НКЦК
НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

УКРАЇНСЬКА ФУНДАЦІЯ БЕЗПЕКОВИХ СТУДІЙ

CYBER DIGEST

Огляд подій в сфері кібербезпеки,
лютий 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

Важливою подією лютого 2024 року стала вдала операція британських правоохоронців проти потужної ransomware групи Lockbit. На угрупування, які використовують ransomware Lockbit, припадає значна частина ransomware атак по всьому світу і припинення їх діяльності дозволить зменшити негативну динаміку таких атак. Ці зусилля британських правоохоронців були доповнені діями української поліції, які заарештували двох учасників цього угрупування. Загалом слід відзначити, що це вже другий помітний успіх правоохоронних органів у боротьбі з великими ransomware групами. Нещодавно американські правоохоронці зупинили роботу угрупування Hive і зараз шукають його лідерів (Державний департамент США оголосив винагороду за інформацію про них).

Вразливості у продуктах Ivanti вже другий місяць створюють проблеми користувачам та кібербезпековим органам по всьому світу. Виходять все нові дані про вразливості у продуктах Ivanti, а ENISA та CERT-EU навіть випустили спільні рекомендації для європейських споживачів. Ця ситуація розвивається на фоні істотного зрушення в кібербезпековій політиці ЄС – там запрацювала перша європейська схема сертифікації для продуктів ІКТ відповідно до Загальних критеріїв. Схема містить в собі елементи різних національних схем сертифікації та має на меті зробити використання ІТ-продуктів європейськими споживачами більш безпечним. Наразі схема лише в процесі впровадження, але ЄС покладає значні надії на неї та подальший розвиток.

7-8 лютого у столиці України відбувся перший Київський міжнародний форум з кібербезпеки 2024: «Стійкість під час кібервійни», започаткований НКЦК при РНБО України разом з партнерами. Загалом у Форумі взяли участь понад тисяча учасників, серед яких топ посадовці України, США, ЄС та НАТО. Під час заходу відбулося 10 панельних дискусій і понад 40 експертних доповідей, які розкривали роль кібербезпеки у сучасних війнах, досвід України у кібервійні, тему кібервійни і міжнародного права, кібердипломатії, посилення стійкості національної системи кібербезпеки через освіту, захищеність месенджерів, роль розвідки кіберзагроз, кібербезпека регіонів та інші. Також в рамках KICRF відбулись змагання з кібербезпеки, у яких взяла участь 21 команда фахівців із державного і приватного секторів. Під час зустрічей на полях форуму, українські та американські посадовці визнали успішною співпрацю між США та Україною у сфері обміну досвідом питань з кібербезпеки та обговорили короткострокові та довгострокові потреби України у сфері кіберзахисту.

Загострюються відносини між США та КНР у сфері кіберсуперництва. Слухання перед Спеціальним комітетом Палати представників з питань Комуністичної партії Китаю висвітлили зростаюче занепокоєння безпекових органів США щодо китайської кіберактивності. В деяких з виступів (як то керівника ФБР чи Колишнього директора Агентства національної безпеки США Пола Накасоне) звучали жорсткі оцінки дій китайських хакерських груп (наприклад, групи Volt Typhoon), які істотно відходять від дій кібершпигунства на користь прямих атак на об'єкти критичної інфраструктури чи створюють там позиції на випадок масштабного конфлікту (застосовуючи метод атаки Living-Off-the-Land). Так, за даними ФБР, група Volt Typhoon впровадила зловмисне ПЗ на сотнях мережевих маршрутизаторах та інших підключених до Інтернету пристроях, створюючи загрозу для водопостачання, електроенергії та залізничних перевезень, що може завдати реальної шкоди. Ще одна загроза від китайських хакерів – можливий негативний вплив на американську військову базу в Гуамі. Американські безпекові структури занепокоєні тим, що китайські кібератаки можуть мати дуже значний вплив на її функціонування. Як проміжний наслідок, 7 лютого CISA, NSA і ФБР разом із ключовими американськими та міжнародними урядовими агентствами (Австралії, Канади та Нової Зеландії) опублікували спільну консультацію щодо кібербезпеки, стосовно діяльності Volt Typhoon. Іншим наслідком стане прийняття більш жорстких вимог до стану кібербезпеки для інфраструктури портів в США (які істотно залежать від китайського обладнання). Очікується, що Президент США прийме найближчим часом відповідний Указ.

Серед досягнень українських кіберфахівців у лютому – затримання двох міжнародних злочинців та призові місця на двох міжнародних змаганнях у сфері кібербезпеки. У результаті спільної операції Служби безпеки, правоохоронних органів США, Великої Британії, Євросоюзу та інших країн-партнерів викрито учасників потужного міжнародного угруповання вимагачів LockBit. Також ГУР розповіло про атаку на російську систему управління дронами, що призвело втрати росіянами доступу до серверів. СБУ також наголосила на важливості інформації, зібраної кібершляхом, для здійснення складних кінетичних операцій.

Занепокоєння урядових структур щодо наступальних дій в кіберпросторі торкнулись і комерційного сектору. В лютому Великобританія та Франція спільно провели першу установчу конференцію, присвячену боротьбі із загрозою комерційного кіберрозповсюдження – тобто безконтрольного поширення з протиправною метою створених комерційними компаніями інструментів, які можуть використовуватись в наступальних кібердіях. За результатами учасники підписали декларацію Процесу Pall Mall, яка фіксує плани учасників ініціативи вивчати альтернативні політики та інноваційні методи боротьби з цією загрозою. Наразі Ізраїль майже не бере участі у цих ініціативах, адже ізраїльські компанії мають значну частку на експортному ринку шпигунського ПЗ.

Загрози кібербезпеці ОТ не лише не зменшуються, але стають все більш системними. Виробники обладнання та ОТ-рішень все частіше знаходять нові вразливості у своїх продуктах – лише у лютому Siemens виявив 275 вразливостей у своїх виробах які активно використовуються у сфері автоматизації виробничих процесів. Звіт Dragos Inc підтверджує, що зловмисники все інтенсивніше входять в цю, відносно нову, сферу – у 2023 році додалось ще три кіберугрупування, які націлені саме на ОТ інфраструктуру (таким чином Dragos наразі відстежує 21 таке угрупування). Проблеми є не лише з виявленням вразливостей, але і зі спробами їх виправити. Дослідження показали, що організації з системами ОТ часто знають про недоліки, які використовуються в їхньому середовищі, але вони не можуть вирішити проблему. Адже гарантійний термін дії деяких застарілих систем закінчився, а особливості технічних процесів чи бізнес-інтереси можуть ставати на заваді оновленню цих активів до найновіших операційних систем.

Кількість кіберінцидентів, опрацьованих CERT-UA за минулий рік зросла на 15,9% у порівнянні з 2022 роком та склала 2543 кіберінциденти. Найпоширенішими типами інцидентів є розповсюдження шкідливого ПЗ, фішинг, шкідливе підключення, компрометація облікового запису та компрометація системи. Зловмисники традиційно проводять розвідувальні операції, вдаються до довготривалого шпигунства та знищення даних та інформаційних систем.

Триває глобальна кібервійна, значною частиною якої є російсько-українське протиборство. російські хакерські групи продовжують проводити кібершпигунські операції проти України (зокрема, одну з таких атак проти українських військових відстежує компанія Securonix Threat Research) або атакують урядові сайти (як, наприклад, сайт Міністерства освіти України). Українські кіберфахівці активно протидіють цим спробам, в тому числі продовжуючи досліджувати наслідки масштабної кібератаки 2023 року проти телекомоператора «Київстар». За даними СБУ російські хакери готували другу хвилю атак, яка мала нанести ще більше шкоди оператору.

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

ЗАПРАЦЮВАЛА ПЕРША ЄВРОПЕЙСЬКА СХЕМА СЕРТИФІКАЦІЇ – EU COMMON CRITERIA (EUCC)

1 лютого стало відомо, що Європейська комісія прийняла першу європейську схему сертифікації, яка забезпечує узгоджені правила та процедури сертифікації на рівні ЄС для продуктів ІКТ відповідно до Загальних критеріїв. Схема містить в собі елементи різних національних схем сертифікації, об'єднаних у рамках угоди про взаємне визнання SOG-IS. Перші сертифікати можуть бути видані через рік.

CISA ПРОВЕЛА ДРУГИЙ СИМПОЗІУМ ЩОДО КІБЕРСТІЙКОСТІ

1 лютого CISA організувала другий регіональний симпозіум програми Cyber Resilient 911 (CR911). Основні учасники – адміністратори системи 911, представники місцевих центрів та IT/кіберспільнот, а також державні координатори взаємодії (SWIC) з кожного штату та території. Тема заходу – огляд поточного ландшафту кіберзагроз і спільних ресурсів, щоб допомогти покращити стан кібербезпеки центрів екстреного зв'язку (ECC). Мета – зібрати поточні потреби, проблеми та прогалини в можливостях учасників щодо кібербезпеки, а також провести ТТХ, присвячені симуляції сценарію кібератаки.

ГЕНЕРАЛ ТІМОТІ ХО ВСТУПИВ НА ПОСАДУ ОЧІЛЬНИКА АНБ І КІБЕРКОМАНДУВАННЯ

У п'ятницю, 2 лютого 2024 року, генерал Тімоті Д. Хо прийняв командування Агентством національної безпеки (АНБ) і кіберкомандуванням США (USCYBERCOM). У травні 2023 року президент Джо Байден обрав Хо на керівну посаду, до сфери відповідальності якої входить кібервійна та оборона Америки, криптографія та радіоелектронна розвідка.

CISA ОГОЛОШУЄ ПРО ОНОВЛЕННЯ РОБОЧОЇ ГРУПИ З УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

6 лютого CISA оголосила про поновлення на наступні два роки мандату Цільової групи з управління ризиками ланцюга постачання (SCRM) інформаційно-комунікаційних технологій (ICT). Ця група, очолювана Національним центром управління ризиками (NRMC) CISA та Координаційними радами секторів інформаційних технологій і комунікацій, є прикладом партнерством між державним та приватним секторами. До січня 2026 року Цільова група буде працювати над питаннями поліпшення управління ризиками у ланцюгу постачання ІКТ.

