НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

УКРАЇНСЬКА ФУНДАЦІЯ БЕЗПЕКОВИХ СТУДІЙ

CYBER DIGEST

Огляд подій в сфері кібербезпеки,
березень 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".

Думки автора, висловлені в цій публікації, не обов'язково відображають погляди Агентства США з міжнародного розвитку або Уряду США.

ЗМІСТ

ОСНОВНІ ТЕНДЕНЦІЇ

Європейський Союз завершує процес прийняття та запуску Акту про кіберстійкість (Cyber Resilience Act), який має істотно змінити безпекові правила у ЄС. Це доповнюється розробкою заходів з регулювання використання ШІ – Європарламент планує ухвалити Закон про штучний інтелект, який передбачатиме регулювання ШІ на основі потенційних ризиків та впливу. В той час як основні зусилля керівництва ЄС зосереджені на побудові кіберзахисту, аналітики оцінюють як саме чинні кібербезпекові структури (такі як CSIRT) можуть бути більш корисними в загальноєвропейському контексті забезпечення кібербезпеки. Серед основних висновків – ці організації мають стати більш проактивними у своїй діяльності.

Інформаційна та кібербезпека були визначені Президентом України Володимиром Зеленським серед п'яти пріоритетів Ради національної безпеки та оборони України під час представлення новопризначеного Секретаря РНБО України Олександра Литвиненка. Зокрема йдеться про зміцнення захисту від ворожих дестабілізаційних операцій та посилення координації всіх державних інституцій у цій сфері, а також розвиток спроможності ударного кіберпотенціалу України. Як вважає заступник Секретаря РНБО України Сергій Демедюк, з огляду на досвід у кібервійні з рф, Україна вже не є полігоном для відпрацювання можливостей рф, а може і має стати регіональним лідером із кібербезпеки, ініціюючи зміни у міжнародних підходах до агресії у кіберпросторі.

Спостерігається помітна ескалація дипломатичного протистояння між західними країнами та КНР щодо можливої відповідальності останньої за втручання в роботу парламентських структур по всьому світу. Міністерство юстиції США оприлюднило свій висновок про те, що китайські хакери атакували європейських законодавців, зокрема членів Міжпарламентського альянсу з питань Китаю, британський уряд офіційно звинуватив Китай у кібератаках на демократичні інститути Великобританії. Фінляндія та Нова Зеландія також приписують китайським хакерським групам атаки на їх парламенти. Вочевидь така активність пов'язана і з тим, що у 2024 році в низці демократичних країнах відбудуться виборчі процеси і країни занепокоєні можливим втручанням в них. Так, ENISA оновила довідник для забезпечення кібербезпеки виборчого процесу, а американська CISA відпрацювала процедури захисту виборчого процесу на прикладі «супервівторка» у березні 2024 року.

Вразливість Ivanti продовжує створювати проблеми кібербезпековим органам та споживачам по всьому світу. Агентства Альянсу Five Eyes попереджають, що зловмисники можуть активно використовувати цю вразливість і підтримувати свою присутність в уражених системах. Зі свого боку Агенція національної безпеки США підтвердило, що вже зараз зловмисники, використовуючи цю вразливість, атакують підприємства оборонного сектору (з метою зниження загроз у стратегічній перспективі Пентагон оперативно затвердив окрему Стратегію кібербезпеки оборонно-промислового сектору), а CISA була навіть змушена відключити декілька своїх систем аби не допустити кібератаки на них. Для США ситуація з Ivanti ускладнюється і через необхідність розв'язання іншої проблеми – опрацювання наслідків лютневої кібератаки хакерів Blackcat проти систем Change Healthcare. Ця атака призвела до негативних наслідків для всієї системи охорони здоров'я країни, яка сильно залежить від страхування. Change Healthcare обробляє близько 50% медичних вимог у Сполучених Штатах, що містить в собі близько 900 тисяч лікарів, 33 тисячі аптек, 5 500 лікарень і 600 лабораторій. Міністерство охорони здоров'я оголосило про початок розслідування інциденту, а Держдепартамент США оголосив про винагороду в 10 мільйонів доларів за інформацію про угрупування Blackcat.

Після низки кіберінцидентів проти організацій сектору водопостачання, США активно переглядає свою політику щодо цього сектору. Крім оновлення відповідних рекомендацій з боку CISA в процес включився Білий дім, оголосивши про плани створити нову робочу групу, метою якої є захист водного сектора від кібератак, спонсорованих державами. Все серйознішим стає сприйняття загроз в космічній сфері – США активно нарощує свої можливості кіберзахисту в цьому домені, а інциденти з фізичною безпекою підводних кабелів може мати довгострокові наслідки для глобальної доступності мережі Інтернет.

російська кіберактивність стає все масштабнішою. Кібербезпекові компанії продовжують дослідження російських кібероперацій проти європейських неурядових організацій, а обсяги кібервтручання групи Midnight Blizzard в системи Microsoft все ще не до кінця зрозумілі. Крім того, стало відомо, що російські хакери націлились на політичні партії Німеччини та активно тестують вайпер AcidPour (модифікація AcidRain, що був застосований на початку військового вторгнення рф до України проти модемів KA-SAT) – вірус, що має знищувати дані в ураженій системі. Схоже, що оновлений вірус, націлений на системи під Linux x86 і міг бути використаний проти низки телекомоператорів в Україні.

У березні ГУР розповіло про успішну спецоперацію проти міноборони рф, під час якої було отримано доступ до серверів та масиву секретної документації. Кіберфахівці СБУ зупинили постачання комплектуючих для російських дронів та крилатих ракет, а також працюють на фронті над знищенням ворожих систем РЕБ і РЕР та перехопленням безпілотників, які координують ракетні та артилерійські удари по силах оборони.

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

ЗА ПЕРШИЙ РІК США ДОМОГЛИСЬ ВИКОНАННЯ ПОНАД 20 З 69 ІНІЦІАТИВ ПЛАНУ ВПРОВАДЖЕННЯ НАЦІОНАЛЬНОЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ

4 березня Офіс національного кібердиректора (ONCD) оприлюднив перші оцінки впровадження нової Стратегії кібербезпеки США та плану її реалізації. Підкреслено, що ONCD активно працював над реалізацією 69 ініціатив з плану впровадження Національної стратегії кібербезпеки. Федеральні агентства досягли прогресу у всіх цих ініціативах, виконавши понад 20 з них. ONCD сподівається вже через рік представити нову версію плану впровадження. Серед проміжних досягнень відзначено:

- оновлення публічно-доступних сценаріїв для кібернавчань;
- проведення декількох успішних операцій проти інфраструктури ransomware угрупувань;
- зміну нормативних вимог безпеки для постачальників продуктів Інтернету речей (IoT) для урядових структур;
- ширше залучення США до міжнародних органів стандартизації;
- виділення у вигляді грантів 130 мільйонів доларів для перевірки безпеки бездротових з'єднань.

ЄВРОПАРЛАМЕНТ ПЛАНУЄ УХВАЛИТИ ЗАКОН ПРО ШТУЧНИЙ ІНТЕЛЕКТ

7 березня Європарламент підтвердив, що планує затвердити нові правила використання штучного інтелекту, які гарантують безпеку, надійність та дотримання фундаментальних прав ЄС, сприяючи при цьому інноваціям. Нове законодавство передбачає регулювання штучного інтелекту на основі потенційних ризиків та впливу. Зокрема, буде заборонено використання програм, що порушують основні права, наприклад, біометричну ідентифікацію на основі конфіденційних даних або маніпулювання поведінкою. Крім того, моделі ШІ повинні відповідати прозорості та правилам авторського права ЄС, а найпотужніші моделі – додатковим вимогам безпеки.

CISA ОГОЛОШУЄ ПРО НОВІ ЗУСИЛЛЯ, СПРЯМОВАНІ НА ЗАХИСТ ЕКОСИСТЕМИ ВІДКРИТОГО КОДУ

7 березня 2024 року CISA оголосила про нові ініціативи, спрямовані на підвищення безпеки екосистеми відкритого коду. Вони містять у собі роботу з репозиторіями для прийняття ними принципів безпеки та започаткування зусиль для добровільної співпраці та обміну інформацією. Ця ініціатива спрямована на зміцнення інфраструктури безпеки програмного забезпечення з відкритим кодом.

У БЮДЖЕТНОМУ ЗАПИТІ НА 2025 РІК ПЕНТАГОН ПРОСИТЬ 14,5 МЛРД НА ЗАХОДИ КІБЕРБЕЗПЕКИ

11 березня було опубліковано фінансовий запит Пентагону на 2025 рік. Він містить у собі запит на 14,5 мільярда доларів на заходи кібербезпеки. Ці кошти будуть спрямовані на три великі програми: кібербезпека відомства, операції в кіберпросторі, дослідження у сфері кібербезпеки. Майже один мільярд доларів буде спрямовано на впровадження архітектури нульової довіри (ZTA) в військових інформаційних мережах.

ЄВРОПАРЛАМЕНТ ПРИЙНЯВ АКТ ПРО КІБЕРСТІЙКІСТЬ (CYBER RESILIENCE ACT)

12 березня Європарламент схвалив нові стандарти кіберстійкості для захисту цифрових продуктів в ЄС – Cyber Resilience Act. Документ має на меті забезпечити безпеку, стійкість та належну інформацію про кібербезпеку продуктів. Важливі та критично важливі продукти будуть класифіковані залежно від їхнього рівня критичності. Продукти, які становлять вищий ризик для кібербезпеки, будуть посилено перевірятися уповноваженим органом, тоді як інші можуть проходити легший процес оцінки відповідності. Депутати також акцентували на збільшенні ролі Агентства Європейського Союзу з кібербезпеки (ENISA) у виявленні та управлінні вразливостями та інцидентами, а також затвердили освітні та навчальні програми для підвищення професійних навичок у сфері кібербезпеки.

SAFECOM І NCSWIC СТВОРЮЮТЬ ЦЕНТР РЕСУРСІВ 911 CYBERSECURITY RESOURCE HUB

Платформа CISA для поліпшення міжвідомчої та міжюрисдикційної співпраці SAFECOM та проєкт CISA з поліпшення безпекових комунікацій на національному рівні NCSWIC спільно створили Ресурсний центр з кібербезпеки 911. Цей ресурс має на меті допомогти центрам екстреного зв'язку (ECC) у питаннях кібербезпеки, пропонуючи централізовану точку для повідомлення про кіберінциденти. Також Ресурсний центр надає доступ до тематичних досліджень та освітніх ресурсів з найкращими практиками захисту мереж.

ENISA ОНОВИЛА ДОВІДНИК ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ВИБОРЧОГО ПРОЦЕСУ

На початку березня, ENISA разом з Групою співробітництва NIS оновили довідник з кібербезпеки виборів напередодні виборів до ЄС 2024 року. У цій оновленій версії документа додано нові загрози у сфері кібербезпеки, зокрема загрози застосування можливостей штучного інтелекту. Довідник містить вичерпний перелік загроз кібербезпеці, опис ризиків і практичних рекомендацій для національних органів влади та суб'єктів ЄС, залучених до проведення виборів.

ПРЕЗИДЕНТ США НОМІНУЄ МАЙКЛА СУЛМАЄРА НА ПОСАДУ ЗАСТУПНИКА МІНІСТРА ОБОРОНИ З КІБЕРБЕЗПЕКИ

22 березня Президент США Джо Байден заявив, що збирається номінувати Майкла Сулмаєра (Michael Sulmeyer) на посаду заступника Міністра оборони з кібербезпеки – це нова посада в системі Міністерства оборони, створена Законом про дозвіл на національну оборону 2023. У минулому Салмейер працював старшим директором з кіберполітики в Раді національної безпеки та старшим радником у Кіберкомандуванні США. Він також був директором проєкту з кібербезпеки в Белферівському центрі науки та міжнародних відносин Гарвардської школи Кеннеді. За попередніми даними Сенат США готовий підтримати цю кандидатуру.

