЯЛЬНІСТЬ БОТОФЕРМИ, З ЯКОЇ 23-РІЧНИЙ ОДЕСИТ ОТРИМУВАВ ПРИБУТОК В РУБЛЯХ

Зловмисника підозрюють у несанкціонованому втручанні в роботу електронних комунікаційних мереж, вчиненому за попередньою змовою з іншими особами. Йому загрожує до п'яти років позбавлення волі. Хлопець від листопада 2022 року по липень 2023 року незаконно втручався в роботу українського мобільного оператора, змінюючи IMEI для SIM-карток та надаючи їх в оренду онлайн-сервісам віртуальних номерів.

Правопорушник забезпечив функціонування ботоферми та співпрацював з російськими платформами, за що отримував винагороду в рублях. Замовники використовували анонімні номери для створення фейкових акаунтів, фішингових розсилок та поширення пропаганди.

У ЛЬВОВІ ПРАВООХОРОНЦІ ВИКРИЛИ ДВОХ БРАТІВ, ЯКІ СТВОРЮВАЛИ ДЛЯ ПРОДАЖУ ФІШИНГОВІ САЙТИ

Як встановили правоохоронці, підозрювані для продажу створювали в мережі Інтернет фішингові сайти та шкідливе програмне забезпечення, що призначене для несанкціонованого втручання в роботу інформаційних (автоматизованих) систем та яке давало доступ до персональних даних громадян. Слідчі повідомили зловмисникам про підозру у вчиненні кримінального правопорушення, їм загрожує позбавлення волі на строк до трьох років.

ПОЛІЦЕЙСЬКІ ВИКРИЛИ ПОСОБНИКА РОСІЙСЬКИХ ХАКЕРІВ, ЯКІ АТАКУВАЛИ ПРОВІДНЕ ПІДПРИЄМСТВО У НІДЕРЛАНДАХ ТА БЕЛЬГІЇ

Кіберполіцейські та слідчі Нацполіції встановили особу киянина, який на замовлення членів російського хакерського угруповання маскував вірус-шифрувальник під виглядом безпечних файлів. Приховану програму хакери рф використали для втручання в роботу комп'ютерних мереж іноземного підприємства.

Послугами киянина за винагороду у криптовалюті скористалася одна з російських хакерських груп для маскування віруса-шифрувальника Conti-malware. А наприкінці 2021 року члени угруповання інфікували прихованим шкідливим програмним забезпеченням комп'ютерні мережі підприємства у Нідерландах та Бельгії. У результаті цих дій вони стали непридатні до використання. Хакери вимагали сплатити викуп за розшифрування комп'ютерів.

У ході розслідування кіберполіцейські встановили причетність зловмисника до російських хакерських угруповань LockBit та Conti. Йому загрожує до 15 років позбавлення волі.

CERT-UA РАЗОМ ІЗ ЦЕНТРОМ КІБЕРБЕЗПЕКИ ЗСУ ВИЯВИЛА ТА ДОСЛІДИЛА АКТИВНІСТЬ УГРУПОВАННЯ UAC-0020 (VERMIN), СПРЯМОВАНУ ПРОТИ СИЛ ОБОРОНИ УКРАЇНИ

Діяльність угруповання Vermin ведеться співробітниками силових відомств тимчасово окупованого Луганська. Остання активність зловмисників була зафіксовано у березні 2022 року. Цього разу вони використовували шкідливе програмне забезпечення SPECTR для викрадення документів, файлів, паролів та іншої інформації. Також використовувався штатний функціонал синхронізації легітимного програмного забезпечення SyncThing.

Активність цього угруповання відстежується CERT-UA за ідентифікатором UAC-0020. Детальніше про зловмисну діяльність та індикатори загроз UAC-0020 у матеріалі CERT-UA.