В США ЗАПУЩЕНО ВЕБСТОРІНКУ РЕСУРСІВ #PROTECT2024 ДЛЯ ДЕРЖАВНИХ І МІСЦЕВИХ ВИБОРЧИХ ПОСАДОВИХ ОСІБ

7 лютого CISA запустило вебсторінку #Protect2024, яка стане центральною точкою для консолідації критично важливих ресурсів, навчальних курсів та пропозицій послуг з безпеки для підтримки понад 8000 виборних юрисдикцій у виборчому циклі 2024 року. Ці зусилля базуються на попередніх роках співпраці з представниками виборчих органів з метою зменшення кібернетичних, фізичних та операційних ризиків для виборчої інфраструктури.

CISA ВИЗНАЧИЛА ПРІОРИТЕТИ JCDC НА 2024 РІК

12 лютого CISA опублікувала пріоритети діяльності JCDC на 2024 рік. JCDC є групою галузевих і державних партнерів, які у 2024 році сконцентруються на шести пріоритетних напрямках:

- захист від зловмисних дій з боку суб'єктів APT,
- підготовку організацій до великих кіберінцидентів,
- підтримку безпеки виборів,
- зменшення впливу програм-вимагачів на критичну інфраструктуру,
- розвиток технологій Secure-by-design,
- забезпечення безпеки виробництва та зменшення ризику, пов'язаного зі штучним інтелектом для критичної інфраструктури.

МІНІСТЕРСТВО ОБОРОНИ США ОПРИЛЮДНИЛО ВІДЕО З ДЕТАЛЯМИ ПРО МАЙБУТНЮ CMMC 2.0 ДЛЯ ПОЛІПШЕННЯ ЯКОСТІ ГРОМАДСЬКОЇ ДИСКУСІЇ

15 лютого Міністерство оборони США оприлюднило відео для поліпшення якості громадського обговорення CMMC (Cybersecurity Maturity Model Certification), яке тривало до 26 лютого 2024 року. У відео роз'яснюються всім зацікавленим сторонам (передусім оборонним підрядникам) запропоновані нові правила для програми CMMC аби спростити процес надання відгуків.

ПРЕЗИДЕНТ США ГОТУЄТЬСЯ ПІДПИСАТИ УКАЗ ПРО ПОЛІПШЕННЯ ЗАХИСТУ ПОРТІВ США ВІД ПОТЕНЦІЙНИХ КІБЕРАТАК

20 лютого Енн Нойберг (Anne Neuberger), заступник радника з національної безпеки з питань кібербезпеки та проривних технологій повідомила, що Адміністрація Байдена-Харріс готується до підписання Указу Президента США (Executive Order), спрямованого на посилення кібербезпеки портів. Указ надасть DHS (більшою мірою CISA) додаткові повноваження щодо визначення вимог кібербезпеки портової інфраструктури. Ці зусилля є відповіддю як на загальну важливість портової інфраструктури для функціонування США, так і значної кількості портових кранів китайського виробництва, які використовуються в американських портах і від яких залежить їх функціонування.

MICROSOFT ЗРОБИТЬ РОЗШИРЕНІ МОЖЛИВОСТІ ВЕДЕННЯ ЖУРНАЛІВ БЕЗКОШТОВНИМ ДЛЯ ВСІХ ФЕДЕРАЛЬНИХ УСТАНОВ США

21 лютого у спільному прес-релізі CISA, OMB, ONCD і Microsoft повідомлено, що Microsoft надасть можливість всім федеральним агентствам користуватись веденням журналів безкоштовно в будь-якому з пакетів послуг. Ця ініціатива спрямована на покращення кібербезпеки, шляхом надання розширених журналів і подовжених періодів зберігання журналів без додаткових витрат для організацій. Також вона повністю узгоджується з вказівками CISA для впровадження Secure by Design у всіх державних установах.

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

ООН РОЗСЛІДУЄ 58 КІБЕРАТАК З БОКУ ПІВНІЧНОЇ КОРЕЇ НА ЗАГАЛЬНУ СУМУ $3 МЛРД

Спостерігачі ООН за санкціями розслідують десятки ймовірних кібератак з боку Північної Кореї, які дозволили цій країні здобути 3 мільярди доларів для розвитку програми ядерної зброї. Розслідування стосується кібератак за період з 2017 по 2023 роки. Повний звіт з цього питання має бути опубліковано на початку березня 2024 року.

ЄС І КАНАДА ПОСИЛЮЮТЬ СТРАТЕГІЧНЕ ЦИФРОВЕ ПАРТНЕРСТВО

1 лютого Комісар з питань внутрішнього ринку Тьєррі Бретон і міністр інновацій, науки та промисловості Канади Франсуа-Філіп Шампань зустрілись, щоб розпочати реалізацію Цифрового партнерства між ЄС і Канадою, започаткованого під час листопадового саміту в Канаді. Співпраця буде зосереджена на вирішенні проблем цифрової трансформації в дослідженнях, промисловості, суспільстві та економіці. Основні пріоритети: штучний інтелект, квантові дослідження, напівпровідники, політика щодо онлайн-платформ, кібербезпека.

31 ОСОБУ ЗААРЕШТОВАНО ПІД ЧАС ГЛОБАЛЬНОЇ ОПЕРАЦІЇ ПРОТИ КІБЕРЗЛОЧИННОСТІ

Я повідомило 2 лютого видання Security Week, операція під назвою Synergia, тривала з вересня по листопад 2023 року та призвела до виявлення понад 1300 підозрілих серверів управління та керування (C&C), 70% з яких було вимкнено. Операція під керівництвом Інтерполу стосувалася Азійсько-Тихоокеанського регіону, Європи, Близького Сходу та Африки (EMEA) та інших регіонів. Було залучено 60 правоохоронних органів з 50 країн-учасниць.

«Тримісячна операція «Синергія» була розпочата у відповідь на зростання, ескалацію та професіоналізацію транснаціональної кіберзлочинності та потребу в скоординованих діях проти нових кіберзагроз», – зазначає одна з учасниць операції компанія Group-IB.

СПІЛЬНА ЗАЯВА ENISA, CERT-EU, ЄВРОПОЛУ ПРО ВРАЗЛИВОСТІ В IVANTI CONNECT SECURE І IVANTI POLICY SECURE

6 лютого була опублікована Спільна заява про вразливості Ivanti Connect Secure і Ivanti Policy Secure. Європейська Комісія, ENISA, CERT-EU, Європол та мережа CSIRTs ЄС уважно слідкують за використанням вразливостей у продуктах Ivanti Connect Secure та Ivanti Policy Secure Gateway. Після початкового виявлення двох вразливостей на початку січня 2024, наприкінці січня було виявлено ще дві, що впливають на всі підтримувані версії продуктів Ivanti. Нові виявлені вразливості дозволяють зловмисникам виконувати команди в системі.

США РАЗОМ З МІЖНАРОДНИМИ ПАРТНЕРАМИ ОПРИЛЮДНИЛИ КОНСУЛЬТАЦІЇ З КІБЕРБЕЗПЕКИ ЩОДО СПОНСОРОВАНОЇ КНР ХАКЕРСЬКОЇ ГРУПИ VOLT TYPHOON

7 лютого CISA, NSA і ФБР разом із ключовими американськими та міжнародними урядовими агентствами (Австралії, Канади та Нової Зеландії) опублікували спільну консультацію щодо кібербезпеки, стосовно діяльності китайського кібератора, відомого як Volt Typhoon. Діяльність Volt Typhoon спрямована на компрометацію критичної інфраструктури США. Директор CISA Джен Істерлі заявила, що вже ліквідовано декілька втручань Volt Typhoon в діяльність критичної інфраструктури в різних секторах, але це, ймовірно, лише вершина айсберга. Крім цього, була оприлюднена інструкція, яка допомагає виявляти TTP, які використовуються такими акторами, як Volt Typhoon. Останні роки свідчать про зсув в діяльності КНР щодо кіберзагроз, з фокусом на руйнівні кібератаки на критичну інфраструктуру США. Кібератори КНР застосовують методи Living-Off-the-Land, що допомагають їм уникають виявлення мережевим захистом та обмежують реєстрацію активностей.

ПРАВООХОРОННІ ОРГАНИ ПРИПИНИЛИ ДІЯЛЬНІСТЬ WARZONE RAT, ДВОХ ОСІБ ЗААРЕШТОВАНО

12 лютого Міністерство юстиції США оголосило, що в результаті міжнародної правоохоронної операції було ліквідовано кіберзлочину компанію Warzone RAT. Warzone – це троян віддаленого доступу, який дозволяє користувачам непомітно підключатися до заражених пристроїв і виконувати різноманітні дії, наприклад, переглядати файли, записувати натискання клавіш, робити знімки екрана, викрадати облікові дані та шпигувати через камеру комп'ютера. Зловмисне програмне забезпечення також відоме як Ave Maria RAT, і воно було помічено в численних атаках, у тому числі вірогідно пов'язаних із державними суб'єктами загрози.

ВЕЛИКОБРИТАНІЯ ТА ФРАНЦІЯ ПРОВЕЛИ ПЕРШУ СПІЛЬНУ КОНФЕРЕНЦІЮ ЩОДО КОМЕРЦІЙНОГО КІБЕРРОЗПОВСЮДЖЕННЯ В МЕЖАХ ІНІЦІАТИВИ PALL MALL

15 лютого Великобританія та Франція спільно організували установчу конференцію, присвячену боротьбі з загрозою комерційного кіберрозповсюдження – поширення з протиправною метою законно створених комерційних інструментів, які можуть використовуватись в наступальних діях. Захід зібрав різноманітні зацікавлені сторони, включаючи уряди, технологічні компанії, групи громадянського суспільства, академічні установи, експертів з кібербезпеки, інвесторів, дослідників та приватні підприємства. Результатом заходу стало підписання декларації Процесу Pall Mall – ініціативи, спрямованої на вивчення альтернатив політики та впровадження інноваційних методів боротьби з цією загрозою.