JCDC СТВОРИВ ОРГАНІЗАЦІЙНУ ОСНОВУ ДЛЯ СПІЛЬНОГО З УЧАСНИКАМИ РИНКУ КІБЕРЗАХИСТУ ТРУБОПРОВОДІВ

26 березня JCDC CISA відзвітувало про вдалий досвід 2023 року у координації зусиль уряду та понад 25 нафтових і газових організацій з планування кіберзахисту трубопроводів – JCDC Pipelines Cyber Defense Planning Effort. Ця ініціатива спрямована на посилення кіберзахисту високопродуктивних магістральних газопроводів від таких загроз як ransomware і загрози від підтримуваних державами хакерів. Результатом співпраці стала розробка базової архітектури безпеки газопроводів ONG Pipelines, яка є моделлю для подальшого інвестування в кібербезпеку цих промислових систем.

США ПОСИЛЮЮТЬ КІБЕРБЕЗПЕКУ СВОГО КОНТИНГЕНТУ В ЯПОНІЇ

26 березня стало відомо, що Командування сил морської піхоти США в кіберпросторі (MARFORCYBER) відправило до III Експедиційного корпусу морської піхоти на Окінаві групу морських піхотинців з відповідним досвідом забезпечення кібербезпеки. Це відбувається в межах нової політики Морської піхоти щодо «кіберротацій».

ФІНЛЯНДІЯ ПОСИЛЮЄ ВЛАСНУ КІБЕРБЕЗПЕКУ ПІСЛЯ ВСТУПУ В НАТО

26 березня Фінляндія, одразу після приєднання до НАТО, оголосила про низку заходів, спрямованих на посилення кібербезпеки країни. Це містить в собі побудову двох дослідницьких центрів кібербезпеки та акселератору кіберінновацій. Дослідницькі центри НАТО, які працюватимуть над новими технологіями, будуть розташовані у фінському місті Еспоо, а акселератор буде працювати з нового об'єкта в Оулу – провідному кібертехнологічному центрі Фінляндії. Також Міністерству оборони та Міністерству транспорту та зв'язку доручено оновити національну стратегію кібербезпеки Фінляндії. Терміновість оновлення національної стратегії кібербезпеки стала очевидною в третьому кварталі 2023 року, коли фінська служба безпеки та розвідки SUPO попередила про різке зростання кількості кібератак з росії.

CISA РОЗПОЧИНАЄ ПРОЦЕС ВПРОВАДЖЕННЯ ЗАКОНУ ПРО ЗВІТНІСТЬ ЩОДО КІБЕРІНЦИДЕНТІВ ДЛЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

27 березня CISA ініціювала наступний крок у впровадженні Закону про звітність щодо кіберінцидентів для критичної інфраструктури від 2022 року (CIRCIA). Цей крок включає оприлюднення проєкту нормативних змін (NPRM), що мають впорядкувати процес звітування про кіберінциденти, спростити виявлення закономірностей у режимі реального часу, заповнити критичні інформаційні прогалини у реагуванні та допомогти швидко розгортати ресурси для надання допомоги суб'єктам, які постраждали від кібератак, а також інформувати інших, хто міг би потенційно постраждати. Наразі триває громадське обговорення запропонованих змін, після чого вони будуть подані на голосування.

США ЗВИНУВАЧУЄ КИТАЙ У КІБЕРАТАЦІ НА ЄВРОПЕЙСЬКИХ ЗАКОНОДАВЦІВ

27 березня Міністерство юстиції США оприлюднило свій висновок про те, що китайські хакери атакували європейських законодавців, зокрема членів Міжпарламентського альянсу з питань Китаю, для збору конфіденційних даних. Обвинувальний акт показав, що понад 1000 електронних листів було надіслано на понад 400 акаунтів з метою збору інформації про інтернет-активність та цифрові пристрої членів альянсу.

ПЕНТАГОН ОПРИЛЮДНИВ СТРАТЕГІЮ КІБЕРБЕЗПЕКИ ОБОРОННО-ПРОМИСЛОВОГО СЕКТОРУ

28 березня Пентагон оприлюднив свою Стратегію кібербезпеки оборонно-промислового сектору, зосереджуючись на чотирьох ключових цілях. Серед них – широке впровадження найкращих практик кібербезпеки, збереження ланцюжків постачання, які мають вирішальне значення для військового виробництва, і покращення зв'язку між державним і приватним секторами. Нова Стратегія узгоджується з іншими стратегічними документами Міністерства оборони: Національною оборонною стратегією до 2022 року, Національною стратегією кібербезпеки до 2023 року та цьогорічною Національною стратегією для оборонної промисловості.

НОВА ЗЕЛАНДІЯ ЗВИНУВАЧУЄ КИТАЙ У ХАКЕРСЬКИХ АТАКАХ НА ПАРЛАМЕНТ У 2021 РОЦІ

26 березня Уряд Нової Зеландії заявив, що офіційно висловив занепокоєння уряду Китаю щодо причетності підтримуваних ним хакерів до кібератак на парламент Нової Зеландії у 2021 році. Відповідні претензії було офіційно передано китайському послу. Таке рішення новозеландського уряду стало результатом розслідування, проведеного Бюро комунікаційної безпеки (GCSB), яке займається кібербезпекою та розвідкою за кордоном. Воно встановило зв'язок між китайською організацією, відомою як APT40, і зловмисною кіберактивністю, націленою на парламентські служби Нової Зеландії у 2021 році.

ПРЕМ'ЄР-МІНІСТР НІДЕРЛАНДІВ МАРК РЮТТЕ ОБГОВОРИВ ІНЦИДЕНТ КІБЕРШПИГУНСТВА ПІД ЧАС ПЕРЕГОВОРІВ ІЗ СІ ЦЗІНЬПІНОМ

27 березня Прем'єр-міністр Нідерландів Марк Рютте підтвердив, що під час зустрічі з лідером КНР Сі Цзіньпіном обговорив нещодавній кіберінцидент пов'язаний із вторгненням китайських хакерів в одну з голландських військових мереж. Це був перший раз, коли Нідерланди офіційно звинуватили КНР у кіберактивності проти інтересів Нідерландів. Результати обговорення двох посадовців невідомі, однак дискусія відбувається на фоні загострення відносин між двома країнами – Нідерланди обмежують експорт високотехнологічного напівпровідникового обладнання голландського гіганта ASML до Китаю.

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

НАТО ТА МОЛДОВА ЗМІЦНЮЮТЬ ЕНЕРГЕТИЧНУ СТІЙКІСТЬ ПРОТИ КІБЕР- ТА ГІБРИДНИХ ЗАГРОЗ

12-14 березня 2024 року у м. Кишинів відбулись навчання НАТО CORE-24 M. Тематика навчань – захист енергетичної інфраструктури від цифрових загроз. Навчання спрямовані на збільшення співпраці між енергетичними операторами та кіберзахисниками для зміцнення готовності до кіберзагроз. Захід зібрав понад 100 учасників з 10 країн та 32 установ.

ВЕЛИКОБРИТАНІЯ ЗВИНУВАЧУЄ КИТАЙ У КІБЕРАТАКАХ НА БРИТАНСЬКУ ДЕМОКРАТІЮ

25 березня британський уряд офіційно звинуватив Китай у кібератаках на демократичні інститути Великобританії. Віцепрем'єр-міністр Олівер Доуден заявив, що за нападами на британську комісію зі спостережень за виборами та на законодавців стоять актори, пов'язані з китайською державою. Велика Британія запровадила санкції проти двох осіб і викликала посла Китаю. Цей крок знаменує зміну позиції Великобританії щодо кібератак Пекіна. Було підкреслено напади на виборчу комісію та депутатів, які критикують Китай. Проте деякі критики в Консервативній партії висловили незадоволення масштабами відповіді Великобританії. Китай відкинув звинувачення, назвавши їх «наклепом» і звинуватив Великобританію в поширенні дезінформації.

США ЗАПРОВАДИЛИ САНКЦІЇ ПРОТИ ВІРОГІДНО ПОВ'ЯЗАНИХ З ДЕРЖАВОЮ КИТАЙСЬКИХ ХАКЕРІВ ЗА АТАКИ НА КРИТИЧНУ ІНФРАСТРУКТУРУ

26 березня після десятків атак на критичну інфраструктуру, США наклали санкції на компанію з Уханя, яку вважають прикриттям для Міністерства державної безпеки Китаю. Міністерство юстиції та фінансів США звинуватило науково-технічну компанію Wuhan Xiaoruizhi у тому, що вона є прикриттям APT31 – китайської хакерської групи, відомої нападами на «широке коло високопоставлених урядовців США та їхніх радників», включаючи співробітників Білого Дому, членів Конгресу від обох партій і кілька міністерств США. У відповідь Китай розкритикував США та Великобританію через заяви про хакерство

АГЕНТСТВА FIVE EYES ПОПЕРЕДЖАЮТЬ ПРО АКТИВНЕ ВИКОРИСТАННЯ ВРАЗЛИВОСТЕЙ ШЛЮЗУ IVANTI

29 лютого Розвідувальний альянс Five Eyes випустив нове попередження щодо кіберзагроз, які використовують відомі вразливості в шлюзах Ivanti Connect Secure та Ivanti Policy Secure, зауважуючи, що Інструмент перевірки цілісності (ICT) може бути обманутий, щоб створити хибне відчуття безпеки та що зловмисники можуть підтримувати постійну присутність у кореневому каталозі навіть після скидання налаштувань пристроїв до заводських.

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

АНБ КАЖЕ, ЩО ВІДСТЕЖУЄ КІБЕРАТАКИ ЧЕРЕЗ ПРОДУКТИ IVANTI, В ТОЙ ЧАС, ЯК ХАКЕРИ АТАКУЮТЬ ОБОРОННИЙ СЕКТОР США

1 березня Агентство національної безпеки США (АНБ) підтвердило, що хакери використовують уразливості корпоративного VPN-пристрою Ivanti для атак на організації в оборонному секторі США. АНБ разом зі своїми міжвідомчими партнерами активно стежить за ситуацією та співпрацює з партнерами, щоб пом'якшити наслідки. Це підтвердження прозвучало після повідомлень Mandiant, що вірогідно китайські хакери намагаються використати вразливості Ivanti Connect Secure, націлюючись на різні галузі промисловості, включаючи оборонну промисловість США.

ОПЕРАТОРИ ШПИГУНСЬКОГО ПЗ PREDATOR ВІДБУДОВУЮТЬ БАГАТОРІВНЕВУ ІНФРАСТРУКТУРУ ДЛЯ АТАК НА МОБІЛЬНІ ПРИСТРОЇ – INSIKT GROUP

Нове дослідження Insikt Group, опубліковане 1 березня, присвячено нещодавно виявленій інфраструктурі, пов'язаній з операторами мобільної шпигунської програми Predator. Вважається, що ця інфраструктура використовується принаймні в одинадцяти країнах, включаючи Анголу, Вірменію, Ботсвану, Єгипет, Індонезію, Казахстан, Монголію, Оман, Філіппіни, Саудівську Аравію та Тринідад і Тобаго. Примітно, що це перша ідентифікація клієнтів Predator у Ботсвані та на Філіппінах. Попри те, що Predator рекламують як інструмент для боротьби з тероризмом і роботи правоохоронних органів, Predator часто застосовують проти громадянського суспільства, націлюючись на журналістів, політиків і активістів. На цей момент не було виявлено конкретних жертв або цілей.

CISA ОНОВИЛО НАБІР РЕКОМЕНДАЦІЙ ДЛЯ КОМУНІКАЦІЇ ПИТАНЬ ГРОМАДСЬКОЇ БЕЗПЕКИ ТА КІБЕРСТІЙКОСТІ

CISA оновило свій інструментарій, який має допомогти зацікавленим органами отримати швидкий доступ до додаткової інформації з важливих питань громадської безпеки (всього 16 напрямків, включаючи реагування на кіберінциденти, ransomware, охорона здоров'я, пожежна безпека тощо). Цей інструментарій, опублікований 4 березня 2024 року, допоможе агентствам підвищити стійкість до нових загроз і об'єднає наявні урядові ресурси для зацікавлених сторін.