ХАКЕРИ АТАКУЮТЬ ПРАЦІВНИКІВ ДЕРЖАВНОГО ТА ОБОРОННОГО СЕКТОРУ ЧЕРЕЗ SIGNAL

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, що діє попередила про цільові кібератаки проти державних службовців, військових і представників оборонних підприємств України. Для своїх цілей зловмисники використовують шкідливу програму DarkCrystal RAT, яку розповсюджують через популярний серед військових месенджер Signal.

Щоб підвищити рівень довіри до таких повідомлень, для відправлення може використовуватися скомпрометований обліковий запис людини зі списку контактів або спільних груп жертви. Описана активність відстежується CERT-UA за ідентифікатором UAC-0200. Більше деталей можна дізнатися у статті.

8. ПЕРША СВІТОВА КІБЕРВІЙНА

ДАНІЯ ПІДВИЩИЛА РІВЕНЬ ЗАГРОЗИ ЩОДО МОЖЛИВИХ РУЙНІВНИХ КІБЕРАТАК ДО 3 ЗА 5-РІВНЕВОЮ ШКАЛОЮ

4 червня Данський центр кібербезпеки (CFCS) підвищив свою оцінку рівня загрози щодо можливих руйнівних кібератак проти Данії з «низького» до «середнього» через зростання загроз з боку росії. Згідно з CFCS, «середній» рівень, або три за п'ятирівневою шкалою, означає наявність одного або кількох суб'єктів, які мають намір і здатність до атак або шкідливої діяльності, але немає жодних ознак чи будь-яких конкретних планів такої діяльності.

РОЗВІДКА НІДЕРЛАНДІВ ВВАЖАЄ, ЩО КИТАЙСЬКА КІБЕРШПИГУНСЬКА ДІЯЛЬНІСТЬ БУЛА ОБШИРНІШОЮ, НІЖ ВВАЖАЛОСЬ СПОЧАТКУ

11 червня Голландська військова розвідка (MIVD) заявила, що продовжує розслідування інциденту з китайським кібершпигунством проти Нідерландів. Наразі розвідка вважає, що кампанія була більш масштабною, ніж передбачалося спочатку, і спрямована загалом проти західних урядів і оборонних компаній. MIVD заявило, що підтримувана державою китайська хакерська група, яка стояла за хакерською атакою на міністерство оборони Нідерландів у 2023 році, за кілька місяців атакувала щонайменше 20 000 жертв по всьому світу.

МІЖНАРОДНИЙ КРИМІНАЛЬНИЙ СУД МОЖЕ ПОЧАТИ РОЗГЛЯДАТИ КІБЕРАТАКИ В УКРАЇНІ ЯК ВОЄННІ ЗЛОЧИНИ

15 червня стало відомо, що прокурори Міжнародного кримінального суду розслідують ймовірні російські кібератаки на українську цивільну інфраструктуру як можливі воєнні злочини. Розслідування перевіряє атаки на інфраструктуру, які поставили під загрозу життя через порушення електропостачання та водопостачання, переривання з'єднань зі службами екстреного реагування або виведення з ладу мобільних служб передачі даних, які передають попередження про повітряний наліт.

УКРАЇНСЬКІ КІБЕРАКТИВІСТИ АТАКУВАЛИ РОСІЙСЬКІ КОМПАНІЇ, ЯКІ ПІДТРИМУЮТЬ ВІЙНУ

Активісти кіберспільноти BO_Team спільно з фахівцями ГУР МО України продовжують атакувати об'єкти на території держави-агресора, завдаючи значних збитків. Вони знищують важливі дані та обладнання, паралізують роботу підприємств, створюють хаос і кепський настрій в росії.

У червні вони заявили про знищення понад 100 терабайтів даних компанії OrbitSoft – розробника програмного забезпечення, що виконувала контракти для російської окупаційної армії. Також було знищено всі дані на 8 серверах компанії Orient Systems, яка розробляла та постачала навігаційне обладнання. Ця компанія співпрацювала з російськими виробниками військової техніки, зокрема БПЛА. Крім того, були знищені всі дані на 19 серверах інтернет-провайдерів у місті Нижній Новгород – «Линктелеком НН» та «Аксесс Телеком». Усім абонентам цих провайдерів надійшли листи з нагадуванням про неминучу розплату за війну проти України.