Ізраїль не брав участі у заході . Відсутність ізраїльських офіційних осіб на кіберконференції в Lancaster House примітна через значну частку Ізраїлю на експортному ринку шпигунського ПЗ.

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

У ЕЛЕКТРОМОБІЛЯХ ВИЯВЛЕНІ ЧИСЛЕННІ ВРАЗЛИВОСТІ НУЛЬОВОГО ДНЯ

1 лютого Cisco Talos Intelligence Group поширила матеріал присвячений кібервразливостям електромобілів, що створює для водіїв нові потенційні ризики та наслідки для їх безпеки. У матеріалі згадуються результати практичного заходу Pwn2Own, під час якої дослідники виявили численні вразливості нульового дня в електромобілях і пов'язаних із ними продуктах, що викликає занепокоєння щодо безпеки підключених транспортних засобів.

ФЕДЕРАЛЬНА СЛУЖБА США ПРИПИНИЛА РОБОТУ БОТНЕТУ KV-BOTNET, ПОВ'ЯЗАНОГО З КИТАЄМ

Уряд США 1 лютого заявив, що нейтралізував ботнет, що складається з сотень американських маршрутизаторів для малих офісів і домашніх офісів (SOHO), захоплених пов'язаною з Китаєм спонсорованою державою загрозливою організацією Volt Typhoon.

Про існування ботнету, який отримав назву KV-ботнет, стало вперше відомо завдяки команді Black Lotus Labs із Lumen Technologies в середині грудня 2023 року. «Переважно ботнет KV складався з маршрутизаторів Cisco та NetGear, які були вразливі, оскільки вони досягли статусу «закінчилося життя»; тобто вони більше не підтримувалися через патчі безпеки їх виробника або інші оновлення програмного забезпечення». Про це йдеться в заяві для преси Міністерства юстиції (DoJ).

КІБЕРЗЛОВМИСНИКИ АТАКУВАЛИ ДИТЯЧУ ЛІКАРНЮ В ЧИКАГО

5 лютого дитяча лікарня Лур'є у Чикаго (обслуговує близько 200 тисяч дітей на рік) повідомила, що відключила свої мережеві системи, оскільки продовжує реагувати на «питання кібербезпеки», залучивши до цього зовнішніх експертів та правоохоронні органи. Масштаби атаки такі, що лікарні довелось повернутись до виключно паперового документообігу – жодні електронні сервіси не працювали, а лікарня функціонувала здебільшого в режимі надзвичайної допомоги. Жодне угрупування не взяло на себе відповідальність за цю кібератаку.

ІРАН ПОСИЛЮЄ КІБЕРОПЕРАЦІЇ ПРОТИ ІЗРАЇЛЮ

6 лютого Microsoft поширило результати свого дослідження щодо іранської кіберактивності. У ньому обговорюється ескалація кібероперацій Ірану проти Ізраїлю після початку бойових дій з ХАМАС у жовтні 2023 року. У матеріалі детально описується еволюція кібертактики Ірану, від початкових (поспішно організованих атак) до більш складних і скоординованих зусиль, підкреслюючи значне зростання кібердіяльності та її поширення на глобальні операції.

НОВИЙ БЕКДОР ZARDOOR ВИКОРИСТОВУВАВСЯ В ДОВГОСТРОКОВІЙ ОПЕРАЦІЇ КІБЕРШПИГУНСТВА ПРОТИ ІСЛАМСЬКОЇ ОРГАНІЗАЦІЇ

8 лютого кіберексперти Cisco Talos поширили інформацію про складну шпигунську кампанію, яка використовує раніше невідоме шкідливе програмне забезпечення Zardoor для проникнення в неназвану ісламську некомерційну організацію. Cisco Talos вважає, що за операцією стоїть висококваліфіковане угрупування. Ця кампанія активна щонайменше з березня 2021 року і демонструє здатність актора уникати виявлення та підтримувати довгостроковий доступ до мережі цілі.

RANSOMWARE AKIRA ТА LOCKBIT АКТИВНО ШУКАЮТЬ ВРАЗЛИВІ ПРИСТРОЇ CISCO ASA

8 лютого HelpNetSecurity з посиланням на дослідника Кевіна Бомонта повідомила, що групи програм-вимагачів Akira та Lockbit намагаються зламати пристрої Cisco ASA SSL VPN, використовуючи кілька старих вразливостей.
Видання пише, що організації, які використовують пристрої Cisco ASA, вразливі до постійних загроз від зловмисників, які використовують відомі вразливості, включно з тими, які були виправлені у 2020 і 2023 роках.

Попри доступні патчі, багато пристроїв залишаються без змін, в результаті чого вони є відкритими для різних методів атак. Зловмисники активно використовують експлойти для підтвердження концепції або розробляють власні, при цьому останні звіти вказують на підвищену активність сканування, націлену на пристрої Cisco AnyConnect VPN переважно зі зловмисних IP-адрес. Групи програм-вимагачів активно використовують ці вразливості, про що свідчить використання CVE-2020-3580 у 2021 році. Нещодавнє оновлення від Cisco щодо CVE-2020-3259 підкреслює важливість швидкого встановлення виправлень для зменшення ризику атак програм-вимагачів.

ДЕРЖДЕПАРТАМЕНТ США ПРОПОНУЄ 10 МЛН ДОЛАРІВ ЗА ІНФОРМАЦІЮ ПРО ЛІДЕРІВ RANSOMWARE HIVE

9 лютого Держдепартамент США запропонував винагороду в розмірі до 10 мільйонів доларів США за інформацію, яка допоможе ідентифікувати або дізнатись місцезнаходження ключових лідерів організованої злочинної групи Hive. Наприкінці 2023 року ФБР змогло припинити діяльність цієї групи, однак лідери угруповання все ще не заарештовані.

ОПРИЛЮДНЕНО НОВИЙ ОПИС ВРАЗЛИВОСТЕЙ В ПРОДУКТАХ IVANTI

9 лютого Ivanti опублікувало оновлену консультацію, де докладно описано низку вразливостей, які впливають на шлюзи Connect Secure і Policy Secure. Деякі з цих вразливостей зараз активно використовуються зловмисниками. Організаціям рекомендується вжити негайних заходів для пом'якшення вразливості шлюзів Ivanti Connect Secure (ICS) і Ivanti Policy Secure (IPS) (CVE-2023-46805, CVE-2024-21887, CVE-2024-21888 і CVE-2024-21893, CVE-2024-22024).

ЧОТИРИ МЕТОДИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ, ЯКІ ХАКЕРИ ВИКОРИСТОВУЮТЬ ДЛЯ ОБХОДУ MFA

Як 12 лютого пише видання The Hacker News, багатофакторна автентифікація (MFA) має вирішальне значення для підвищення безпеки доступу, але вона не на 100% надійна. Попри переваги, хакери можуть обійти MFA за допомогою тактики соціальної інженерії, як-от атаки «противник посередині», миттєвого бомбардування MFA, маніпуляції зі службою обслуговування та заміни SIM-карти. Ці методи користуються слабкими місцями в процесах автентифікації, підкреслюючи важливість надійних паролів і багатошарових стратегій захисту. Попри те, що MFA додає ще один рівень безпеки, організації все одно повинні надавати пріоритет безпеці паролів, щоб зменшити ризик компрометації.

ТРИВАЮЧА КОМПАНІЯ КОМПРОМЕТАЦІЇ AZURE НАЦІЛЕНА НА ВИЩЕ КЕРІВНИЦТВО КОМПАНІЙ ТА ЗАСТОСУНКИ MICROSOFT 365

12 лютого видання Dark Reading повідомило про триваючу кампанію, націлену на корпоративні хмари Microsoft Azure, яка вже скомпрометувала десятки середовищ і сотні людей. Діяльність передбачає викрадання даних, фінансове шахрайство та видавання себе за іншу особу в різних організаціях. Постраждалі організації знаходяться в різних географічних регіонах і галузях. Проте фішинг спрямований на дуже стратегічних осіб у кожній організації.

ВІДОМЕ ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ BUMBLEBEE ПОВЕРТАЄТЬСЯ З НОВИМИ МЕТОДАМИ АТАКИ

Видання Infosecurity повідомило 13 лютого, що зловмисне ПЗ Bumblebee повернулося в лютому 2024 року після чотирьох місяців відсутності, використовуючи суттєво інший ланцюг атак порівняно з попередніми проникненнями. Це ПЗ часто використовувалося кількома загрозливими суб'єктами з березня 2022 року по жовтень 2023 року. За цей період було ідентифіковано 230 кампаній. Bumblebee служить початковим посередником доступу, завантажуючи та виконуючи додаткові корисні навантаження, такі як Cobalt Strike і Meterpreter.

Нова кампанія використовує методи соціальної інженерії, надсилаючи електронні листи з URL-адресами OneDrive, що містять документи Word із макросами. Ці макроси створюють сценарій для виконання наступного етапу атаки, завантаження та запуску DLL Bumblebee. Ця кампанія виділяється використанням документів із підтримкою макросів VBA, що відрізняє її від попередніх підходів. Хоча кампанію не було приписано конкретному загрозливому суб'єкту, деякі методи збігаються з діяльністю групи TA579. Відродження загроз, таких як TA577, що розповсюджує зловмисне програмне забезпечення Qbot, вказує на високі операційні темпи, які, як очікується, продовжаться влітку 2024 року.