CISA ТА ПАРТНЕРИ ЗАБЕЗПЕЧИЛИ БЕЗПЕКУ «СУПЕРВІВТОРКА»

CISA, у координації з партнерами, повідомила про те, що їм вдалось належним чином забезпечити безпеку виборів у «супервівторок» (5 березня – дата проведення праймеріз у більшості штатів). Розмістивши у себе Центр виборчих операцій, CISA активно обмінювалась інформацією про загрози в режимі реального часу між федеральними, державними, місцевими органами влади та приватним сектором. Ця ініціатива є частиною ширших зобов'язань CISA щодо підтримки державних та місцевих посадових осіб у захисті виборчої інфраструктури.

Вже 6 березня CISA оприлюднила огляд «Супервівторок: Короткий огляд місії CISA із забезпечення безпеки виборчого процесу» в якому висвітлила основні організації, спрямовані на підтримку членів виборчих комісій по всій країні під час «супервівторка». Це включало роботу новопризначених радників з питань виборчої безпеки, надання індивідуальної підтримки та ресурсів для задоволення унікальних потреб виборчих комісій.

NSA ОПРИЛЮДНИЛО ІНСТРУКЦІЇ ЩОДО ВИЗНАЧЕННЯ РІВНЯ ЗРІЛОСТІ ДЛЯ МЕРЕЖ «НУЛЬОВОЇ ДОВІРИ»

5 березня 2024 року NSA випустило інформаційний бюлетень з кібербезпеки під назвою «Просування до нульової довіри в усіх компонентах мережі та навколишнього середовища». Це керівництво має на меті допомогти організаціям обмежити ворожі дії у своїх мережах для захисту конфіденційних даних і критично важливих систем. У документі наголошується на впровадженні принципів нульової довіри для посилення внутрішнього мережевого контролю і сегментації, а також описуються основні підходи для впровадження практик нульової довіри, такі як відображення потоків даних, сегментація мереж для ізоляції критично важливих ресурсів.

APT GHOSTSEC ПРОВОДИТЬ СПІЛЬНІ ОПЕРАЦІЇ З ІНШИМИ УГРУПОВАННЯМИ

5 березня у блозі Cisco Talos обговорюється діяльність APT групи GhostSec та їхня співпраця з ransomware групами Stormous. У ньому описується еволюція арсеналу GhostSec, включаючи розробку ransomware GhostLocker 2.0 і таких інструментів, як GhostSec Deep Scan та GhostPresser. Альянс цих угруповань націлився на декілька країн, що свідчить про розширення їхньої шкідливої діяльності та зростання технічних можливостей GhostSec.

КІБЕРАТАКА ЗМУСИЛА КАНАДСЬКУ ФІНАНСОВУ РОЗВІДКУ ВІДКЛЮЧИТИ СИСТЕМИ ВІД ІНТЕРНЕТУ

5 березня Агентство фінансової розвідки Канади FINTRAC оголосило про припинення роботи своїх корпоративних систем через кіберінцидент, який стався на вихідних. Інцидент не стосується розвідувальних чи секретних систем Центру, повідомило агентство, але характер інциденту не розголосило. Агентство заявило, що «тісно співпрацює зі своїми федеральними партнерами, включаючи Канадський центр кібербезпеки, щоб захистити та відновити свої системи». FINTRAC, Канадський центр аналізу фінансових транзакцій і звітів, є державним органом, заснованим для виявлення та розслідування відмивання грошей і подібних злочинів.

НОВА ГРУПА APT LOTUS BANE СТОЇТЬ ЗА НЕДАВНІМИ АТАКАМИ НА ФІНАНСОВІ УСТАНОВИ В'ЄТНАМУ

6 березня видання The Hacker News повідомило, що фінансова установа у В'єтнамі була атакована раніше незадокументованим загрозливим суб'єктом під назвою Lotus Bane, який вперше був виявлений у березні 2023 року. Group-IB зі штаб-квартирою в Сінгапурі описала хакерське угруповання як APT, яка діє щонайменше з 2022 року. Точна специфіка ланцюжка зараження поки що залишається невідомою, але вона передбачає використання різноманітних шкідливих артефактів, які служать сходинкою для наступного етапу. Більш детально про загрозу у звіті Group-IB.

NSA ОПРИЛЮДНИЛО ДЕСЯТЬ НАЙКРАЩИХ СТРАТЕГІЙ ЗМЕНШЕННЯ ЗАГРОЗИ ХМАРНОЇ БЕЗПЕКИ

7 березня 2024 року NSA випустило посібник під назвою «Десять стратегій пом'якшення наслідків хмарної безпеки», в якому пропонує найважливіші практики безпеки для клієнтів хмарних сервісів. Цей звіт, розроблений у партнерстві з CISA, охоплює комплексні заходи кібербезпеки для ефективного управління хмарним середовищем. Він підкреслює важливість дотримання моделей спільної відповідальності, безпечного управління ідентифікацією/доступом та захисту даних серед інших стратегій, щоб запобігти перетворенню організації на мішень для зловмисників.

АФІЛЬОВАНА ЗА КНР APT ГРУПА EARTH KRAHANG ПРОВОДИТЬ МАСШТАБНУ КІБЕРШПИГУНСЬКУ ОПЕРАЦІЮ

У дослідницькій статті Trend Micro від 18 березня розкривається кібершпигунська діяльність Earth Krahang – APT групи, яку дослідники пов'язують з КНР. Діяльність цієї групи націлена на державні організації по всьому світі, зокрема на країни Південно-Східній Азії, Європи, Америки та Африки. Однією з улюблених тактик зловмисника є використання встановленого ним доступу до урядової інфраструктури для атаки на інші державні організації, а також зловживання захопленою інфраструктурою для розміщення шкідливих корисних навантажень. Також вони надсилають фішингові електронні листи цілям в державному сектору за допомогою скомпрометованих облікових записів електронної пошти.

МИНУЛОГО МІСЯЦЯ CISA БУЛА ЗМУШЕНА ВІДКЛЮЧИТИ ДВІ СИСТЕМИ ВІД МЕРЕЖІ ПІСЛЯ ЗЛАМУ IVANTI

8 березня Агентство з кібербезпеки та безпеки інфраструктури США (CISA) повідомило, що кібератака спонукала його відключити дві системи від Інтернету минулого місяця. Постраждалі системи використовували застарілу технологію, яка мала бути замінена, і, як повідомляється, була зламана через уразливості в продуктах Ivanti VPN. Системи, які були зламані та виведені з ладу, це шлюз захисту інфраструктури CISA та їх інструмент оцінки хімічної безпеки.

БЕРЕЗНЕВІ ОНОВЛЕННЯ MICROSOFT УСУВАЮТЬ 61 ВРАЗЛИВІСТЬ, ВКЛЮЧАЮЧИ КРИТИЧНІ НЕДОЛІКИ HYPER-V

13 березня корпорація Microsoft випустила щомісячне оновлення системи безпеки, яке усуває 61 помилку безпеки в її програмному забезпеченні, включаючи дві критичні проблеми, що впливають на Windows Hyper-V, які можуть призвести до DoS атак і віддаленого виконання коду. З 61 уразливості дві мають оцінку «Критичні», 58 – «Важливі», а одна – «Низький рівень серйозності». Жоден із недоліків не позначено як загальновідомий або такий, що використовується для активної атаки на момент випуску, але шість із них позначено оцінкою «використання більш ймовірне».

ВИТІК ДАНИХ З ФРАНЦУЗЬКОГО АГЕНТСТВА З ПИТАНЬ ЗАЙНЯТОСТІ ТОРКНУВСЯ 43 МІЛЬЙОНІВ ОСІБ

13 березня урядове агентство з питань зайнятості Франції France Travail повідомило, що хакери викрали особисту інформацію приблизно 43 мільйонів осіб. Зловмисники отримали доступ до записів про шукачів роботи, які зареєструвалися в агентстві протягом останніх двох десятиліть. Викрадені дані включають повні імена, дати народження, номери соціального страхування (NIR), ідентифікатори France Travail, адреси електронної пошти, поштові адреси та номери телефонів.

11 ОБЛІКОВИХ ЗАПИСІВ ЕЛЕКТРОННОЇ ПОШТИ МІЖНАРОДНОГО ВАЛЮТНОГО ФОНДУ ЗЛАМАНО

Як 15 березня повідомило видання BleepingComputer, Міжнародний валютний фонд визнав кіберінцидент, виявлений минулого місяця, під час якого невідомі зловмисники зламали одинадцять облікових записів електронної пошти МВФ. Представник МВФ повідомив BleepingComputer, що постраждалі акаунти були знову захищені, але додаткові деталі не можуть бути розголошені з міркувань безпеки. Крім того, було підтверджено, що МВФ використовує служби електронної пошти Microsoft 365, хоча на основі результатів розслідування на той час не було схоже, що інцидент був пов'язаний з атакою на Microsoft.

ВІРОГІДНО РОСІЙСЬКЕ ЗЛОВМИСНЕ ПЗ ACIDPOUR, НАЦІЛЕНЕ НА ПРИСТРОЇ LINUX X86

19 березня видання The Hacker News повідомило, що в мережі виявлено новий варіант зловмисного програмного забезпечення AcidRain для стирання даних під назвою AcidPour, який спеціально розроблений для націлювання на пристрої Linux x86. AcidRain вперше з'явився на світ на початку російсько-української війни, коли це зловмисне ПЗ було розгорнуто проти модемів KA-SAT американської супутникової компанії Viasat. Згодом країни Five eyes, а також Україна та Європейський Союз приписали кібератаку росії. Наразі невідомо, проти кого планується застосувати це ПЗ, хоча компанія SentinelOne каже, що поінформувала українські урядові установи.

ПОНАД СТО ОРГАНІЗАЦІЙ СТАЛИ МІШЕННЮ ОСТАННІХ АТАК STRELASTEALER

22 березня з посиланням на звіт Palo Alto Networks, видання Security Week повідомило, що понад 100 організацій у США та ЄС стали мішенню нещодавніх масштабних фішингових кампаній, які розповсюджували зловмисне програмне забезпечення для викрадення інформації під назвою StrelaStealer. StrelaStealer збирає облікові дані від добре відомих клієнтів електронної пошти та надсилає їх на контрольований зловмисником сервер керування (C&C), указаний у конфігурації зловмисного програмного забезпечення. Спам-повідомлення в основному надсилалися організаціям у сфері високих технологій. Останні атаки включали вкладення ZIP, яке містило файл JScript, призначений для запуску остаточного корисного навантаження у формі DLL.

ФІНЛЯНДІЯ ПРИПИСУЄ КІБЕРАТАКУ НА ФІНСЬКИЙ ПАРЛАМЕНТ КИТАЙСЬКОМУ УГРУПОВАННЮ APT31

26 березня фінська поліція повідомила, що пов'язаний з Китаєм загрозливий актор APT31, стоїть за порушенням роботи фінського парламенту наприкінці 2020 року та на початку 2021 року, повідомляє BleepingComputer. У пресрелізі поліції сказано: «Кримінальне розслідування включало детальні дослідження та аналіз, а також міжнародний обмін інформацією. Національне бюро розслідувань тісно співпрацювало з міжнародними партнерами та Службою безпеки та розвідки Фінляндії. Кримінальне розслідування триває». Поліція встановила особу одного підозрюваного у причетності до події.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

СОЮЗНИКИ НІМЕЧЧИНИ ПО НАТО ЗАНЕПОКОЄНІ ТИМ, ЩО НІМЕЦЬКІ ВІЙСЬКОВІ ВИКОРИСТОВУЮТЬ МЕСЕНДЖЕР НА БАЗІ APPGALLERY HUAWEI

У грудні минулого року BWI GmbH, спеціалізований IT-провайдер Бундесверу, запустив застосунок BundesMessenger для п'яти мільйонів федеральних службовців (включно з військовими) – месенджер доступний в AppGallery Huawei, а також PlayMarket та AppStore. З 2021 року близько 100 тисяч німецьких солдатів використовують іншу програму – BwMessenger – також розроблену BWI, і яка також доступна у Huawei AppGallery. І Міністерство оборони Німеччини і BWI заявили, що програми в магазині Huawei безпечні. Однак кіберексперти з інших країн висловлюють сумніви щодо цього і занепокоєні тим, що КНР може отримати доступ до даних, що передаються цією мережею. Ці занепокоєння посилились після нещодавнього оприлюднили запису чотирьох офіцерів ВПС Люфтваффе. Міністерство внутрішніх справ Німеччини заявило, що в країні немає централізованої заборони на програмне або апаратне забезпечення китайського виробництва.