РОСІЙСЬКІ ЕНЕРГЕТИЧНІ КОМПАНІЇ, ІТ-КОМПАНІЇ ТА ДЕРЖАВНІ УСТАНОВИ ПОСТРАЖДАЛИ ВІД ТРОЯНА DECOY DOG

4 червня видання the Hacker News повідомило, що російські компанії та установи зазнали кібератак, які доставляють версію зловмисного ПЗ Decoy Dog для Windows. Компанія з кібербезпеки Positive Technologies відстежує кластер активності під назвою Operation La-hat, приписуючи його APT групі HellHounds, яка компрометує обрані ними організації та закріплюється в їхніх мережах, залишаючись непоміченими роками. Є дані, що зловмисник націлений на російські компанії принаймні з 2021 року, а розробка зловмисного ПЗ почалася ще в листопаді 2019 року.

РОСІЙСЬКІ ХАКЕРИ АТАКУВАЛИ САЙТ ІСПАНСЬКОЇ КОМПАНІЇ, ЯКА РЕМОНТУЄ ТАНКИ LEOPARD ДЛЯ УКРАЇНИ

5 червня Іспанська компанія Santa Barbara Systems, яка входить до складу General Dynam-ics, і займається ремонтом танків Leopard для постачання в Україну, зазнала кібератаки на свій вебсайт. Відповідальність за атаку взяла на себе хакерська група NoName, яка залишила повідомлення в Telegram. Група відома своєю діяльністю проти країн, що підтримують Україну.

КІБЕРАТАКА ПОРУШИЛА РОБОТУ СУПЕРМАРКЕТІВ ПО ВСІЙ РОСІЇ

Популярна російська роздрібна мережа з понад 1000 магазинами по всій країні на початку червня постраждала від кібератаки, яка призвела до перебоїв у її роботі на кілька днів. Мережа супермаркетів «Верний» 3 червня підтвердила злом, додавши, що вони все ще працюють над повним відновленням роботи.

Невідомі зламали сайт і мобільний додаток компанії. Згідно з повідомленнями, через атаку супермаркети «Верний» не могли обробляти банківські картки або приймати та доставляти онлайн-замовлення.

БІЛОРУСЬКІ ХАКЕРИ АТАКУВАЛИ МІНОБОРОНИ УКРАЇНИ В РАМКАХ НОВОЇ ШПИГУНСЬКОЇ КАМПАНІЇ

4 червня фірма з кібербезпеки Cyble повідомила, що білоруські державні хакери атакували Міністерство оборони України та військову базу в рамках нової операції з кібершпигунства.

Дослідники приписали напади угрупованню Ghostwriter, пов'язаному з Білоруссю та відомому своїми нападами на Україну, Литву, Латвію та Польщу. Під час останньої кампанії, за якою у квітні спостерігали дослідники фірми, хакери надсилали своїм цілям фішингові електронні листи з вкладеннями, які містили файли зображень дронів і шкідливу електронну таблицю Microsoft Excel.

РОСІЙСЬКІ ХАКТИВІСТИ ОБІЦЯЮТЬ МАСОВІ АТАКИ ПРОТИ ВИБОРІВ В ЄС

7 червня видання The Register повідомило, що російська хактивістська група NoName057(16) разом із сімома іншими групами погрожувала атакувати європейську інтернет-інфраструктуру на початку виборів до ЄС. Це помста за санкції Європарламенту та так звану «русофобію». Хоча конкретні плани не були деталізовані, слід очікувати DDoS атаки, які є поширеною тактикою, яку використовують NoName і союзні групи, такі як KillNet і Anonymous russia.