МІНОБОРОНИ США ПОВІДОМИЛО ПОНАД 20 ТИСЯЧ ОСІБ ПРО РОЗКРИТТЯ ЇХНІХ ПЕРСОНАЛЬНИХ ДАНИХ ПІСЛЯ ВИТОКУ ЕЛЕКТРОННОЇ ПОШТИ З ХМАРИ

Міністерство оборони США (DOD) поінформувало приблизно 20 600 осіб про те, що їхню особисту інформацію було розкрито під час витоку даних електронної пошти, який стався між 3 та 20 лютого 2023 року. Порушення конфіденційності було пов'язане з випадковим виявленням сенситивних листів у незахищеній хмарній пошті уряду США, розміщеній на хмарній платформі Microsoft. Сервер був доступний без пароля через неправильну конфігурацію. Після цього Міноборони вилучило сервер із загального доступу та працює з постачальником послуг над покращенням заходів кібербезпеки. Серед доступних документів була внутрішня військова електронна пошта, в тому числі пов'язана з командуванням спеціальних операцій США, а також конфіденційна інформація про персонал і анкети допуску. Викриття даних виявив дослідник безпеки Анураг Сен, який повідомив про це TechCrunch, що призвело до захисту сервера.

MICROSOFT І OPENAI ПОВІДОМЛЯЮТЬ, ЩО ХАКЕРИ ВИКОРИСТОВУЮТЬ CHATGPT ДЛЯ ВДОСКОНАЛЕННЯ КІБЕРАТАК

14 лютого Microsoft і OpenAI повідомили, що знайшли докази того, що кіберзлочинці, включаючи групи, підтримувані росією, Північною Кореєю, Іраном і Китаєм, використовують великі мовні моделі (LLM), такі як ChatGPT, для посилення своїх кібератак. Ці групи використовують LLM у різних цілях, таких як дослідження цілей, вдосконалення сценаріїв і вдосконалення методів соціальної інженерії. Попри те, що поки що не виявлено значних атак з використанням LLM, Microsoft і OpenAI вживають профілактичних заходів, закриваючи пов'язані облікові записи та активи цих хакерських груп. Корпорація Microsoft попереджає про майбутні ризики, такі як підробка голосу за допомогою штучного інтелекту, і розробляє рішення, такі як Security Copilot, щоб посилити захист кібербезпеки.

TURLA APT ШПИГУЄ ЗА ПОЛЬСЬКИМИ НЕУРЯДОВИМИ ОРГАНІЗАЦІЯМИ

15 лютого кіберексперти з Cisco Talos опублікували статтю про використання Turla APT нового бекдору TinyTurla-NG для нападу на польські неурядові організації. Цей інструмент наступного покоління відповідає стилю кодування та функціональності свого попередника, TinyTurla, але запроваджує нові можливості та знаменує розширення арсеналу зловмисного програмного забезпечення Turla, вказуючи на ширшу стратегію підтримки геополітичних цілей росії.

МІНІСТЕРСТВО ЮСТИЦІЇ США ПОРУШИЛО РОБОТУ РОСІЙСЬКОГО БОТНЕТУ, ОПЕРАТОРОМ ЯКОЇ ВИСТУПАЛА В/Ч 26165 (ГРУ РФ)

16 лютого Міністерство юстиції США повідомило про проведення санкціонованої судом операції, яка дозволила порушити роботу ботнету, оператором якої виступало російське гру (використовуючи програму Moobot). Ботнет використовував загальновідомі паролі адміністратора за замовчуванням для отримання контролю над сотнями маршрутизаторів Ubiquiti Edge OS. Військова частина 26165 гру (оператор ботнету), також відома як APT 28, Sofacy Group, Forest Blizzard, Pawn Storm, Fancy Bear і Sednit, створила та використовувала ботнет для проведення кампаній фішингу та збору облікових даних проти об'єктів, які цікавили російський уряд – урядові структури США та інших країн, а також військові організації, служби безпеки та приватні організації. Наразі 31 в портовій інфраструктурі працює 31 мільйон американців, а самі порти приносять бюджету 5.4 трильйони доларів.

НАЦІОНАЛЬНЕ АГЕНТСТВО З БОРОТЬБИ ЗІ ЗЛОЧИННІСТЮ (NCA) ВЕЛИКОБРИТАНІЇ ОГОЛОСИЛО ПРО ВЗЯТТЯ ПІД КОНТРОЛЬ ІНФРАСТРУКТУРИ RANSOMWARE LOCKBIT

20 лютого NCSC поширив заяву Національне агентство з боротьби зі злочинністю (NCA) щодо взяття під контроль технічної інфраструктури, яка лежить в основі роботи LockBit, включаючи її основну платформу, а також майданчик на якому раніше розміщувалися дані, вкрадені у жертв. LockBit одне з найбільших ransomware угрупувань у світі та порушення його роботи може мати довгострокові позитивні наслідки.

ПІВНІЧНОКОРЕЙСЬКІ ХАКЕРИ НАЦІЛЕНІ НА ОБОРОННІ КОМПАНІЇ ПО ВСЬОМУ СВІТУ

У спільному звіті, опублікованому Федеральним відомством із захисту конституції Німеччини (BfV) і Національною розвідувальною службою Південної Кореї (NIS), йдеться про те, що спонсорованим державою Північної Кореї суб'єктам загрози приписують кампанії кібершпигунства, націлені на оборонний сектор у всьому світі. Сумнозвісну групу Lazarus Group звинувачують в одному з двох хакерських інцидентів, в яких було використано соціальну інженерію для проникнення в оборонний сектор у рамках тривалої операції під назвою «Робота мрії». Кампанія триває з серпня 2020 року.

ЗЛОВМИСНИКИ ЗЛОВЖИВАЮТЬ GOOGLE CLOUD RUN У КАМПАНІЯХ ОРІЄНТОВАНИХ НА ЛАТИНСЬКУ АМЕРИКУ

20 лютого фахівці Cisco Talos поширили результати свого нового дослідження з докладним описом того, як зловмисники використовують Google Cloud Run для розповсюдження банківських троянів, таких як Astaroth, Mekotio та Ousaban, у Латинській Америці та Європі. Починаючи з вересня 2023 року, відбулось помітне збільшення кількості шкідливих операцій, які використовують цей метод. У звіті підкреслюється співпраця або зв'язок між зловмисниками, які поширюють ці варіанти зловмисного програмного забезпечення, та розвитком загроз у кіберпросторі.

КИТАЙСЬКІ ХАКЕРИ СКОРИСТАЛИСЯ ВРАЗЛИВІСТЮ FORTIGATE, ЩОБ ЗЛАМАТИ ГОЛЛАНДСЬКУ ВІЙСЬКОВУ МЕРЕЖУ

У 2023 році китайські державні хакери зламали комп'ютерну мережу, яку використовують збройні сили Нідерландів, націлившись на пристрої Fortinet FortiGate.

«Ця [комп'ютерна мережа] використовувалася для несекретних досліджень і розробок (НДДКР)», – йдеться в заяві Служби військової розвідки та безпеки Нідерландів (MIVD). «Оскільки ця система була автономною, вона не призвела до будь-яких пошкоджень оборонної мережі». У мережі було менш як 50 користувачів.

КАНАДСЬКА ПОЛІЦІЯ ПОВІДОМИЛА ПРО КІБЕРАТАКУ НА СВОЇ ІНФОРМАЦІЙНІ МЕРЕЖІ

24 лютого Федеральна поліція Канади повідомила, що її системи зазнали серйозної кібератаки, водночас атака не вплинула на роботу організації та не загрожувала безпеці канадців. Канадська поліція повідомила, що розпочала розслідування атаки та намагається визначити масштаби порушення, додавши, що наразі не має жодних відомостей про вплив на розвідувальні служби.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

У ДОВГОСТРОКОВІЙ ПЕРСПЕКТИВІ ЯК ЗЛОВМИСНИКИ, ТАК І ФАХІВЦІ З БЕЗПЕКИ, БУДУТЬ МАТИ СВОГО COPILOT НА БАЗІ ШІ – PALO ALTO NETWORKS

1 лютого один з ключових фахівців Palo Alto Networks Кайл Вілхойт оприлюднив власні прогнози щодо ролі ШІ у сфері кібербезпеки на коротку, середню та довгострокову перспективу. В частині коротких і середньострокових загроз основною сферою застосування стане виробництво діпфейків та дезінформації. Водночас у довгостроковій перспективі він очікує появи інтелектуальних помічників (Copilot) на базі ШІ, які будуть допомагати у виконанні рутинних дій як зловмисникам, так і захисникам інформаційних систем.

США ГОТОВІ РІШУЧЕ ВІДПОВІСТИ НА КІБЕРЗАГРОЗУ З БОКУ КИТАЮ

1 лютого генерал армії Пол М. Накасоне, виступаючи перед Спеціальним комітетом Палати представників з питань Комуністичної партії Китаю, повідомив, що кіберактори в Китаї використовують зловмисне програмне забезпечення для атак на критичну інфраструктуру США, включаючи системи з водопостачання, електроенергією та паливом. Його слова свідчать про те, що ці дії спрямовані на створення прихованих позицій, які КНР може використати у разі кризи чи конфлікту. Накасоне також підкреслив, що США мають власний кіберпотенціал, який діє як стримуючий фактор для китайської кіберагресії. На його думку, Китай є «майже рівним супротивником» США в кіберпросторі, однак США зберігають і збережуть у майбутньому свою перевагу в кіберпросторі.

ЗЛОЧИНЦІ ОРГАНІЗУВАЛИ ВІДЕОКОНФЕРЕНЦІЮ З ДІПФЕЙКАМИ УЧАСНИКІВ АБИ ЗМУСИТИ СПІВРОБІТНИКА НАДІСЛАВ 25 МІЛЬЙОНІВ ДОЛАРІВ ШАХРАЯМ

5 лютого South China Morning Post розповіла, що офіс транснаціональної компанії в Гонконгу зазнав значних фінансових збитків на суму 200 мільйонів гонконзьких доларів (25,6 мільйона доларів США) через складну аферу із застосуванням технології deep-fake. У шахрайстві була відтворена цифрова версія головного фінансового директора компанії разом з іншими співробітниками, які з'явилися під час відеоконференції, даючи вказівки працівнику переказати кошти. Цей інцидент є першим у своєму роді в Гонконзі, який пов'язаний із великою сумою та використанням технології deepfake для імітації відеоконференції з кількома особами, де всі учасники (крім жертви) були сфабрикованими зображеннями реальних людей.