CISCO TALOS: НЕ ВСЕ МАЄ БУТИ ОБОВ'ЯЗКОВО «МАСОВОЮ ГЛОБАЛЬНОЮ КІБЕРАТАКОЮ»

У «Бюлетені джерел загроз» від 14 березня 2024 року, підготовленому Cisco Talos, досліджується сприйняття великих кібератак у контексті нещодавніх гучних збоїв у роботі відомих сервісів (збої у роботі Meta, Webex, AT&T тощо). У матеріалі обговорюється тенденція негайно підозрювати кібератаки за будь-якими технічними проблемами. Робиться висновок, що це спроба знайти швидкі та прості відповіді на складні питання, бажання потрапити у заголовки медіа та неготовність споживачів інформації сприймати складні пояснення. Однак у перспективі це може створити загрозу за моделлю «Обережно вовки» (численних фальшивих повідомлень про загрозу) і що суспільство може виявитись не готовим до справжньої масштабної кібератаки коли це станеться насправді.

США АКТИВНО БУДУЮТЬ ПЛАНИ ДЛЯ ЗАХИСТУ КОСМІЧНИХ ЗАСОБІВ ВІД КІБЕРЗАГРОЗ

Федеральні агентства та законодавці США вживають заходів для боротьби з новою кіберзагрозою в космосі. Агентство з кібербезпеки та безпеки інфраструктури (CISA) планує вивчити, чи є потреба в нових вимогах безпеки для космічних засобів і розширити можливості реагування на інциденти. Крім того, CISA має на меті посилити підтримку критичної інфраструктури, що залежить від можливостей космічного базування, у разі кібератаки. Законодавці Сенату представили законодавство для посилення супутникової кібербезпеки, вимагаючи від CISA розробити онлайн-ресурси, а від Білого Дому – створити федеральну стратегію боротьби з кіберзагрозами для супутникових систем. Попри те, що комітет схвалив законопроєкт, він очікує голосування у залі, оскільки законодавці вивчають варіанти його вдосконалення.

ВІД ДІПФЕЙКІВ ДО ЗЛОВМИСНОГО ПЗ: ЗРОСТАЮЧА РОЛЬ ШІ В КІБЕРАТАКАХ

Дослідники Insikt Group провели експерименти з різними моделями штучного інтелекту та описали висновки у звіті, опублікованому 19 березня.

Їхні висновки свідчать про те, що у 2024 році найбільш вірогідними способами зловмисного застосування ШІ будуть цільові діпфейки та операції впливу. Діпфейки, створені за допомогою інструментів з відкритим вихідним кодом, можна використовувати, щоб видати себе за керівників. А аудіо та відео, створені ШІ, можуть покращити кампанії соціальної інженерії. Очікується, що вартість створення контенту для операцій впливу значно знизиться, що полегшить клонування вебсайтів або створення фейкових ЗМІ. Штучний інтелект також може допомогти розробникам зловмисного ПЗ уникнути виявлення та допомогти суб'єктам загрози в розвідці, наприклад, у виявленні вразливих промислових систем або пошуку чутливих об'єктів.

RANSOMWARE НАЦІЛИЛИСЬ НА КАЗИНО ТА ІНДУСТРІЮ РОЗВАГ

27 березня Trustwave SpiderLabs заявило, що виявила зловмисників, що націлились на казино та індустрію розваг. Інциденти з MGM Resorts і Rivers Casino підкреслюють привабливість цього сектора для кіберзлочинців через значні обсяги фінансових і персональних даних. У блозі пропонується поглиблений аналіз різних ransomware груп, включаючи BlackCat/AlphV, Akira, Medusa, Royal і BianLian, з детальним описом їхніх методик і початкових векторів доступу.

ENISA ОПРИЛЮДНИЛА ПРОГНОЗ КІБЕРЗАГРОЗ ДО 2030 РОКУ

27 березня ENISA оприлюднила свій звіт «Передбачення загроз кібербезпеці до 2030 року», в якому описуються форсайтні передбачення нових кіберзагроз (або чинних, які збережуть свою актуальність), з якими може зіштовхнутись ЄС найближчим часом. Топ-10 загроз виглядає наступним чином:

- компрометація ланцюжків постачання у взаємопов'язаному ПЗ;
- нестача навичок;
- людські помилки та вразливості в старих кіберфізичних системах;
- експлуатація невиправлених старих систем у перевантаженій міжгалузевій технологічній екосистемі;
- зростання цифрового стеження з боку авторитарних урядів;
- транскордонні надавачі послуг як єдина точка помилок;
- просунута дезінформація та компанії операцій впливу;
- зростання просунутих гібридних загроз;
- зловживання ШІ;
- фізичний вплив на навколишнє середовище через знищення критичної цифрової інфраструктури.

5. КРИТИЧНА ІНФРАСТРУКТУРА

ЗРОСТАЮТЬ МАСШТАБИ НАСЛІДКІВ ВІД КІБЕРАТАКИ ПРОТИ UNITEDHEALTH GROUP

Хоча кібератака на один з підрозділів UnitedHealth Group – Change Healthcare відбулась ще 21 лютого, однак наслідки цієї кібератаки відчуваються і в березні 2024 року. Кібератака на підрозділ Change Healthcare мала прямий вплив на всю систему охорони здоров'я країни, яка сильно залежить від страхування. Change Healthcare обробляє близько 50% медичних вимог (страхування) у США, що містить в собі близько 900 тисяч лікарів, 33 тисяч аптек, 5 500 лікарень і 600 лабораторій. Атака вплинула на численних невеликих постачальників медичних послуг і аптеки, а споживачі стикались з проблемами відшкодування за медичні послуги. Як наслідок, 13 березня Міністерство охорони здоров'я та соціальних служб заявило про початок великого розслідування щодо цього зламу, аби дізнатися, чи не було порушено безпеку даних про здоров'я громадян та чи дотримувалась компанія законодавства США про конфіденційність у сфері охорони здоров'я. 27 березня Державний департамент США оголосив про винагороду в 10 мільйонів доларів за інформацію про ransomware банду Blackcat, яка відповідальна за цей кіберінцидент. Наразі точно невідомо як саме відбулося відновлення роботи UnitedHealth, але за деякими даними компанія пішла на співпрацю зі злочинцями та виплатила їм 22 мільйони доларів.

ВИЯВЛЕНО НИЗКУ КРИТИЧНИХ ЗАГРОЗ КІБЕРБЕЗПЕЦІ ПІДПРИЄМСТВАМ ГІРНИЧОДОБУВНОЇ ГАЛУЗІ

Стаття в блозі Trustwave, опублікована 1 березня 2024 року, присвячена загрозам і тенденціям кібербезпеки, що впливають на гірничодобувну галузь. У ній висвітлюються питання можливих збоїв роботі та крадіжка даних як наслідки швидкого переходу галузі на цифрові технології – це створює для зловмисників ширше поле для кібератак. У статті підкреслюється важливість надійних заходів кібербезпеки, планів реагування на інциденти та формування культури обізнаності з питань безпеки для подолання цих викликів.

ВИЯВЛЕНО БАГАТОСТУПЕНЕВУ АТАКУ ПРОТИ АМЕРИКАНСЬКОЇ АВТОМОБІЛЬНОЇ КОМПАНІЇ З ВИКОРИСТАННЯМ QR-КОДІВ

У публікації в блозі Proofpoint від 7 березня 2024 року обговорюється складна атака з використанням QR-коду, спрямована проти американської автомобільної компанії. Метою кампанії було здійснення шахрайства з компенсаціями. Для того, аби уникнути виявлення штатними системами захисту електронної пошти, зловмисники вбудували шкідливий QR-код в PDF-файл. А для додаткового заплутування систем захисту організації вхід на фішингову сторінку був «посилений» використанням CAPTCHA Cloudflare аби створити видимість легітимного ресурсу.

ДОРАДЧА ГРУПА БІЛОГО ДОМУ ВВАЖАЄ, ЩО РИНКОВИХ МЕХАНІЗМІВ «НЕДОСТАТНЬО», ЩОБ ЗАБЕЗПЕЧИТИ КІБЕРБЕЗПЕКУ ОКІ

Консультативний комітет з телекомунікацій національної безпеки, до складу якого входять представники найбільших телекомунікаційних компаній США, а також компаній з кібербезпеки, 7 березня опублікував звіт, в якому рекомендує федеральному уряду створити нові програми економічного стимулювання, такі як податкові знижки та федеральні гранти, щоб спонукати власників і операторів критичної інфраструктури підвищити стандарти кібербезпеки, розробити нові способи захисту від покарання під час обміну інформацією щодо кіберінцидентів, яка може бути загально корисною, та спростити дедалі складніший національний режим регулювання у сфері кібербезпеки.

УРЯД ВЕЛИКОБРИТАНІЇ ОПУБЛІКУВАВ ІНСТРУКЦІЇ З БЕЗПЕКИ В ХМАРІ ДЛЯ ОТ

Національний центр кібербезпеки Великої Британії (NCSC) опублікував інструкції, щоб допомогти організаціям, які використовують оперативні технології (ОТ), вирішити переносити чи ні свої системи диспетчерського контролю та збору даних (SCADA) у хмару. Документ містить розділи про розуміння рушійних сил бізнесу та хмарних можливостей, організаційної готовності та придатності технологій і хмарних рішень.

БІЛИЙ ДІМ ЗАКЛИКАЄ ШТАТИ ПОСИЛИТИ КІБЕРБЕЗПЕКУ У ВОДНОМУ СЕКТОРІ

За даними SecurityWeek, Агентство з охорони навколишнього середовища США (EPA) 19 березня оголосило про плани створити нову робочу групу, спрямовану на захист водного сектора від кібератак, спонсорованих державами. Адміністратор EPA Майкл Ріган і радник з національної безпеки Джейк Салліван надіслали листа всім губернаторам США, запросивши міністрів навколишнього середовища, охорони здоров'я та внутрішньої безпеки взяти участь в обговореннях щодо захисту критичної інфраструктури водного сектору від кіберзагроз. Рада національної безпеки (NSC) Білого дому та EPA закликають усі штати взяти участь у цьому діалозі, щоб сприяти швидкому вдосконаленню кібербезпеки водних ресурсів і зміцнити співпрацю між державними та федеральними органами та системами водопостачання.

ЧВЕРТЬ ПРОМИСЛОВИХ ОРГАНІЗАЦІЙ БУЛИ ЗМУШЕНІ ПРИПИНИТИ ФУНКЦІОНУВАННЯ СВОЇХ ОТ СИСТЕМ ЧЕРЕЗ КІБЕРАТАКИ – ДОСЛІДЖЕННЯ PALO ALTO NETWORKS

20 березня Palo Alto Networks оприлюднили результати проведеного ними у грудні 2023 року дослідження щодо безпеки ОТ-систем. Дослідження охопило дві тисячі респондентів з 16 країн. Три чверті респондентів сказали, що виявили зловмисну кіберактивність у своєму середовищі ОТ, а 24% сказали, що вони були змушені припинити роботу ОТ через успішну атаку – або через фактичний збій, або як превентивний захід.

УРЯД ТА ЕНЕРГЕТИЧНИЙ СЕКТОР ІНДІЇ ЗАЗНАЛИ ЗЛОМУ В РАМКАХ КАМПАНІЇ КІБЕРШПИГУНСТВА

27 березня видання The Record повідомило, що дослідники виявили нову шпигунську кампанію, націлену на урядові установи Індії та енергетичну галузь країни, яка здійснювалася за допомогою модифікованої версії викрадача інформації з відкритим кодом під назвою Hack-BrowserData. Ця версія, яка може збирати облікові дані для входу в браузер, файли cookie та історію. Дослідники голландської компанії з кібербезпеки EclecticIQ виявили кампанію на початку березня, але не приписали її конкретному загрозливому суб'єкту.