Нідерландські політичні партії повідомили про DDoS-атаки перед закриттям виборчих дільниць 6 червня, а HackNet взяла на себе відповідальність. Головний аналітик Mandiant Джон Хултквіст порадив не перебільшувати вагу цих атак, наголошуючи, що їхня мета – створити сумніви щодо безпеки виборів, а не завдати значної шкоди.

ВОЄННІ ВІДЕО НА ДИТЯЧОМУ КАНАЛІ: РОСІЯ ВТРУЧАЄТЬСЯ В ЄВРОПЕЙСЬКІ ЕФІРИ

7 червня видання «Економічна правда» з посиланням на Bloomberg повідомила, що з середини березня принаймні три супутники французького оператора Eutelsat SA зазнали серйозного втручання з боку росії. Перебої на цих телеканалах тривали до кінця травня. У двох випадках – 28 березня та 17 квітня – втручання замінило програму дитячого розважального каналу BabyTV компанії Walt Disney Co. на російські військові відео. У результаті нідерландський кабельний оператор Ziggo видалив BabyTV зі своєї пропозиції для перегляду.

STICKY WEREWOLF РОЗШИРЮЄ ЦІЛІ КІБЕРАТАК У РОСІЇ ТА БІЛОРУСІ

6 червня дослідники з кібербезпеки фірми Morphisec розкрили деталі загрози, відомої як Sticky Werewolf, яка була пов'язана з кібератаками на організації в росії та Білорусі. Фішингові атаки були спрямовані на фармацевтичну компанію, російський науково-дослідний інститут, що займається мікробіологією та розробкою вакцин, а також на авіаційний сектор, виходячи за межі їх первинної уваги державних організацій, йдеться у звіті Morphisec.

У ШВЕЙЦАРІЇ КОНСТАТУЮТЬ ЗБІЛЬШЕННЯ КІЛЬКОСТІ КІБЕРАТАК НАПЕРЕДОДНІ МИРНОГО САМІТУ В УКРАЇНІ

11 червня Президентка Швейцарії Віола Амхерд під час пресконференції заявила, що кібератаки на її країну почастішали останніми тижнями, але не надала більше деталей. Міністр закордонних справ Ігнаціо Кассіс заявив, що існує явна «зацікавленість» у зриві Саміту миру.
Офіційні особи не приписували інциденти конкретній країні, але росія, ймовірно, є підозрюваною, оскільки вона не була запрошена і неодноразово називала саміт «безглуздим і шкідливим», оскільки він базується на мирних пропозиціях президента України Володимира Зеленського.

ПОЛІТИЧНІ ПАРТІЇ ЄС ЗАЗНАЛИ DDOS-АТАК НА ПОЧАТКУ ВИБОРІВ – CLOUDFLARE

У день виборів до Європарламенту у Нідерландах, а також напередодні Cloudflare спостерігав DDoS-атаки, націлені на кілька інтернет-ресурсів, пов'язаних із виборами чи політикою. 6 червня кілька сайтів політичних партій у Нідерландах зазнали кібератак, відповідальність за які взяла на себе проросійська хакерська група під назвою HackNeT.

ФРАНЦУЗЬКІ ДИПЛОМАТИЧНІ УСТАНОВИ СТАЛИ ОБ'ЄКТАМИ КІБЕРАТАК, ПОВ'ЯЗАНИХ З РОСІЄЮ

За даними французького агентства з інформаційної безпеки ANSSI, спонсоровані державою актори, пов'язані з росією, здійснили цілеспрямовані кібератаки на французькі дипломатичні установи. Ці атаки приписують групі, відомій як Midnight Blizzard (раніше Nobelium), також відстежуваній як APT29, BlueBravo, Cloaked Ursa, Cozy Bear і The Dukes. ANSSI відрізняє їх від іншого кластера, Dark Halo, відповідального за атаку SolarWinds у 2020 році.