РОСІЯ І КИТАЙ ЗВІРЯЮТЬ ДІЇ ЩОДО «ВІЙСЬКОВОГО ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ»

Китай та росія домовилися консультуватися та координувати застосування ШІ у військових цілях. Під час переговорів у Пекіні 1 лютого чиновники обох країн обмінялися оцінками щодо військового використання ШІ. Вони обговорили доктринальні настанови та ініціативи, не називаючи залучених чиновників. Вони також погодилися посилити координацію в групі державних експертів (GGE) щодо смертельних систем автономної зброї (LAWS), яка є частиною підтримуваного ООН форуму. На зустрічі було підкреслено, що російські та китайські підходи до цього питання не суперечать одне одному та необхідність подальшої співпраці, як у двосторонньому форматі, так і на багатосторонніх платформах, таких як GGE та LAWS. Ця зустріч підкреслює більш широку стратегічну координацію між Пекіном та москвою в різних традиційних та нових областях.

НОВІ ТЕХНОЛОГІЇ ПОСИЛЮЮТЬ КІБЕРЗАГРОЗИ З БОКУ ПІВНІЧНОЇ КОРЕЇ

13 лютого на сайті Binding Hook опубліковано статтю присвячену зростаючим кіберзагрозам, які представляє Північна Корея. Підкреслюється роль нових технологій, таких як штучний інтелект, у покращенні кібероперацій цієї країни. Також стаття описує історію кібератак з боку Північної Кореї та міжнародної реакції, спрямованої на пом'якшення цих загроз.

ЗЛОЧИННІ ГРУПИ ПІВДЕННО-СХІДНОЇ АЗІЇ ЗМУШУЮТЬ ЛЮДЕЙ СТАВАТИ КІБЕРЗЛОЧИНЦЯМИ

21 лютого Інститут кібермиру опублікував статтю про експлуатацію людей у Південно-Східній Азії, які були силою змушені до кіберзлочинності. Висвітлюючи становище молодих людей, ошуканих шахрайськими пропозиціями про роботу, стаття висвітлює діяльність розгалуженої мережі примусових шахрайських онлайн-операцій, наголошуючи на необхідності міжнародної співпраці та надійних правоохоронних органів для боротьби з цією кризою.

DHS ЗАПУСКАЄ ПЕРШУ У СВОЄМУ РОДІ ІНІЦІАТИВУ НАЙМУ 50 ЕКСПЕРТІВ ЗІ ШТУЧНОГО ІНТЕЛЕКТУ У 2024 РОЦІ

Повідомляється, що новий «Корпус штучного інтелекту» DHS допоможе відповідальніше використовувати технології ШІ в стратегічних сферах внутрішньої безпеки, включаючи зусилля з протидії фентанілу, боротьби з сексуальною експлуатацією та насильством над дітьми, надання імміграційних послуг, зміцнення критичної інфраструктури та підвищення кібербезпеки.
Корпус штучного інтелекту підсилить працівників DHS експертами з технологій, моделей і додатків штучного інтелекту та машинного навчання (ML), які підтримуватимуть політичні ініціативи для забезпечення безпечного та надійного використання штучного інтелекту, одночасно захищаючи конфіденційність, громадянські права та громадянські свободи.

5. КРИТИЧНА ІНФРАСТРУКТУРА

США ВВЕЛИ САНКЦІЇ ПРОТИ ШЕСТИ ІРАНСЬКИХ ЧИНОВНИКІВ ЗА КІБЕРАТАКИ НА КРИТИЧНУ ІНФРАСТРУКТУРУ

3 лютого Управління з контролю за іноземними активами Міністерства фінансів США (OFAC) оголосило про санкції проти шести посадовців, пов'язаних з іранською розвідкою, за напади на об'єкти критичної інфраструктури в США та інших країнах.

Міністерство фінансів заявило, що вважає цих осіб відповідальними за проведення «кібероперацій, під час яких вони зламали та розмістили зображення на екранах програмованих логічних контролерів виробництва ізраїльської компанії Unitronics».

СТАЛО ВІДОМО ПРО ВИПРАВЛЕНУ AIRBUS ВРАЗЛИВІСТЬ У ПЗ, ЯКЕ ВИКОРИСТОВУЄТЬСЯ ДЛЯ БЕЗПЕЧНОГО ЗЛЬОТУ ТА ПОСАДКИ ЛІТАКІВ

3 лютого дослідники з Pen Test Partners у своєму блозі описали знайдену ними вразливість (вже виправлену) у програмі Flysmart+ Manager, який використовується пілотами Airbus для синхронізації даних та отримання інформації для безпечного зльоту та посадки. Дослідники описали досить складну і малоймовірну (але реальну) атаку на це ПЗ, завдяки якому потенційні зловмисники могли вплинути на зліт та посадку літака. Компанії знадобилось 19 місяців аби виправити цю вразливість.

ВИЯВЛЕНО ДВІ СЕРЙОЗНІ ВРАЗЛИВОСТІ В MITSUBISHI ELECTRIC FACTORY AUTOMATION

5 лютого Mitsubishi Electric повідомило, що у низці його продуктів (EZSocket, FR Configurator2, GT Designer3, GX і MT Works, MELSOFT Navigator і MX), які використовуються для автоматизації виробництва, виявлено дві серйозні вразливості. Експлуатуючи їх, зловмисник може мати можливість незаконно під'єднатись до продуктів, а також розкривати, змінювати, знищувати чи видаляти інформацію в продуктах. Наразі компанія ще не випустила патчів для виправлення ситуації. Хоча атаки можна здійснити через мережу Інтернет, але наразі не відомо чи є такі системи підключеними до мереж загального користування (продукти використовують пропрієтарний мережевий протокол). Фахівці вказують, що якщо ж зловмисникам вдасться реалізувати загрозу, то вони зможуть отримати доступ до інженерної робочої станції. А отже зможуть спілкуватися з ПЛК і перепрограмувати його, а також інсталювати нові утиліти на інженерній робочій станції.

CISA ТА EPA СПІВПРАЦЮЮТЬ У СФЕРІ КІБЕРРЕСУРСІВ У СЕКТОРІ ВОДОПОСТАЧАННЯ ТА ВОДОВІДВЕДЕННЯ

7 лютого 2024 року CISA та Агентство захисту навколишнього середовища (EPA) провели спільний захід у LinkedIn на тему «Підвищення кібербезпеки водного сектора», де презентували ресурси, спеціально розроблені для цієї галузі, зокрема Інструментарій кібербезпеки сектору водопостачання та водовідведення, представлений спільно CISA та EPA у січні 2024 року. Цей набір є важливим кроком у зміцненні стійкості водного сектору проти кіберзагроз, забезпечуючи практичні рішення для управління ризиками. Інструментарій включає Посібник з реагування на інциденти кібербезпеки, послуги оцінки кібербезпеки та інші ресурси, які сприяють підготовці до кіберінцидентів. CISA та EPA планують періодично оновлювати набір інструментів, щоб відповідати змінюваним потребам сектора.

КІБЕРБЕЗПЕКА ОТ ІНФРАСТРУКТУРИ ЗНАХОДИТЬСЯ В ЗОНІ РИЗИКУ ЧЕРЕЗ ПРОБЛЕМИ З ОНОВЛЕННЯМ ЇЇ ПРОШИВОК – ДАНІ ЗВІТУ TXONE NETWORKS

5 лютого тайванська компанія TXOne Networks, яка опікується питаннями кібербезпеки ОТ, оприлюднила свій звіт про ситуацію з безпекою ОТ по всьому світу. Один з висновків – організації з системами ОТ часто знають про недоліки, які використовуються в їхньому середовищі, але вони не можуть вирішити проблему оскільки гарантійний термін дії деяких застарілих систем закінчився. При цьому особливості технічних процесів чи бізнес-інтереси можуть завадити оновленню цих активів до найновіших операційних систем. Інший висновок – як одного з основних джерел інцидентів безпеки ОТ, респонденти найчастіше називали обслуговування ОТ (52%). В момент проведення такого оновлення можуть виникати загрози потрапляння в актив шкідливого коду.

НІМЕЦЬКИЙ ВИРОБНИК АКУМУЛЯТОРІВ VARTA ЧЕРЕЗ КІБЕРАТАКУ ЗМУШЕНИЙ БУВ ЗУПИНИТИ П'ЯТЬ ЗАВОДІВ

13 лютого німецький виробник акумуляторів Varta повідомив, що через кібератаку був змушений зупинити п'ять заводів. Їх робота була припинена до проведення повноцінної оцінки впливу кібератаки на IT системи.

SIEMENS ТА SCHNEIDER ELECTRIC ОПРИЛЮДНИЛИ РЕКОМЕНДАЦІЇ ПРО 275 ВРАЗЛИВОСТЕЙ В ПРОДУКТАХ SCALANCE, SINEC ТА ІНШИХ

13 лютого компанія Siemens та Schneider Electric оприлюднили свої рекомендації щодо зниження ризиків у низці продуктів. Майже половина вразливостей стосується комутаторів Scalance XCM-/XRM-300 (рівень серйозності «критичний» або «високий»), ще 60 в рішенні для управління промисловою мережею Sinec. Частина рекомендацій стосується вразливостей в продуктах Scalance W1750D (марка Aruba), Sidis Prime, Location Intelligence та Scalance SC-600. У продуктах Simatic CP 343-1, Parasolid, Polarion ALM, Simatic RTLS, Simcenter Femap, Unicam FX і Tecnomatix Plant Simulation. Вразливості Schneider Electric стосуються продуктів EcoStruxure Control Expert, EcoStruxure Process Expert і Modicon M340, M580 і M580.