6. АНАЛІТИЧНІ ОЦІНКИ

ЄВРОПЕЙСЬКІ CSIRT МАЮТЬ ПЕРЕЙТИ ДО ПРОАКТИВНИХ МІСІЙ

У статті Тейлор Гроссмана «Європейські команди швидкого реагування в кіберпросторі повинні переорієнтуватись на проактивні місії», опублікованій 1 березня 2024 року на сайті Binding Hook, обговорюються поточні виклики які постали перед командами швидкого реагування в кіберпросторі НАТО і ЄС та їх ефективність. Дослідниця звертає увагу, що спроби створення команд реагування на рівні ЄС та НАТО малоефективні через складні бюрократичні процеси та не можливість швидко реагувати на зміну ситуацію. А отже їх можливості допомогти у дійсно кризовій ситуації досить незначні. Відтак вона наголошує, що такі команди мають перейти до проактивної моделі підтримки, адже саме національні команди будуть завжди більше залучені у подоланні криз і посиленні стійкості кібербезпеки своїх країн.

СУМА СЕРЕДНЬОГО ПОЧАТКОВОГО ВИКУПУ RANSOMWARE 2023 РОЦІ СЯГНУЛА 600 ТИСЯЧ ДОЛАРІВ США

Видання Security Boulevard повідомило 1 березня, що компанія Arctic Wolf, яка надає керовані послуги безпеки, виявила, що медіанний початковий викуп, який вимагають кіберзлочинці, зріс на 20% за рік до 600 тисяч доларів, причому в юридичному, державному, роздрібному та енергетичному секторах медіанна вимога становить один мільйон доларів США або більше. Загалом, виробництво, бізнес-послуги та освіта/некомерційні організації страждають найбільше, зазначається у звіті компанії. Більшість атак ransomware продовжують використовувати раніше відомі вразливості. Більше частина (60%) інцидентів пов'язані з вразливостями, розкритими до 2022 року. Лише 3,4% інцидентів пов'язані з використанням вразливостей нульового дня.

VOLT TYPHOON І НЕОБХІДНІСТЬ ПЕРЕГЛЯДУ КІБЕРСТРАТЕГІЇ США

5 березня у виданні Lawfare колишній заступник помічника Міністра з питань політики в Департаменті внутрішньої безпеки Пол Розенцвейг висловив думку, що нещодавнє кібервторгнення Китаю підкреслює необхідність перегляду стратегії кібербезпеки США. На його думку, атака Volt Typhoon підкреслює недоліки американської концепції «взаємно гарантованого зриву», яка базується на припущенні, що кіберзброї не переростуть у конфлікти в реальному світі. Стратегія США була спрямована на стримування прямих атак на американську інфраструктуру шляхом утримання китайських засобів під загрозою. Однак нещодавнє вторгнення Volt Typhoon свідчить про те, що Китай, можливо, розглядає масштабне руйнування інфраструктури як частину своєї стратегії конфлікту.

Масштаби вторгнень Volt Typhoon вказують на те, що Китай може планувати підривні дії на випадок геополітичної напруженості або військових конфліктів. Це ставить під сумнів припущення США про те, що руйнування інфраструктури неможливо уявити, і викликає занепокоєння щодо ефективності поточної стратегії стримування.

АНАТОМІЯ АТАКИ BLACKCAT ОЧИМА КОМАНДИ РЕАГУВАННЯ НА ІНЦИДЕНТИ

6 березня видання Security Week розмістило статтю, в якій йдеться про те, що команда з реагування на інциденти компанії Sygnia втрутилася, коли неназвана компанія зіткнулася з атакою ransomware, організованою BlackCat. Атака, ініційована через порушення ланцюга постачання, була спрямована на неправильно налаштовані Apache Hadoop, Confluence, Docker і Redis. Sygnia порадила жертві відключитися від Інтернету, щоб зловмисники не могли зашифрувати все середовище та стерти свої сліди. Попри спробу зловмисника викрасти дані та розпочати шифрування, рішучі дії зірвали їхні наміри, продемонструвавши важливість сміливих захисних заходів. Генеральний директор Sygnia підкреслив важливість розуміння поведінки зловмисників і терміновість реагування. Хоча зловмисникам вдалося викрасти деякі дані, рішучі дії жертви запобігли подальшій експлуатації. Цей інцидент підкреслює критичну роль своєчасного та рішучого реагування на інциденти, навіть перед обличчям неминучих загроз, у пом'якшенні кібератак і мінімізації їхнього впливу.

КІБЕРЗЛОЧИНЦІ ІМІТУЮТЬ УРЯДОВІ ОРГАНІЗАЦІЇ США ЧЕРЕЗ РОБОЧІ ЕЛЕКТРОННІ АДРЕСИ ТА ФІШИНГОВІ АТАКИ – PROOFPOINT

7 березня Security Week, розповіло, що принаймні з 2021 року організації в США стикалися з цілеспрямованими кампаніями з фішингу та компрометації бізнес електронної пошти (BEC) з боку зловмисника, відомого як TA4903, як продемонструвала компанія Proofpoint. Ці атаки були спрямовані на отримання корпоративних облікових даних, щоб вчиняти шахрайство з рахунками-фактурами або перенаправлення заробітної плати, для чого зловмисники часто створювали нові підроблені домени державних установ і приватних організацій у різних секторах. Спочатку, імітуючи державні установи, такі як Міністерство праці, актор розширив коло своєї діяльності та включив Департаменти житлового будівництва та міського розвитку, торгівлі, транспорту, сільського господарства та Управління малого бізнесу (SBA).

У середині 2023 року зловмисник перейшов до імітації малого та середнього бізнесу і посилив атаки BEC, запровадивши нові тактики, такі як QR-коди у вкладених PDF-файлах, і використовуючи теми-приманки, пов'язані з кібератаками та платежами. Крім того, зловмисник використовував безкоштовні адреси електронної пошти та домени, які підмінюють юридичні особи США, для доставлення фішингових повідомлень, демонструючи постійну еволюцію тактики, спрямованої на обман жертв. Компанія Proofpoint спостерігала, як актор намагався захопити існуючі потоки електронної пошти, що вказує на постійну загрозу кібербезпеці організацій.

У 2023 РОЦІ ЗБИТКИ ВІД КІБЕРЗЛОЧИННОСТІ ПЕРЕВИЩИЛИ 12,5 МІЛЬЯРДА ДОЛАРІВ – ФБР

7 березня Центр розгляду скарг на злочини в Інтернеті (IC3) ФБР опублікував річний звіт за 2023 рік, у якому йдеться, що кількість скарг на кіберзлочини зросла майже на 10%, порівняно з попереднім роком. В США подали понад 880 тисяч скарг, а збитки їх авторів склали понад 12,5 мільярдів доларів, що на 22% більше, ніж у 2022 році.

Фішинг залишається основним порушенням, за яким йдуть витоки особистих даних, вимагання та шахрайство з технічною підтримкою. Інвестиційне шахрайство спричинило найбільші збитки в розмірі 4,57 мільярда доларів США, за яким іде компрометація бізнес електронної пошти в розмірі 2,9 мільярда доларів США.

Скарги на ransomware перевищили 2800 зі збитками, що наближаються до 60 мільйонів доларів. Причому найбільш цільовими секторами стали охорона здоров'я, критичне виробництво, державні установи, IT та фінансові послуги. IC3 повідомила про успіх у відшкодуванні збитків від шахрайських грошових переказів, заморозивши майже 538 мільйонів доларів із зареєстрованих 758 мільйонів доларів, причому LockBit і BlackCat визначені як найактивніші групи ransomware.

ПРОГНОЗ КОМПАНІЇ THALES ЗА 2024 РІК ПОКАЗУЄ ЗРОСТАННЯ НЕБЕЗПЕКИ ВІД АТАК RANSOMWARE

Згідно з звітом 2024 Thales Data Threat Report, складеного компанією Thales на основі опитування майже 3000 спеціалістів з IT та безпеки у 18 країнах у 37 галузях, минулого року кількість компаній, які стали жертвами атаки ransomware, зросла на 27%, при цьому 8% сплатили викуп. 43% підприємств не пройшли перевірку відповідності, і ці компанії в 10 разів частіше страждають від витоку даних, другий рік поспіль помилки людини вважаються основною причиною витоку даних.

CISCO TALOS: ДЕТАЛІ НАПАДУ РОСІЙСЬКОГО УГРУПОВАННЯ TURLA НА ЄВРОПЕЙСЬКІ НУО

Cisco Talos опублікувала оновлення своїх попередніх висновків щодо кампанії кібершпигунства, проведеної російським загрозливим актором Turla. Кампанія була спрямована проти польської НУО, яка працює у сфері зміцнення польської демократії та допомоги Україні в умовах російського вторгнення, і використовувала нещодавно виявлений бекдор, відомий як TinyTurla-NG. Talos окреслює повний ланцюжок знищення, який використовує загроза, підкреслюючи їхню тактику налаштування виключень антивірусного програмного забезпечення, щоб уникнути виявлення їхнього бекдору перед розгортанням TinyTurla-NG. Після встановлення виключень бекдор записується на диск і встановлює постійну присутність.

У 2024 РОЦІ ВІДБУВАЄТЬСЯ ПОМІТНЕ ЗРОСТАННЯ ВИКОРИСТАННЯ ШІ У КІБЕРАТАКАХ – ЗВІТ TRUSTWAVE SPIDERLABS

У звіті Trustwave SpiderLabs 2024 «Технологічний ландшафт загроз» (від 20 березня) висвітлено зростаюче використання штучного інтелекту в атаках з використанням електронної пошти та фішингових атаках, що створює нові виклики для кібербезпеки. У звіті підкреслюється роль ШІ у створенні складного фішингового контенту, який обходить традиційні заходи безпеки, що спонукає до впровадження передових стратегій захисту.

ЗВІТ ВІД NSTAC: ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ Є ВАЖЛИВИМ ДЛЯ ЗНАЧНОГО ЗМЕНШЕННЯ РИЗИКІВ КІБЕРБЕЗПЕКИ

Президентський консультативний комітет із національної безпеки телекомунікацій (NSTAC) 20 березня 2024 року опублікував свій звіт «Вимірювання та стимулювання впровадження найкращих практик кібербезпеки» для телекомунікаційного сектору. В ньому обговорюються питання використання штучного інтелекту з метою істотного зниження ризиків кібербезпеки (як то раннього виявлення загроз, швидшого реагування на кіберінциденти). Також наголошується на проблемі не системності інвестицій в кібербезпеку – організації все більше вкладають в кібербезпекові рішення, однак часто ці рішення не сумісні між собою, що вказує на брак консолідованих, цілісних рішень у цій сфері.

ФОНД ЗАХИСТУ ДЕМОКРАТІЙ ЗАКЛИКАЄ КОНГРЕС США СТВОРИТИ НОВИЙ РІД ВІЙСЬК – КІБЕРСИЛИ

Автори дослідження, опублікованого 25 березня, закликають Конгрес США створити новий рід військ, який займатиметься операціями з кібербезпеки та буде працювати поряд з ВПС, ВМС та іншими родами військ. Вони стверджують, що поточні військові конфігурації не створюють найкращих умов для США у боротьбі з супротивниками у кіберпросторі. Дослідження ґрунтується на інтерв'ю з близько 75 анонімними нинішніми та відставними військовослужбовцями. Пропонується створити кіберсили, які будуть частиною збройних сил та матимуть 10 000 військовослужбовців і бюджет у 16,5 мільярдів доларів

У РАЗІ МАСШТАБНОГО КОНФЛІКТУ З КИТАЄМ, КИТАЙСЬКІ КІБЕРАТАКИ БУДУТЬ БІЛЬШОЮ МІРОЮ НАЦІЛЕНІ НА ДОСЯГНЕННЯ ПСИХОЛОГІЧНОГО ВПЛИВУ НА АМЕРИКАНСЬКИХ ГРОМАДЯН

Дослідник Джошуа Ровнер у своєму матеріалі від 25 березня, аналізує ситуацію навколо можливого конфлікту між США та КНР та поведінки сторін у кіберпросторі. Він вказує на те, що американські офіційні особи підкреслюють можливі катастрофічні наслідки китайських кібердій, однак він звертає увагу на дві обставини. Перша – більшість дійсно важливих військових мереж від'єднанні від мережі Інтернет і маловразливі перед хакерськими атаками. Друга – китайські кібератаки проти цивільної інфраструктури будуть більше спрямовані на соціальні ефекти (викликання паніки), ніж на виведення з ладу цих систем, як елементу військових завдань.