Nobelium відомий тим, що використовує скомпрометовані законні облікові записи електронної пошти для фішингових кампаній проти дипломатичних установ. Цей тип атак також відстежується під назвою Diplomatic Orbiter. У травні 2023 року європейські посольства в Києві, включно з посольством Франції, зазнали фішингових атак з надсиланням листі з темою «Продається дипломатичний автомобіль». Черговий напад на посольство Франції в Румунії не вдався.

У США ЗАБОРОНИЛИ ПРОДАЖ АНТИВІРУСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ КАСПЕРСЬКОГО ЧЕРЕЗ ЗВ'ЯЗКИ З РОСІЄЮ

21 червня видання The Washington Post повідомило, що адміністрація Байдена заборонила «Лабораторії Касперського» поширювати антивірусне ПЗ та продукти кібербезпеки в США, посилаючись на загрозу національній безпеці. Міністр торгівлі Джина Раймондо зазначила, що це рішення було прийнято після ретельного розслідування та відображає побоювання, що росія може використати Kaspersky для доступу до особистої інформації американців і використання її як зброї. Kaspersky спростував ці заяви, пояснивши заборону геополітичною напругою. Заборона, яка набуває чинності 29 вересня, дасть користувачам час знайти альтернативи, але залишить їх перед ризиками кібербезпеки, якщо вони продовжуватимуть використовувати продукти Kaspersky. Цей крок розширює попередні обмеження та відображає зростаючу увагу США до технологічних компаній, що належать іноземним власникам, у питаннях конфіденційності та безпеки даних.

Через день після того, як російську компанію заборонило Міністерство торгівлі, Управління з контролю за іноземними активами Міністерства фінансів США (OFAC) запровадило санкції проти десятка осіб, які обіймають посади виконавчого та вищого керівництва в «Лабораторії Касперського».

РОСІЙСЬКІ ХАКЕРИ АТАКУВАЛИ TEAMVIEWER

27 червня виробник програмного забезпечення для віддаленого управління робочим столом TeamViewer заявив, що виявив «порушення» у своїй корпоративній IT-мережі. Як стало пізніше відомо, в атаці підозрюються Cosy Bear (вони ж APT29 і Midnight Blizzard). Атака була організована через обліковий запис одно з співробітників. TeamViewer запевняє своїх користувачів, що інцидент стосувався лише їх корпоративної IT-мережі, яка відділена від виробничого середовища та платформи підключення TeamViewer.

УКРАЇНСЬКА IT-АРМІЯ ВИВЕЛА З ЛАДУ РОСІЙСЬКІ ОНЛАЙН-СЕРВІСИ

21 червня українські хакери здійснили масштабну атаку на такі великі російські банки, як Сбербанк і ВТБ, зробивши їхні послуги недоступними для деяких користувачів. Українські кіберфахівці провели масштабну операцію проти російської платіжної системи «Мир» та інших фінансових, комунікаційних та електронних майданчиків країни-агресора, повідомляє Міністерство цифрової трансформації у соцмережах.

КІБЕРБАНДА EXCOBALT НАЦІЛЕНА НА РІЗНІ ГАЛУЗІ В РОСІЇ ЗА ДОПОМОГОЮ НОВОГО БЕКДОРУ GORED

22 червня видання The Hacker News повідомило, що російські організації стали мішенню банди кіберзлочинців під назвою ExCobalt, що використовує раніше невідомий бекдор на базі Golang, відомий як GoRed. Як йдеться у звіті Positive Technologies, ExCobalt зосереджується на кібершпигунстві та включає кількох членів, які діють принаймні з 2016 року та, ймовірно, колись були частиною сумнозвісної банди Cobalt Gang. Атаки, здійснені угрупованням, протягом останнього року виділили різні галузі в росії, включаючи уряд, інформаційні технології, металургію, гірничодобувну промисловість, розробку програмного забезпечення та телекомунікації.