У 2023 РОЦІ ЩОНАЙМЕНШЕ 21 ХАКЕРСЬКА ГРУПА БУЛА НАЦІЛЕНА НА ОТ ІНФРАСТРУКТУРУ – ЗВІТ DRAGOS INC

20 лютого відома компанія Dragos Inc, що займається безпековими рішеннями для промислової інфраструктури, оприлюднила свій звіт про тенденції 2023 року. За їх даними у 2023 році загальна кількість злочинних угрупувань, які сконцентровані на атаці ОТ систем, досягла 21. За минулий рік до них додались три нові групи – VOLTZITE (китайський актор націлений на сферу електроенергетики), GANANITE (сконцентрований на країнах СНД та Центральній Азії) і LAURIONITE (фокус на авіаційну, автомобільну та виробничу галузі). Групи використовують різні методи та інструменти, серед яких: загальнодоступні докази концепції (proof of concept, POC), націленість на ресурси Oracle E-Business Suite iSupplier, методи Living-Off-the-Land.

КІБЕРАТАКА НА CHANGE HEALTHCARE ПОРУШИЛА ФУНКЦІОНУВАННЯ АПТЕК ПО ВСІЙ АМЕРИЦІ

22 лютого стало відомо, що IT-провайдер Change Healthcare зазнав масштабної кібератаки, яка змусила його відключити частину своїх систем. Change Healthcare відповідає за інформування аптек в США щодо замовлень за рецептами (перевірка права пацієнтів на лікування та обробки замовлень на ліки з огляду на їхню страхову ситуацію) та про деякі інші послуги. Аптеки по всій країні (які користуються послугами цього провайдера) змушені були або відмовляти пацієнтам у видачі ліків, або продавати їм за повну вартість і лише за готівку. UnitedHealth (якій належить Change Healthcare) повідомила, що за даними експертів, які працюють над усуненням проблеми, організація зазнала атаки від спонсорованої державою кібергрупи.

6. АНАЛІТИЧНІ ОЦІНКИ

КИТАЙСЬКІ ХАКЕРСЬКІ ОПЕРАЦІЇ ПЕРЕЙШЛИ НА ЗНАЧНО БІЛЬШИЙ РІВЕНЬ НЕБЕЗПЕКИ, ПОПЕРЕДЖАЄ США

1 лютого видання Defense One розмістило матеріал, в якому йдеться про виступ директорів ФБР, АНБ та Агентства з кібербезпеки та безпеки інфраструктури перед законодавцями. Вони попередили, що кібердіяльність Китаю виходить за межі шпигунства та крадіжки даних і переходить до прямих атак на критично важливу інфраструктуру США. Повідомляється, що хакерська група Volt Typhoon, пов'язана з Китаєм, розміщує зловмисне ПЗ на мережевих маршрутизаторах та інших підключених до Інтернету пристроях, створюючи загрозу для водопостачання, електроенергії та залізничних перевезень, що може завдати реальної шкоди. Директори підкреслили ризик того, що Китай націлиться на водоочисні споруди, електричні мережі, нафто- та газопроводи та транспортні системи. Діяльність Китаю може бути пов'язана з військовою доктриною, яка ставить мету викликати паніку у суспільстві супротивників, особливо у сценаріях, пов'язаних із Тайванем. Сполучені Штати прагнуть вплинути на розрахунки Китаю, викриваючи та засуджуючи таку кібердіяльність, використовуючи вразливість Китаю до негативної громадської думки. ФБР виявило сотні маршрутизаторів, зламаних групою Volt Typhoon, що свідчить про постійну загрозу кібербезпеці США. Ще одна загроза від китайської кіберактивності це можливий негативний вплив на американську військову базу в Гуамі – американські безпекові структури занепокоєні тим, що китайські кібератаки можуть мати дуже значний вплив на її функціонування.

ВИПЛАТИ ВИМАГАЧАМ ПЕРЕВИЩИЛИ ОДИН МІЛЬЯРД ДОЛАРІВ У 2023 РОЦІ, ДОСЯГНУВШИ РЕКОРДНОГО РІВНЯ ПІСЛЯ ПАДІННЯ У 2022 РОЦІ

У звіті компанії Chainalysis, оприлюдненому 7 лютого, йдеться про те, що 2023 рік знаменує собою значне повернення програм-вимагачів із рекордними виплатами та суттєвим збільшенням обсягу та складності атак – і це становить суттєву різницю у порівнянні зі спадом, який спостерігався у 2022 році.

У 2023 році вимагачі активізували операції, націлившись на вагомі установи та критичну інфраструктуру, включаючи лікарні, школи та державні установи. Великі атаки програм-вимагачів на ланцюг постачання були здійснені з використанням повсюдного програмного забезпечення для передачі файлів MOVEit, що вплинуло на компанії від BBC до British Airways. У результаті цих та інших атак банди вимагачів досягли безпрецедентного рівня, перевищивши один мільярд доларів США у вимаганні платежів у криптовалюті від жертв. Компанія пояснює спад 2022 року російською агресією в Україні, адже вона з одного боку порушила існуючі схеми, а з іншого – призвела до того, що хакери перемкнули свою увагу на політично-мотивовані операції.

ЯК ВИГЛЯДАЄ CYBER COM 2.0?

Видання OODA Loop пише, що Кіберкомандування США (CYBERCOM) переживає значну реструктуризацію, відому як CYBERCOM 2.0, мета якого – адаптуватися до нових кіберзагроз. Вона включає розширення команд кібермісій і зміщення уваги з боротьби з тероризмом на загрози з боку держав. Попри реструктуризацію, подвійне керівництво з Агентством національної безпеки (АНБ) залишається незмінним, що викликає занепокоєння щодо слабкого контролю за виконанням повноважень та потенційного конфлікту інтересів. Акцент CYBERCOM на наступі, а не на захисті, про що свідчать нещодавні операції проти державних і недержавних суб'єктів, може посилити напруженість у кіберпросторі та спонукати ворогів прийняти подібну тактику. Необхідність ретельного розгляду наслідків дій CYBERCOM і потенційних стратегій помсти є надзвичайно важливою, щоб уникнути ненавмисної ескалації, зауважує видання.

ЛИШЕ 54% ЗМІН КОДУ ЗАСТОСУНКУ ПРОХОДЯТЬ ПОВНУ ПЕРЕВІРКУ БЕЗПЕКИ ПЕРЕД РОЗГОРТАННЯМ

12 лютого кібербезпекова компанія CrowdStrike оприлюднила свій звіт про стан безпеки застосунків. Було опитано 400 спеціалістів із безпеки застосунків у Сполучених Штатах, щоб дізнатися, як їх організації захищають застосунки, які інструменти та процеси вони використовують, і наскільки ефективна їхня робота. Всі фахівці вказують, що збільшення кількості застосунків в організаціях створює новий великий простір загроз (в тому числі персональним даним, які в них можуть оброблюватись), при цьому безпеку такої кількості нових IT систем забезпечити все складніше. Серед ключових цифр – лише 54% змін коду застосунків проходять повну перевірку безпеки, перш ніж перш їх розгорнуть у робочу версію.

G7 СПРИЙМАЮТЬ КІБЕРАТАКИ ЯК ДРУГИЙ ЗА ВЕЛИЧИНОЮ РИЗИК ДЛЯ СВОЇХ КРАЇН

12 лютого було оприлюднено Мюнхенський звіт про безпеку за 2024 рік. Одним з елементів звіту є Мюнхенський індекс безпеки (MSI). Відповідно до даних звіту, все більше країн відчувають кіберзагрози значним елементом безпекового ризику. Так, для країн G7 кіберзагрози посіли друге місце серед ризиків – одразу після екстремальних погодних явищ. Загалом загроза кібератак зросла у цьому індексі на п'ять позицій з минулого року.

У 2023 РОЦІ ЗЛОВМИСНИКИ СТАЛИ АКТИВНІШЕ ВИКОРИСТОВУВАТИ PDF ДЛЯ ЗАРАЖЕННЯ СИСТЕМ

Новий звіт HP Inc про тренди кібербезпеки, опублікований 15 лютого, висвітлює окремі тенденції в діяльності кіберзлочинців у 2023 році. Одним з висновків є помітне (з 4% у 2022 до 11% у 2023 році) зростання кількості спроби використати PDF для розгортання зловмисного ПЗ чи створення бекдорів в системах для подальшого продажу їх ransomware групам.

У 2023 РОЦІ НА 71% ЗРОСЛА КІЛЬКІСТЬ КІБЕРАТАК З ВИКОРИСТАННЯМ ДІЙСНИХ ОБЛІКОВИХ ЗАПИСІВ

21 лютого IBM X-Force поширило свій щорічний звіт Threat Intelligence Index 2024 з оцінками 2023 року та прогнозами на 2024 рік. Серед важливих висновків 2023 року – істотне (на 71%) зростання кількості кібератак з використанням дійсних облікових записів користувачів. Також звіт відмічає, що у 2023 році кількість нових вразливостей «нульового дня» була меншою ніж у 2022 році – лише 172 (на 72% менше порівняно з 2022 роком). Як і багато інших дослідників, фахівці IBM X-Force також роблять висновок, що на даному етапі очікувані загрози від використання генеративного інтелекту виявились перебільшеними, однак у майбутньому ця ситуація може швидко змінитись.

ЗВІТ SANS SOC SURVEY 2023 ВИЗНАЧАЄ ЧОТИРИ КЛЮЧОВИХ ВИКЛИКИ У РОЗВИТКУ СУЧАСНИХ SOC

21 лютого було поширено ключові результати з щорічного дослідження SANS Institute SOC Survey 2023. Серед іншого документ визначає низку базових викликів з якими стикаються всі сучасні SOC незалежно від сектору та обсягу організації:

- зростання занепокоєння з приводу нерозуміння контексту (тобто більш широкого погляду на загрози кібербезпеки, що ускладнює прийняття рішень);
- брак автоматизації та оркестровки (відсутність автоматизованих процесів перешкоджає ефективності, оскільки ручні завдання стають трудомісткими та повторюваними);
- навігація в «сліпих зонах» (SOC часто не бачить всю IT-інфраструктуру організації, а отже виникають потенційні сліпі зони, що дає зловмисникам можливість використовувати вразливості);
- дефіцит кваліфікованого персоналу (попит на професіоналів з кібербезпеки постійно перевищує кількість наявних кадрів, що створює серйозну проблему для організацій у створенні та підтримці надійних команд із безпеки).