ОГЛЯД ЕКСПЛОЙТІВ НУЛЬОВОГО ДНЯ У 2023 РОЦІ

27 березня Google Threat Analysis Group (TAG) і Mandiant опублікували звіт про вразливості нульового дня у 2023 році, виявивши, що минулого року було використано 97 таких вразливостей. Постачальники комерційного відеоспостереження (CSV) стояли за 75% використаних вразливостей нульового дня, які вплинули на продукти Google. У звіті зазначається: «Усі вразливості, які ми віднесли до CSV у 2023 році, стосувалися мобільних пристроїв і браузерів, і CSV спричинили 64% усіх використовуваних вразливостей мобільних пристроїв і браузерів (24 із 37).

НАСТАВ ЗОЛОТИЙ ВІК АВТОМАТИЗОВАНОГО ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

У статті, опублікованій The Hacker News 29 березня, наголошується на важливості пентестування у виявленні вразливостей, якими можна скористатися. Поточний метод тестування є дорогим, тому багато компаній проводять його лише за необхідності, зазвичай раз на рік для відповідності вимогам. Однак нові технології, що використовують автоматизацію та ШІ, зробили революцію в цьому процесі, зробивши регулярне пентестування мережі легким і доступним. Автори тексту наводять переваги автоматичного тестування.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

ПРЕЗИДЕНТ УКРАЇНИ ПРЕДСТАВИВ СЕКРЕТАРЯ РНБО ОЛЕКСАНДРА ЛИТВИНЕНКА Й ОКРЕСЛИВ П'ЯТЬ КЛЮЧОВИХ ЗАВДАНЬ ДЛЯ РАДИ, СЕРЕД ЯКИХ ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА

Президент України Володимир Зеленський 29 березня представив новопризначеного Секретаря Ради національної безпеки і оборони України Олександра Литвиненка. Президент окреслив ключові завдання для нового Секретаря Ради національної безпеки і оборони України, серед яких: є посилення можливостей України в прогнозуванні, санкційна політика, доктринальна робота та робота Ставки Верховного Головнокомандувача, інформаційна та кібербезпека, проєкти рішень та контроль за їх виконанням.

РНБО УКРАЇНИ ВІДІГРАВАТИМЕ КЛЮЧОВУ РОЛЬ У КООРДИНАЦІЇ ТА РОЗВИТКУ СПРОМОЖНОСТЕЙ УДАРНОГО КІБЕРПОТЕНЦІАЛУ КРАЇНИ

Кібербезпека та інформаційна безпека, зокрема зміцнення захисту від ворожих дестабілізаційних операцій та посилення координації всіх державних інституцій у цій сфері, а також розвиток спроможності ударного кіберпотенціалу країни визначені Президентом України Володимиром Зеленським як пріоритетний напрямок оновленої роботи Рада національної безпеки і оборони України. Про це він заявив під час представлення новопризначеного секретаря РНБО України Олександра Литвиненка.

НКЦК ПОГЛИБЛЮЄ СПІВПРАЦЮ З КМЄС ЗАДЛЯ ПОСИЛЕННЯ КІБЕРСТІЙКОСТІ УКРАЇНИ ТА КРАЇН-ЄС

Заступник Секретаря РНБО України Сергій Демедюк, керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України Наталія Ткачук та керівник управління забезпечення діяльності НКЦК Сергій Прокопенко 14 березня 2024 року провели робочу зустріч з керівником відділу національної та державної безпеки Консультативної Місії Європейського Союзу Юха Вехмаскоскі. Під час зустрічі були обговорені ключові аспекти співпраці між Україною та Європейським Союзом у сфері кібербезпеки. Особливу увагу було приділено шляхам поглиблення практичного співробітництва для ефективної розбудови національної системи кібербезпеки України та обміну досвідом з країнами ЄС.

МІНОБОРОНИ ПРЕЗЕНТУВАЛО ІННОВАЦІЙНІ РІШЕННЯ ЩОДО ЦИФРОВІЗАЦІЇ СТАНДАРТІВ НАТО

Представники Центру інновацій Міноборони взяли участь в щорічній конференції НАТО TIDE Sprint 2024 у Дрездені, яка сприяє розвитку військових IT-систем НАТО та країн-партнерів. Вони продемонстрували, як за допомогою хмарних обчислень та обробки великих даних цифровізовувати вже чинні стандарти НАТО, а також поділились досвідом розробки екосистеми управління бойовим простором DELTA. Окрему увагу було приділено процесам покращення кібербезпеки, а також презентовано технологію інтеграції дронів до системи DELTA та інших систем, що відбувається завдяки співпраці з Мінцифрою, партнерами з ГО «Аеророзвідка» та компанією Cossack Labs.

РФ ВЕДЕ КІБЕРВІЙНУ НЕ ЛИШЕ ПРОТИ УКРАЇНИ, А Й КРАЇН ЄС І НАТО

Керівник служби з питань інформаційної безпеки та кібербезпеки Апарату РНБО України, секретар НКЦК Наталія Ткачук, відкриваючи захід у Чернівецькій військовій адміністрації, зазначила, що кібератаки вже стали невід'ємним інструментом, який використовує ворог проти України. «Проте сьогодні рф веде кібервійну не лише проти нашої держави, а й країн Європейського Союзу та НАТО. І ми розуміємо, що війна в кіберпросторі триватиме навіть після припинення військових дій на полі бою. Тож сьогодні як ніколи важливо вміти ефективно та оперативно реагувати на кіберзагрози на всіх рівнях: як на загальнодержавному та регіональному всередині країни, так і на міждержавному – взаємодіючи з нашими партнерами», – зазначила секретар НКЦК.

УКРАЇНА МАЄ СТАТИ РЕГІОНАЛЬНИМ ЛІДЕРОМ ІЗ КІБЕРБЕЗПЕКИ

Про це заявив заступник Секретаря РНБО України Сергій Демедюк під час XV Всеукраїнської науково-практичної конференції Національної академії СБУ «Актуальні проблеми управління інформаційною безпекою держави». «Україна не може чекати, доки міжнародна спільнота почне нормативно розділяти кіберагресію від кіберзлочинності, а повинна сама ініціювати це вже зараз, тому що Україна вже не є полігоном для відпрацювання кібератак росіянами, це вже фронт. І, зважаючи на наш досвід, маємо стати регіональним лідером із кібербезпеки» – наголосив він.

90% КРИТИЧНИХ КІБЕРІНЦИДЕНТІВ ВІДБУВАЮТЬСЯ САМЕ В РЕГІОНАХ

Представники Національного координаційного центру кібербезпеки при РНБО України та Національного Департаменту кібербезпеки Румунії провели офлайн-тренінги з кібербезпеки для представників громад, об'єктів критичної інфраструктури та студентів Чернівецької області. Представники НКЦК зазначили, що 90% критичних кіберінцидентів відбуваються саме в регіонах. Тому в межах заходу понад 50 представників суб'єктів кібербезпеки та об'єктів критичної інфраструктури регіону детально обговорили ключові загрози кібербезпеці регіонів та напрями протидії. Особливу увагу було приділено проблемним питанням взаємодії на регіональному рівні та викликам у підвищенні обізнаності про кібербезпеку.

ЗА ПІДТРИМКИ НКЦК РОЗПОЧАЛОСЬ НАВЧАННЯ ВЕТЕРАНІВ І ВЕТЕРАНОК ЗА ПРОГРАМОЮ РЕІНТЕГРАЦІЇ «КІБЕРЗАХИСНИКИ»

Головна мета програми полягає у створенні умов для отримання ветеранами необхідних навичок та знань для успішної кар'єри у сфері кібербезпеки. Проєкт передбачає комплексне навчання з кіберзахисту та кібероборони, а також сприяє працевлаштуванню в державному секторі або інституціях сектору кібербезпеки України. Впродовж курсу учасники, з-поміж іншого, вивчатимуть принципи кібербезпеки та їх застосування, техніки шифрування та їх роль у захисті інформації, а також розпізнавання та реагування на різноманітні типи кібератак.

GOOGLE ЗАПУСКАЄ БЕЗОПЛАТНУ НАВЧАЛЬНУ ОНЛАЙН-ПРОГРАМУ «ОСНОВИ КІБЕРБЕЗПЕКИ ДЛЯ БІЗНЕСУ»

Програма «Безпечніше з Google» призначена для власників, керівників та співробітників малих і середніх підприємств, які бажають захистити свій бізнес від кіберзагроз, отримати практичні знання про кібергігієну та розпізнавання кібератак. У навчальний план входять 4 навчальні тренінги з практичними завданнями, бізнес-кейси та опціональні 1:1 консультації. Учасники зможуть скористатися досвідом провідних українських експертів у захисті бізнесу та даних клієнтів. Детальніше про програму та реєстрацію можна дізнатися за посиланням.

МІНЦИФРА ТА КІБЕРПОЛІЦІЯ СПІЛЬНО З ВГО «МАГНОЛІЯ» ЗАПУСТИЛИ ПОРТАЛ ПОВІДОМЛЕНЬ ПРО СЕКСУАЛЬНЕ НАСИЛЬСТВО НАД ДІТЬМИ В ІНТЕРНЕТІ

З 4 березня в Україні діє перший портал повідомлень про матеріали, пов'язані із сексуальним насильством над дітьми в мережі – StopCrime. Повідомити про можливий злочин на тему сексуального насильства над дітьми в інтернеті можна за посиланням: https://stopcrime.ua/net-crime. Надіслане повідомлення може бути анонімним. Головне надати посилання, де розміщено контент. Для подальшого розслідування та блокування такого контенту громадська організація «Магнолія», як член Міжнародної мережі, збиратиме, аналізуватиме та передавати його до Департаменту кіберполіції та в Інтерпол.

ОЧІЛЬНИК КІБЕРПОЛІЦІЇ ЮРІЙ ВИХОДЕЦЬ ВЗЯВ УЧАСТЬ У ДВОДЕННОМУ ТРЕНІНГУ, ПРИСВЯЧЕНОМУ ВДОСКОНАЛЕННЮ РОБОТИ ПІДРОЗДІЛУ

Під час заняття про формування іміджу кіберполіцейського, ініційовані громадською спілкою «Глобальний центр взаємодії в кіберпросторі», учасники обговорили стратегії співпраці з громадськістю та підвищення довіри до кіберполіції. Учасники також розглянули стратегії розвитку кіберполіції для підвищення ефективності та її міжнародний імідж, включаючи розкриття онлайн шахрайств, участь в міжнародних операціях і співпраця з Європолом за допомогою мережевої платформи SIENA. Також учасники обговорили питання кіберзахисту, протидії кіберзлочинам та отримання цифрових доказів.

ПРЕДСТАВНИКИ НКЦК ТА ДИРЕКТОРАТУ З КІБЕРБЕЗПЕКИ РУМУНІЇ ПРОВЕЛИ ЛЕКЦІЇ ДЛЯ СТУДЕНТІВ ЧНУ ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА

У рамках робочого візиту до Чернівців, представники НКЦК при РНБО України та Національного Директорату з кібербезпеки Румунії провели захід для студентів Чернівецького національного університету імені Юрія Федьковича. Під час заходу фахівці НКЦК розповіли слухачам про важливість професій у сфері кібербезпеки, а також поділилися зі студентами своїм досвідом і знаннями у сфері міжнародного співробітництва та протидії хакерським угрупованням. Крім того, гості з Румунії представили студентам важливий матеріал про правила кібергігієни та презентували посібник з безпечного використання соцмереж, що стане корисним інструментом для молодого покоління у сучасному світі.

ДЕРЖСПЕЦЗВ'ЯЗКУ АКТИВНО ВИКОРИСТОВУЄ КІБЕРПОЛІГОНИ ДЛЯ НАВЧАННЯ ТА ТРЕНУВАННЯ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

На конференції «Цифрова трансформація як каталізатор європейської інтеграції України» заступник Голови Держспецзв'язку Олександр Потій розповів, що Державна служба спеціального зв'язку та захисту інформації України активно використовує кіберполігони для підготовки не лише власних фахівців, але й спеціалістів з інших державних структур та об'єктів критичної інфраструктури. Навчання відбувається як на власних полігонах Держспецзв'язку, так і на майданчиках партнерів з США, Естонії та інших країн. У найближчому майбутньому подібними полігонами планується обладнати регіональні центри кібербезпеки. Це дасть змогу створити мережу, яка буде забезпечувати не лише навчання фахівців на місцях, але й віддалене навчання спеціалістів з усієї країни.