ГРОМАДЯНИНА РОСІЇ ЗВИНУВАЧУЮТЬ У КІБЕРАТАКАХ НА УКРАЇНУ ПЕРЕД ВТОРГНЕННЯМ У 2022 РОЦІ

27 червня у США проти 22-річного росіянина було висунуто звинувачення у ймовірній участі в організації кібератак проти України та її союзників у дні, що передували повномасштабному військовому вторгненню росії в Україну на початку 2022 року. Підсудного Аміна Тимовича Стігала вважають пов'язаним з гру. Він залишається у розшуку. Якщо його визнають винним, йому загрожує максимальне покарання у вигляді п'яти років позбавлення волі.

У КРИМУ ПОПЕРЕДЖАЮТЬ ПРО ЗБОЇ В ІНТЕРНЕТІ ЧЕРЕЗ DDOS-АТАКИ НА МІСЦЕВИХ ОПЕРАТОРІВ ЗВ'ЯЗКУ

27 червня місцева влада Криму попередила про збої в роботі Інтернету через DDoS-атаки, націлені на телекомунікаційних провайдерів. «Масовані» DDoS-атаки були запущені проти телекомунікаційних компаній Криму 26 червня та тривали щонайменше два дні. У Севастополі атаки здебільшого були спрямовані на місцевого Інтернет-провайдера Miranda Media, який пов'язаний з російським національним оператором зв'язку «Ростелеком».

НАСКІЛЬКИ ІЗОЛЬОВАНИЙ РОСІЙСЬКИЙ ІНТЕРНЕТ? НАСЛІДКИ ВІЙНИ В УКРАЇНІ

Цифровий суверенітет – це глобальна концепція, яка передбачає контроль над Інтернетом та його інфраструктурою, і росія вживає значних заходів для досягнення цього протягом останніх двох десятиліть. Попри спроби відключитися від глобальної мережі Інтернет, російський Інтернет, на відміну від китайського, залишається децентралізованим і його важко повністю ізолювати. Збільшення кількості випадків ізоляції в поєднанні з санкціями та внутрішньою цензурою після вторгнення в Україну послабило стійкість росії в Інтернеті.

Багато технологічних компаній припинили діяльність у росії, що ще більше погіршило її надійність Інтернету. Багаторічна цензура в росії посилилася, заблокувавши багато соціальних мереж і новинних сайтів, заборонивши послуги VPN і спричинивши вихід міжнародних хостингових компаній. Ця взаємна ізоляція посилюється санкціями ЄС проти російських ЗМІ та взаємними геоблокуючими зусиллями росії та західних країн.

9. РІЗНЕ

ФБР КАЖЕ, ЩО МАЄ 7000 КЛЮЧІВ ДЕШИФРУВАННЯ ПРОГРАМ-ВИМАГАЧІВ LOCKBIT

На Бостонській конференції з кібербезпеки 2024 року Браян Ворндран, помічник директора кібервідділу ФБР, сказав, що агентство може допомогти жертвам відновити дані, зашифровані програмним забезпеченням-вимагачем LockBit. Він заявив, що агентство отримало понад 7000 ключів дешифрування програми-вимагача LockBit, і закликав жертв зв'язатися з ФБР.

MICROSOFT ЗОБОВ'ЯЗАВСЯ ПОВНІСТЮ ВИКОНАТИ ВСІ 25 РЕКОМЕНДАЦІЙ З УРЯДОВОГО ЗВІТУ ЩОДО ВРАЗЛИВОСТІ У MICROSOFT EXCHANGE

Під час слухань у Комітеті з внутрішньої безпеки Палати представників Конгресу США, віцеголова та президент корпорації Microsoft Бреда Сміт публічно зобов'язався виконати всі рекомендації, які були визначені у звіті «Огляд вторгнення восени 2023 року у Microsoft Exchange Online» підготовленого Радою з огляду кібербезпеки (Cyber Safety Review Board), створеної відповідно до Указу Президента США №14028 у 2022 році. Звіт вказував на численні проблеми безпеки, які є наслідком корпоративної культури Microsoft, в якій питання безпеки депріоритизовані.