ВИТІК ДАНИХ КИТАЙСЬКОЇ КІБЕРБЕЗПЕКОВОЇ КОМПАНІЇ I-SOON РОЗКРИВАЄ ЇХ ЗВ'ЯЗКИ З КИТАЙСЬКИМИ СПЕЦІАЛЬНИМИ СЛУЖБАМИ

22 лютого видання Newsweek поширило матеріал про витік документів китайської кібербезпекової компанії I-Soon – приватного підрядника, який активно співпрацює зі спеціальними службами КНР. Документи вказують, що підрядник активно залучений до поширення пропаганди, спостереження за активістами, які живуть за кордоном, а також порушення роботи мереж Wi-Fi. Також один з документів містив електронну таблицю яка вказувала на те, що I-Soon має 459 гігабайтів даних щодо дорожніх картах Тайваню, який Китай вважає своєю територією. Сховище даних було виявлено на GitHub аналітиком кіберзагроз із Тайваню.

Згідно з виданням APNews, Дамп, який аналітики вважають дуже значущим, навіть якщо він не розкриває жодних особливо нових чи потужних інструментів, включає сотні сторінок контрактів, маркетингових презентацій, посібників із продуктів, а також списків клієнтів і співробітників. Вони детально розкривають методи, використовувані китайською владою для стеження за дисидентами за кордоном, злому інших країн і просування пропекінських наративів у соціальних мережах.

НОВА ЕРА ХАКТИВІЗМУ

22 лютого видання The Hacker News відзначає помітне зростання явища хактивізму протягом останніх двох років, зокрема через триваючі війни та геополітичні конфлікти по всьому світу. Хактивізм, який передбачає використання хакерських методів для досягнення політичних чи соціальних цілей, став мейнстримом і переплітається з політичними конфліктами. Хактивістські групи націлені як на приватні, так і на державні організації, часто викликають страх, невпевненість і сумнів (FUD) у суспільстві.

Telegram став загальною платформою для спілкування хактивістів і координації їх діяльності, попри спроби платформи протистояти зловмисній поведінці. Хактивісти продемонстрували стійкість, створюючи нові канали та продовжуючи свою діяльність навіть після заборони.

У 2023 році значна частина хактивізму виникла через війну проти України, причому Європа була найбільш постраждалим регіоном. Проросійські хактивістські групи націлилися на такі країни, як Україна, Польща та Швеція. Серед цих груп Anonymous Sudan виділяється своєю непослідовністю та мінливими мотиваціями, тоді як NoName057(16) виглядає більш політично послідовним. Загалом хактивізм перетворився на складне та впливове явище, яке стирає межі між віртуальними та фізичними конфліктами.

54% АМЕРИКАНЦІВ РОЗКРИЛИ Б ДАНІ СВОГО ОБЛІКОВОГО ЗАПИСУ ЗАРАДИ ОТРИМАННЯ ЗНИЖКИ

23 лютого розробник продукту NordVPN поділився результатами свого дослідження щодо готовності американської аудиторії ділитись персональними даними в обмін на обіцянку отримання знижки. Більша частина готова ділитись даними своєї електронної пошти та своїм повним ім'ям, понад 10% готові ділитись інформацією про роботодавця. Автори опитування вказують, що така готовність людей ділитись персональними даними ставить питання про надійність систем кібербезпеки організацій роздрібної торгівлі, які найбільше стикаються з персональними даними покупців.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

У КИЄВІ ВІДБУВСЯ МІЖНАРОДНИЙ ФОРУМ З КІБЕРБЕЗПЕКИ 2024

7-8 лютого у столиці України відбувся перший Київський міжнародний форум з кібербезпеки 2024: «Стійкість під час кібервійни», започаткований НКЦК при РНБО України та партнерами. Захід відкривав Секретар РНБО України Олексій Данілов. Також зі сцени Форуму виступив Михайло Федоров, Віцепрем'єр-міністр з інновацій, розвитку освіти, науки та технологій — Міністр цифрової трансформації України та представники міжнародної кіберспільноти, серед яких: Натаніель Фік, посол США з особливих повноважень з питань кіберпростору Держдепартаменту США, Йоганнек Белфорт, директор з питань безпеки та оборонної політики Європейської служби зовнішньої діяльності, Юхан Лепасар, директор Агентства ЄС з питань кібербезпеки (ENISA), Март Ноорма, керівник Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE), Джен Істерлі, директор Агентства США з питань кібербезпеки та захисту критичної інфраструктури (CISA).

Загалом у Форумі взяли участь понад тисяча учасників. За два дні заходу відбулося 10 панельних дискусій і понад 40 доповідей експертів, які охоплювали широкий спектр тем, серед яких: роль кібербезпеки у сучасних війнах, досвід України у кібервійні, кібервійна і міжнародне право, кібердипломатія, посилення стійкості національної системи кібербезпеки через освіту, захищеність месенджерів, роль розвідки кіберзагроз, кібербезпека регіонів та інші.

У рамках KICRF відбулися дводенні змагання з кібербезпеки Capture the Flag. Участь взяла 21 команда, загальна кількість учасників — 121 фахівець із державного і приватного секторів.

УКРАЇНА ТА США ПОГЛИБЛЮЮТЬ СТРАТЕГІЧНЕ ПАРТНЕРСТВО У СФЕРІ КІБЕРБЕЗПЕКИ

В рамках Київського міжнародного форуму з кібербезпеки відбулася зустріч Віцепрем'єр-міністра з інновацій, розвитку освіти, науки та технологій – Міністра цифрової трансформації Михайла Федорова та Голови Державної служби спеціального зв'язку та захисту інформації України Юрія Мироненка з Послом з особливих доручень з питань кіберпростору та цифрової політики Державного департаменту США Натаніелем Фіком і Директором агентства з кібербезпеки та безпеки інфраструктури Департаменту національної безпеки Сполучених Штатів Америки (CISA) Джен Істерлі. У зустрічі також взяла участь Посол США в Україні Бріджит Брінк.

Сторони зійшлися на думці, що запланована раніше співпраця, зокрема щодо обміну досвідом між США та Україною з питань, пов'язаних з кіберпростором, є успішною та поділилися баченням актуальних напрямів роботи, які необхідно активізувати. На зустрічі також обговорили коротко- та довгострокові потреби України у сфері кіберзахисту.

УКРАЇНСЬКІ ТА ЕСТОНСЬКІ ФАХІВЦІ З КІБЕРБЕЗПЕКИ ДОМОВИЛИСЯ ПРО ПОСИЛЕННЯ СПІВПРАЦІ

Задля визначення подальших напрямів спільної роботи у сфері кіберзахисту делегація кіберфахівців з Естонії з офіційним візитом відвідала Держспецзв'язку. Під час зустрічі активно обговорювалися перспективи посилення взаємодії між Урядовою командою реагування на комп'ютерні надзвичайні події CERT-UA та аналогічним підрозділом з Естонії – CERT-EE. Ключове – забезпечити ефективний та максимально оперативний двосторонній обмін інформацією про кіберзагрози, результати дослідження кібератак, вразливості в захисті інформаційних систем, а також обмін досвідом реагування на дії російських хакерів. Учасники зустрічі також обговорили подальшу реалізацію ініціатив у межах Меморандуму про співпрацю з Департаментом державної інфосистеми (RIA), що відповідає за кібербезпеку Естонії.

ДЕРЖСПЕЦЗВ'ЯЗКУ ПОСИЛЮЄ СПІВПРАЦЮ У СФЕРІ КІБЕРЗАХИСТУ ТА ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Заступник Голови Держспецзв'язку Олександр Потій провів зустріч з представниками іноземної делегації у складі Генерального Директора Фонду цивільних досліджень та розвитку США CRDF Global Майка Дігнема, старшого радника Фонду Томаса Калахена та регіонального директора представництва Фонду Михайла Верича, які з візитом завітали до Служби. Ключовими питаннями для обговорення стали захист українських інформаційних ресурсів у кіберпросторі та захист об'єктів критичної інфраструктури, які зазнають різноманітних загроз, пов'язаних передусім з російською агресією проти нашої держави. Партнери висловили готовність не просто продовжувати всебічну підтримку України, а й посилювати співпрацю.

НКЦК РОЗПОЧАВ НАВЧАННЯ «УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ» ДЛЯ ФАХІВЦІВ ОВА

У рамках посилення заходів щодо забезпечення кібербезпеки на регіональному рівні НКЦК при РНБО України спільно з Центром кіберзахисту Нацбанку та за підтримки CRDF Global в Україні розпочав навчання «Управління вразливостями» (VDP) для представників обласних військових адміністрацій. В програмі беруть участь понад 70 профільних технічних спеціалістів з усіх областей України.

Навчальний курс VDP триватиме сім тижнів. Під час навчання спеціалісти з кібербезпеки отримають теоретичні та практичні знання щодо мережевих технологій, оцінки відповідності кращим практикам, тестування інформаційних систем та вебзастосунків на вразливості, опрацювання взаємодії під час інформування про інциденти та вразливості.

ДЕРЖСПЕЦЗВ'ЯЗКУ ПОСИЛЮЄ ЗНАННЯ ТА НАВИЧКИ З РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ КЕРІВНИЦТВА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ТА ДЕРЖОРГАНІВ

Державна служба спеціального зв'язку та захисту інформації України разом з партнерами провела другий одноденний офлайн семінар «Реагування на кіберінциденти» для заступників керівників державних органів та об'єктів критичної інфраструктури з питань цифрового розвитку, цифрових трансформацій і цифровізації (CDTO). Серед завдань, над якими працювали CDTO, було моделювання ситуації виявлення факту несанкціонованого доступу до інформаційно-комунікаційних систем (ІКС) та формування порядку дій щодо ізоляції ІКС, вживання заходів з ідентифікації поверхні атаки та її зменшенні тощо.