ПРИ ДЕРЖСПЕЦЗВ'ЯЗКУ ПОЧАЛА РОБОТУ ГАЛУЗЕВА РАДА З РОЗРОБКИ ПРОФСТАНДАРТІВ

Галузева рада займатиметься організацією та безпосереднім розробленням професійних стандартів у галузі інформаційних технологій, кібербезпеки та захисту інформації. Також члени галузевої ради братимуть участь у розробці стандартів освіти, стандартів та інструментів оцінювання кваліфікацій і результатів навчання, у прогнозуванні потреб у відповідних кадрах. До складу галузевої ради увійшли представники державних органів, відповідальних за кібербезпеку, освітяни та науковці, представники професійної та громадської спільноти. У ході першого засідання вони обговорили питання розбудови кадрового потенціалу та створення Національної рамки кваліфікацій України з кібербезпеки, введення професійних стандартів у промисловий сектор і в освітній процес, а також план роботи на 2024 рік.

ЗА ПІДТРИМКИ USAID ВІДБУЛАСЯ КОНФЕРЕНЦІЯ «КІБЕРДІАГНОСТИКА КРИТИЧНОЇ ІНФРАСТРУКТУРИ: ПОСИЛЕННЯ ЦИФРОВОГО ЗАХИСТУ»

Під час конференції учасники обмінювались досвідом та ідеями, отриманими під час реалізації Програми діагностики стану кібербезпеки операторів критичної інфраструктури (ОКІ) від Проєкту USAID «Кібербезпека критично важливої інфраструктури України». Програма розроблена на основі настанов NIST Cybersecurity Framework, які допомагають організаціям удосконалити цифровий захист. На сьогодні запущено 40 кібердіагностик та 20 організацій отримали перші результати. Також учасники ознайомилися з нормативно-правовими вимогами до проведення кібердіагностик та підходами до оцінки рівня кіберзахисту ОКІ.

ФАХІВЦІВ ФІНАНСОВОГО СЕКТОРУ НАВЧАЛИ ЗАХИЩАТИСЯ ВІД КІБЕРАТАК

Держспецзв'язку за підтримки проєкту EU4DigitalUA провели командно-штабні навчання CIREX.CYBER.Ransomware, у яких взяли участь майже три десятки фахівців з державних органів і приватних організацій фінансового сектору. Учасники вчилися боротися з кібератаками за допомогою програм-вимагачів. Також серед важливих завдань командно-штабних навчань було отримання інформації щодо того, наскільки ефективно різні органи, установи та підприємства здатні взаємодіяти між собою, оперативно обмінюватися інформацією про кіберінциденти та у разі виявлення проблем – віднайти шляхи їх розв'язання.

ДЕРЖАВНИЙ ЦЕНТР КІБЕРЗАХИСТУ СПІЛЬНО З UNIT 42 PALO ALTO NETWORKS ПРОВІВ ДОСЛІДЖЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ SMOKELOADER

Державний центр кіберзахисту Держспецзв'язку (ДЦКЗ) спільно з командою дослідників загроз Unit 42 компанії Palo Alto Networks детально дослідив шкідливе програмне забезпечення SmokeLoader. Дослідження сфокусовано на відстежування розповсюдження SmokeLoader в Україні у період з травня по листопад 2023 року. За цей період зафіксовано значне зростання атак, пов'язаних із застосуванням цього програмного забезпечення, на державний, оборонний та фінансовий сектори (у звіті проаналізовано 23 хвилі фішингових атак). Завантажити звіт можна за посиланням:
https://scpc.gov.ua/api/files/8e300d33-6257-4d7f-8f72-457224268343

ГУР РОЗПОВІЛО ПРО НОВІ МАСШТАБНІ АТАКИ НА РОСІЮ

Під ударом опинились не лише російські державні, а й приватні структури, які сплачують податки та фінансують війну проти України. Упродовж тижня з 11 по 18 березня 2024 року:

- атаковано ресурси ПАТ «ростєлєком» — виведено з ладу комунікаційне обладнання забайкальського та красноярського краю рф;
- отримано доступ до системи електронного документообігу «правітєльства бєлгородской області», здійснено фейкові розсилки 12 тисячам місцевих чиновників;
- атаковано та виведено з ладу комунікаційне обладнання ТОВ «бєлзнак»;
- захоплено та знищено серверну інфраструктуру разом з резервними копіями хостінг-провайдера «1Gb.ru» та десятків тисяч веб-сайтів, які він обслуговував;
- виведено з ладу понад 40 мережевих пристроїв Mikrotik в «центрє управлєнія городскім автоелєктротранспортом» у новосібірску.

Завдані ворогу збитки можуть обчислюватись сотнями тисяч доларів.

КІБЕРФАХІВЦІ СБУ ЗАБЛОКУВАЛИ ПОСТАЧАННЯ КОМПЛЕКТУЮЧИХ ДЛЯ ПАРТІЇ РОСІЙСЬКИХ «ШАХЕДІВ» І КРИЛАТИХ РАКЕТ

Про це розповів начальник Департаменту кібербезпеки СБУ Ілля Вітюк в ефірі телемарафону. «Ми здійснюємо перекриття ланцюгів постачання комплектуючих до російської зброї. Один із прикладів – вже заблокували постачання сервомоторів для виробництва 1600 «Шахедів» і 4000 мікросхем для крилатих ракет», – повідомив Ілля Вітюк. Окрім того, він розповів, що кіберфахівці працюють на лінії фронту над знищенням ворожих систем РЕБ і РЕР, а також над перехопленням ворожих безпілотників, які координують ракетні та артилерійські удари по Силах оборони.

ГУР РОЗПОВІЛО ПРО ЗЛАМ МІНОБОРОНИ РОСІЇ

ГУР МО України розповіло, що реалізувало чергову успішну спецоперацію проти держави-агресора росії — у результаті атаки вдалось отримати доступ до серверів міністерства оборони рф. Тепер українська спецслужба володіє програмним забезпеченням для захисту інформації та шифрування, яке використовувало мо рф, а також — масивом секретної службової документації російського міністерства війни. Йдеться про накази, звіти, розпорядження, доповіді та інші документи, які циркулювали між понад 2000 структурних одиниць силового відомства росії. Одержана інформація дозволяє встановити повну будову системи російського міноборони та його ланок.

СБУ СПІЛЬНО З ПРАВООХОРОНЦЯМИ ЛАТВІЇ ЗНЕШКОДИЛА ПІДПІЛЬНИЙ КОЛ-ЦЕНТР, ЯКИЙ ВИДУРЮВАВ ГРОШІ У ГРОМАДЯН ЄС

Кіберфахівці Служби безпеки спільно з Нацполіцією, прокуратурою та правоохоронними органами Латвійської Республіки ліквідували міжнародну схему виманювання коштів з інвесторів електронних бірж. Зловмисники створили підпільний кол-центр, який діяв під виглядом одного із незалежних фінансових регуляторів ЄС та пропонували європейським вкладникам у фондові проєкти онлайн-бірж «захист інвестицій». Таким чином шахраї сподівались видурювати у потерпілих мільйонні суми у гривневому еквіваленті. Однак співробітники СБУ викрили зловмисників на «старті» їхньої злочинної діяльності, задокументували декілька фактів шахрайських маніпуляцій і затримали головних фігурантів. Їм загрожує до 8 років тюрми.

ЧЕРКАСЬКІ КІБЕРПОЛІЦЕЙСЬКІ ВИКРИЛИ ШКОЛЯРА, ЯКИЙ АДМІНІСТРУВАВ TELEGRAM-КАНАЛ ІЗ ЗАБОРОНЕНИМ КОНТЕНТОМ

14-річний киянин створив Telegram-канал через який розповсюджував заборонені матеріали, в тому числі й порнографічного характеру. За видалення таких публікацій він вимагав гроші. За місцем проживання підлітка правоохоронці провели санкціонований обшук. Слідчі вилучили мобільний телефон з якого здійснювалося адміністрування Telegram-каналу та інші речові докази, які підтверджують факт вчиненого правопорушення. Слідство триває.

СБУ ЗАТРИМАЛА «КРОТА» ФСБ, ЯКИЙ НАМАГАВСЯ ВЛАШТУВАТИСЯ ДО ПОЛІЦІЇ, ЩОБ ШПИГУВАТИ ЗА «ГВАРДІЄЮ НАСТУПУ» ТА ПІДРОЗДІЛАМИ ЗСУ

Кіберфахівці Служби безпеки зірвали спробу фсб «завести» свого агента до складу Сил оборони України. У результаті спецоперації на Київщині затримано зрадника, який за вказівкою фсб намагався влаштуватися до Національної поліції та збирати інформацію про підрозділи правоохоронного органу, насамперед ті, що входять до «Гвардії наступу» МВС України. Він був завербований російськими спецслужбами через його прокремлівські коментарі в російських Telegram-каналах. Також він передавав геолокації «потрібних» об'єктів російському куратору та отримував грошову винагороду за це. Під час обшуку у нього вилучили мобільний телефон з доказами спілкування з ФСБ. Затриманий підозрюється у державній зраді і під вартою йому загрожує довічне ув'язнення.

КІБЕРПОЛІЦЕЙСЬКІ ХАРКІВЩИНИ ВИКРИЛИ ЧЛЕНІВ ЗЛОЧИННОГО УГРУПОВАННЯ, ЯКЕ ПРИВЛАСНЮВАЛО ОБЛІКОВІ ЗАПИСИ КОРИСТУВАЧІВ ІНТЕРНЕТУ

Правоохоронці оголосили підозру трьом членам організованої злочинної групи, які привласнювали чужі електронні поштові скриньки та акаунти в Instagram. Фігуранти використовували метод брутфорсу для підбору паролів та за рік сформували базу викрадених облікових записів понад 100 мільйонів користувачів з усього світу. Вони мешкали у різних регіонах України та розподіляли обов'язки через інтернет, формуючи бази для продажу в даркнеті. Наразі зловмисникам оголошено підозру, їм загрожує 15 років позбавлення волі. Також відпрацьовується версія співпраці фігурантів з агентами країни-агресора, оскільки викрадені акаунти, зокрема, використовувались для проведення ІПСО в інтересах рф.

ПОЛІЦЕЙСЬКІ ВИКРИЛИ ЗЛОЧИННУ ГРУПУ, ЯКА ЧЕРЕЗ ФІШИНГОВИЙ ВЕБСАЙТ ВИМАНЮВАЛА У ЛЮДЕЙ ГРОШІ

Правоохоронці припинили діяльність шахраїв, які за допомогою фішингових сайтів викрадали необхідні дані громадян для несанкціонованого втручання в інтернет-банкінг і проводили транзакції з банківських рахунків потерпілих. Встановлено, що збитки від їх дій становлять майже 119 тисяч гривень. Чотирьом фігурантам повідомили про підозру. Їм загрожує до 8 років позбавлення волі.

ВІД ПОЧАТКУ РОКУ РОСІЙСЬКІ ХАКЕРИ АКТИВІЗУВАЛИ АТАКИ ПРОТИ УКРАЇНИ

Перші місяці цього року демонструють збільшення кількості кібератак, які здійснюють російські хакери на українські інформаційні системи. Тому варто очікувати, що 2024 рік для нашої країни буде важчим з погляду ведення кібервійни. Про це у коментарі виданню The Economist сказав Голова Держспецзв'язку Юрій Мироненко. За його словами 10% атак здійснюються кіберпідрозділами російських спецслужб, а решта – афілійованими злочинними хакерськими групами. При цьому найактивнішим російським кіберпідрозділом є «Армагеддон», який належить фсб.

8. ПЕРША СВІТОВА КІБЕРВІЙНА

РОСІЯ ПРАГНЕ ВИКОРИСТАТИ «ВТОМУ ВІД ВІЙНИ» ЗАХОДУ ДЛЯ ПЕРЕМОГИ В УКРАЇНІ

Нове дослідження Insikt Group, опубліковане 29 лютого, присвячено стратегічному підходу росії до її війни проти України, та те, як цей підхід взаємодіє з уявленнями та політикою Заходу. У кремлі вважають, що країни Заходу відчувають «втому від війни», що робить подальшу економічну та військову підтримку України дедалі менш популярною. Попри це росія визнає, що Захід має можливості продовжувати підтримувати Україну, і прагне вплинути на вибори на Заході у 2024 році та використати політичні занепокоєння щодо подальшої підтримки України.

У РОСІЙСЬКИХ УНІВЕРСИТЕТАХ СТУДЕНТІВ СИСТЕМНО НАВЧАЮТЬ ХАКЕРСТВА — СБУ

В інтерв'ю журналу Forbes керівник департаменту кібербезпеки СБУ Ілля Вітюк серед іншого повідомив, що СБУ має документи, які свідчать, що національна система масштабування кіберагресії у рф працює мінімум з 2016 року. Офіцери чинного резерву ГРУ та ФСБ навчають студентів кібернаступальних дисциплін у військових та технічних вишах. Студенти проводять науково-технічні роботи зі створення програмних засобів, вивчають архітектуру логістики, енергетики, водопостачання України та інших країн, пишуть курсові та магістерські роботи про це. Після навчання здібних студентів можуть брати на роботу в урядові розвідувальні органи чи до спецслужб.

MICROSOFT ПІДТВЕРДЖУЄ, ЩО РОСІЙСЬКІ ХАКЕРИ ВКРАЛИ ВИХІДНИЙ КОД І ДЕЯКІ СЕКРЕТИ КЛІЄНТІВ

8 березня компанія Microsoft повідомила, що підтримуваний кремлем загрозливий актор Midnight Blizzard (він же APT29 або Cosy Bear) після злому, про який стало відомо у січні 2024 року, зміг отримати доступ до деяких сховищ її вихідного коду та внутрішніх систем. Компанія підкреслила, що поки не знайшла доказів того, що клієнтські системи, розміщені на сервері Microsoft, були скомпрометовані. Компанія Redmond, яка продовжує розслідувати масштаби порушення, заявила, що російська державна установа намагається використати різні типи секретної інформації, які вона знайшла під час атаки, включно з тими, якими клієнти та Microsoft обмінювалися електронною поштою.

УРЯД ФРАНЦІЇ ЗАЗНАВ КІБЕРАТАК «БЕЗПРЕЦЕДЕНТНОЇ» ІНТЕНСИВНОСТІ

11 березня Прем'єр-міністр Франції заявив, що урядові установи країни зазнали кібератак «безпрецедентної інтенсивності». Описи інцидентів свідчать про DDoS атаку. Французький уряд створив кризовий підрозділ для врегулювання ситуації. Хто стоїть за нападами, поки невідомо. Проросійська хакерська група Anonymous Sudan у своєму Telegram-каналі взяла на себе відповідальність за «масовану кібератаку» на інфраструктуру Міжміністерського управління цифрових справ Франції.

УКРАЇНСЬКІ ХАКЕРИ ЗЛАМАЛИ СИСТЕМУ ОПЛАТИ ПРОЇЗДУ МОСКОВСЬКОГО МЕТРО

13 березня Міністерство цифрової трансформації України повідомило, що українська IT-армія атакувала низку урядових та місцевих порталів, серед них – система оплати проїзду «Тройка». Це одна з найбільших систем оплати квитків у росії, яка обслуговує 38 регіонів. Тож через «збій» власники транспортних карток у москві та казані не могли оплатити квитки, поповнити картку проїзду та розрахуватися за паркування.

ЗА ДАНИМИ NSA, РОСІЯ СПРОБУЄ ВПЛИНУТИ НА АМЕРИКАНСЬКІ ВИБОРИ З МЕТОЮ ПОСЛАБЛЕННЯ ПІДТРИМКИ УКРАЇНИ

15 березня один з керівників АНБ США Роб Джойс, відповідаючи на питання журналістів, повідомив, що за їхніми даними основні зусилля росії з підриву американських виборів будуть спрямовані на зменшення підтримки України. Особливу роль в цьому можуть відігравати такі інструменти як ChatGPT або інші генеративні ШІ, які дозволяють одній людині продукувати одразу багато правдивого контенту.

ГРУПА, ПОВ'ЯЗАНА З SANDWORM, ЙМОВІРНО, ВИВЕЛА З ЛАДУ УКРАЇНСЬКИХ ІНТЕРНЕТ-ПРОВАЙДЕРІВ

російські державні хакери, ймовірно, стоять за недавніми атаками на чотири невеликих українських інтернет-провайдерів, що призвели до збою їхньої роботи, який тривав понад тиждень. Відповідальність за ці інциденти у своєму Telegram-каналі взяло на себе Угруповання «Солнцепек». Українські чиновники повідомили, що є докази, що це угруповання вірогідно також стоїть за кібератакою 2023 року на «Київстар».

GPS І ЗВ'ЯЗОК ЛІТАКА МІНІСТРА ОБОРОНИ ГРАНТА ШЕППСА БУЛО ПОРУШЕНО ЧЕРЕЗ АТАКУ ЗАСОБАМИ РЕБ

15 березня російські хакери зламали GPS і зв'язок літака Dassault Falcon 900 Міністра оборони Великобританії Гранта Шаппса за допомогою атаки засобами РЕБ. Літак Міністра оборони Гранта Шаппса вилетів з Польщі, де він відвідав британські війська на навчаннях Steadfast Defender, до Великобританії. Під час візиту Глава Міноборони Великої Британії підтвердив повну підтримку України з боку його держави. Пілоти RAF підтвердили, що GPS та інші комунікаційні сигнали літака були заблоковані протягом майже 30 хвилин, поки міністр летів поблизу російського м. Калінінград, що сусідить з Польщею.

РОСІЯНИ БІЛЬШЕ НЕ ЗМОЖУТЬ ОТРИМАТИ ДОСТУП ДО ХМАРНИХ СЕРВІСІВ MICROSOFT ТА ЗАСОБІВ БІЗНЕС-АНАЛІТИКИ

Microsoft планує цього місяця призупинити доступ до своїх хмарних сервісів для російських користувачів через європейські санкції, накладені на росію після її вторгнення в Україну. Softline, один з найбільших дистриб'юторів продуктів Microsoft у росії, оголосив, що місцеві користувачі втратять доступ до хмарних сервісів Microsoft 20 березня. Кілька інших місцевих технологічних компаній також отримали попередження від Microsoft про призупинення. Однак, за неофіційною інформацією Microsoft, призупинення може бути відкладено до кінця місяця.

НА ДУМКУ КЕРІВНИЦТВА CISA КНР МОЖЕ ВИКОРИСТАТИ РОСІЙСЬКУ ТАКТИКУ АТАКИ НА ОКІ

21 березня Джен Істерлі, директорка Агентства кібербезпеки та захисту інфраструктури, обговорює критичну важливість підтримки України з боку США на тлі російських кінетичних та кібератак. У статті підкреслюються ширші наслідки конфлікту для глобальної кібербезпеки, а також те, як такі супротивники, як Китай, можуть використовувати подібну тактику проти критично важливої інфраструктури США та їхніх союзників. Вона підкреслює необхідність постійної підтримки для стримування супротивників і захисту демократичних цінностей від авторитарних загроз.

США ЗАПРОВАДИЛИ САНКЦІЇ ПРОТИ РОСІЯН, ЯКІ СТОЯТЬ ЗА КАМПАНІЄЮ КІБЕРВПЛИВУ DOPPELGANGER

21 березня Управління з контролю за іноземними активами Міністерства фінансів США (OFAC) оголосило про санкції проти двох громадян росії та відповідних компаній, якими вони володіють, за участь в операціях кібервпливу. Звинувачення висунули засновнику московської компанії Social Design Agency (SDA) Іллі Гамбашидзе і генеральному директору і нинішньому власнику російської компанії Group Structura LLC (Структура) Миколі Тупікіну, яких звинувачують у наданні послуг російському уряду у зв'язку з «іноземною кампанією шкідливого впливу». Кампанія з дезінформації відстежується ширшою кібербезпековою спільнотою під назвою Doppelganger, яка, як відомо, таргетує цільову аудиторію в Європі та США за допомогою неавтентичних сайтів новин і облікових записів у соціальних мережах.

РОСІЙСЬКІ ХАКЕРИ ВІРОГІДНО НАЦІЛИЛИСЯ НА УКРАЇНСЬКІ ТЕЛЕКОМУНІКАЦІЇ ЗА ДОПОМОГОЮ ОНОВЛЕНОГО ШКІДЛИВОГО ПЗ ACIDPOUR

Згідно з новими висновками SentinelOne, опублікованими 22 березня, зловмисне програмне забезпечення під назвою AcidPour, яке знищує дані, могло бути застосовано в атаках проти чотирьох операторів зв'язку в Україні. Компанія також підтвердила зв'язок між шкідливим програмним забезпеченням і AcidRain, прив'язавши його до кластерів загроз, пов'язаних з російською військовою розвідкою. AcidPour є варіантом AcidRain, вайпера, який використовувався, щоб зробити модеми Viasat KA-SAT працездатними на початку російсько-української війни на початку 2022 року та порушити військовий зв'язок України.

РОСІЙСЬКІ ХАКЕРИ ВИКОРИСТОВУЮТЬ ШКІДЛИВЕ ПЗ WINELOADER ДЛЯ НАПАДУ НА ПОЛІТИЧНІ ПАРТІЇ НІМЕЧЧИНИ – MANDIANT

Згідно з звітом компанії Mandiant, бекдор WINELOADER, який використовувався в останніх кібератаках на дипломатичні установи з використанням фішингових приманок щодо дегустації вина, вважається роботою хакерської групи, пов'язаної зі службою зовнішньої розвідки росії, яка відповідала за злом SolarWinds і Microsoft. У Mandiant заявили, що Midnight Blizzard (він же APT29, BlueBravo або Cosy Bear) приблизно 26 лютого 2024 року використала зловмисне програмне забезпечення для фішингової атаки на німецькі політичні партії, з використанням електронних листів з логотипом Християнсько-демократичного союзу (ХДС). Атака на політичну партію з боку кластера APT29 спостерігається вперше. Зазвичай він націлюється на дипломатичні місії. На думку компанії, така атака становить ширшу загрозу для політичних партій в ЄС.

США ЗАПРОВАДИЛИ САНКЦІЇ ПРОТИ ТРЬОХ КРИПТОВАЛЮТНИХ БІРЖ, ЩО ДОПОМАГАЛИ РФ УХИЛЯТИСЯ ВІД САНКЦІЙ

26 березня Управління з контролю за іноземними активами Міністерства фінансів США (OFAC) наклало санкції на три криптовалютні біржі за надання послуг, які використовуються для ухилення від економічних обмежень, накладених на росію після її вторгнення в Україну на початку 2022 року. Серед них такі біржі, як Bitpapa IC FZC LLC, Crypto Explorer DMCC (AWEX) і Общество с ограниченной ответственностью Центр Обработки Электронных Платежей (ТОЕР). Загалом санкції торкнулися тринадцяти організацій і двох фізичних осіб, які працюють у російському секторі фінансових послуг і технологій.

9. РІЗНЕ

КОМПАНІЯ INTELLEXA, ЩО ВИРОБЛЯЄ ШПИГУНСЬКЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ПОТРАПИЛА ПІД САНКЦІЇ США

6 березня Міністерство фінансів США наклало санкції на групу кіберспостереження та двох її ключових керівників, Тала Діліана та Сару Хамоу, за заохочення використання шпигунського програмного забезпечення по всьому світу. За словами Міністерства фінансів, шпигунське програмне забезпечення Intellexa, відоме як Predator, використовувалося для таємного стеження за офіційними особами США, журналістами та експертами з політики.
Це перший випадок, коли уряд США застосував санкції до конкретних людей, окрім компаній, пов'язаних зі зловживанням комерційним шпигунським програмним забезпеченням.
І це означає, що Білий дім та уряд США підсилює зусилля щодо приборкання індустрії шпигунського ПЗ.