РОЗВІДІНФОРМАЦІЯ, ЗІБРАНА КІБЕРМЕТОДАМИ, ДОПОМАГАЄ СБУ ПРОВОДИТИ УНІКАЛЬНІ СПЕЦОПЕРАЦІЇ – ІЛЛЯ ВІТЮК

Про це розповів начальник Департаменту кібербезпеки СБУ Ілля Вітюк на Київському міжнародному форумі з кібербезпеки «Стійкість під час кібервійни»: «Ми діємо проактивно: проникаємо глибоко до систем ворога. Наша основна мета – отримати важливу розвідувальну інформацію, яка потім використовується у топових спецопераціях СБУ. Це і ліквідації воєнних злочинців, і ураження військових об'єктів та інфраструктури, що працює на російський ВПК, та інші. У багатьох спецопераціях СБУ сьогодні присутній кіберкомпонент».

Крім того, за його словами, зібрана розвідінформація передається Силам оборони або ж міжнародним партнерам, якщо це стосується, наприклад, спроб уникнення санкцій з боку рф. Таким чином СБУ перешкоджає росії налагодити нові ланцюжки постачання, щоб продовжувати війну проти України.

УКРАЇНСЬКІ КОМАНДИ ПЕРЕМОГЛИ У NATO TIDE HACKATHON 2024

NATO TIDE Hackathon – щорічне змагання, яке проводить Командування НАТО з трансформації для пошуку інноваційних рішень та розв'язання проблем взаємосумісності Альянсу. Він є частиною циклу подій, мета яких – покращити взаємосумісність НАТО та союзників через пошук інноваційних рішень та підходів.

Цього року хакатон був організований спільно з голландським IT-командуванням та цього року проходив в Амстердамі. У ньому взяли участь 34 команди з 21 країни — представники державних та оборонних структур, а також 5 команд з приватного сектору. Змагання проходили за трьома ключовими напрямками: Wargaming LLM, Pharmaceutical Thesaurus та Noisy Speech to Text. Українські команди Valkyrie-1 та Valkyrie-2 перемогли у перших двох.

КОМАНДА ДЕРЖАВНОГО ЦЕНТРУ КІБЕРЗАХИСТУ ДЕРЖСПЕЦЗВ'ЯЗКУ ПОСІЛА ДРУГЕ МІСЦЕ НА КІБЕРНАВЧАННЯХ У ВАРШАВІ

Українська команда «Netflix&Chill» посіла друге місце у загальному рейтингу змагань, що пройшли в межах кібернавчань із захисту об'єктів критичної інфраструктури, які тривали з 5 по 9 лютого 2024 року у Варшаві (Польща). Загалом у змаганнях взяли участь 16 команд з Німеччини, Албанії, Польщі, Естонії, Литви, Словаччини, Словенії, Молдови та Румунії.

Проведення кібернавчань також забезпечило поглиблене вивчення таргетованих атак на об'єкти критичної інфраструктури енергетичного сектору, визначення індикаторів обміну та розробку стратегій пом'якшення впливу спрямованих на енергетичний сектор.

УРЯДОВА КОМАНДА CERT-UA У 2023 РОЦІ ОПРАЦЮВАЛА 2543 КІБЕРІНЦИДЕНТИ

CERT-UA за минулий рік опрацювала 2543 кіберінциденти, що на 15,9% більше ніж за 2022 рік. Найбільше зловмисники атакують уряд та урядові організації, місцеві органи влади та сектор безпеки та оборони, комерційні організації, енергетичний сектор, телекомунікації та багато інших установ.

Найпоширенішими типами інцидентів є розповсюдження шкідливого програмного забезпечення, фішинг, шкідливе підключення, компрометація облікового запису та компрометація системи. Метою зловмисників є розвідувальні операції, довготривале шпигунство, знищення даних та інформаційних систем. Кількість ворожих атак продовжує збільшуватися.

ОПРАЦЬОВАНО 46 ТИСЯЧ КРИТИЧНИХ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ЗВІТ ОПЕРАТИВНОГО ЦЕНТРУ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ДЦКЗ

Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Держспецзв'язку оприлюднив звіт за результатами роботи системи виявлення вразливостей (СВВ) та реагування на кіберінциденти в IV кварталі 2023 року. За цей період за допомогою засобів системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було опрацьовано 1,4 мільярда подій, отриманих за допомогою засобів моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки, детектовано 2 мільйони підозрілих подій інформаційної безпеки (при первинному аналізі) та опрацьовано 46 тисяч критичних подій інформаційної безпеки (потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу). При цьому зафіксовано та оброблено безпосередньо аналітиками безпеки 357 кіберінцидентів. Повний текст звіту ДЦКЗ: https://scpc.gov.ua/uk/articles/341

СБУ СПІЛЬНО З ПРАВООХОРОНЦЯМИ США, ВЕЛИКОЇ БРИТАНІЇ ТА ЄС ВИКРИЛА МІЖНАРОДНЕ УГРУПОВАННЯ ХАКЕРІВ-ВИМАГАЧІВ

Кіберфахівці Служби безпеки спільно з правоохоронними органами США, Великої Британії, Євросоюзу та інших країн-партнерів провели масштабну спецоперацію у різних частинах світу. У результаті спільних дій викрито учасників потужного міжнародного угруповання хакерів під назвою «LockBit». За матеріалами справи, зловмисники викрадали у відомих компаній таємну інформацію і персональні дані, а потім вимагали за них «викуп». Серед організаторів та учасників угруповання були громадяни України та рф.

Протягом майже 5 років зловмисники здійснили понад три тисячі кібератак проти фінансових установ та корпорацій західних країн, які надають оборонну допомогу Україні. Для викрадення корпоративних відомостей хакери використовували спеціально розроблені програми-вимагачі.

ПОЛІЦЕЙСЬКІ ВИКРИЛИ ЖИТЕЛЯ ОДЕСИ, ЯКИЙ ОБМАНОМ ОТРИМУВАВ ІНФОРМАЦІЮ ПРО БАНКІВСЬКІ КАРТКИ УКРАЇНЦІВ

Поліцейські встановили, що житель Одеси створив і розмістив у популярних соціальних мережах посилання на сайт, зовнішній вигляд якого повністю копіював дизайн сайту Державної допомоги в рамках програми «єПідтримка». З переходом громадян за посиланням з фішинговими формами по грошову допомогу від держави зловмисник отримував реквізити їхніх платіжних карток: номер, CVV код, термін дії та інші. За скоєне йому загрожує позбавлення волі.

СБУ ЗАТРИМАЛА ДІЛКІВ, ЯКІ ДОПОМОГЛИ ФСБ ВЗЯТИ ПІД КОНТРОЛЬ МАЙЖЕ ВЕСЬ ІНТЕРНЕТ-ТРАФІК В ТИМЧАСОВО ОКУПОВАНОМУ ДОНЕЦЬКУ

Кіберфахівці Служби безпеки затримали у Києві керівників підконтрольного фсб рф інтернет-провайдера із Донецька. Зловмисники співпрацюють з агресором на тимчасово захопленій частині України, але намагалися «легалізуватися» у столиці. Зокрема на серверах провайдера встановлено спеціалізоване обладнання російської спецслужби, яке дозволяє фсб моніторити всі інтернет-дії мирного населення регіону.

Одержані відомості фсб використовує для вербування мешканців регіону та їх подальшого залучення до розвідувально-підривної діяльності проти України. Зловмисники перебувають під вартою. Їм загрожує до 15 років тюрми.

КІБЕРПОЛІЦЕЙСЬКІ ВІННИЧИНИ ВИКРИЛИ ХАКЕРА, ЯКИЙ «ЗАРОБИВ» ПОНАД 3,5 МЛН ГРН НА ВИКРАДЕННІ ДАНИХ МЕШКАНЦІВ США ТА КАНАДИ

Хакер створив та адміністрував кілька сайтів, де пропонував користувачам безкоштовно завантажити різноманітне програмне забезпечення. Фігурант розгорнув в інтернеті цілу рекламну кампанію для «просування» підконтрольних вебресурсів, а насправді за допомогою шкідливого програмного забезпечення викрадав і продавав персональні дані жителів Канади та США. Зловмиснику повідомлено про підозру, йому загрожує до 8 років позбавлення волі з конфіскацією майна.

РОСІЙСЬКІ ЗАГАРБНИКИ ПОСИЛЮЮТЬ ЗАХОДИ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ НА УКРАЇНЦІВ В ОКУПАЦІЇ

Головне управління розвідки Міністерства оборони України інформує, що мешканців окупованих громад Херсонщини масово під'єднують до російського супутникового телебачення під назвою «русскій мір», щоб перекрити канали доступу до інформації про реальну ситуацію на фронті, в Україні та світі. Наразі росіяни встановили вже понад 18 тисяч відповідних пристроїв.

Також у тимчасово окупованих українських громадах Донеччини загарбники переводять на власне програмне забезпечення та комунікаційні сервіси роботу окупаційних адміністрацій та розширюють мережу покриття російського мобільного зв'язку: у 2023-24 роках було встановлено понад 700 базових станцій, а на Херсонщині — понад 200, що становить понад 85% усього мобільного покриття в окупованому регіоні.

ГУР РОЗПОВІЛО ПРО УСПІШНУ КІБЕРАТАКУ НА ПРОГРАМИ КЕРУВАННЯ ДРОНАМИ РФ

Кіберфахівці ГУР МО України здійснили чергову успішну операцію проти російських окупантів, що призвело до масового збою програми керування дронами. Цей софт росіяни встановлюють для перепрошивки безпілотників марки DJI під потреби ведення бойових дій – забезпечення функціонування системи «свій-чужий». За попередніми даними, внаслідок кібератаки ГУР МО України сервери перестали працювати, тож усе програмне забезпечення розпізнається як "чуже" і відмовляє рашистам у доступі.

CERT-UA РОЗПОВІВ ПРО КІБЕРАТАКУ НА СИЛИ ОБОРОНИ УКРАЇНИ

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA зафіксувала та вжила заходів щодо нейтралізації нової кібератаки, спрямованої на представників Сил оборони України. Зловмисники намагалися вразити комп'ютери військових шкідливим програмним забезпеченням. Атака була здійснена через месенджер Signal. За даними CERT-UA, активність здійснюється щонайменше з осені 2023 року, має точковий характер та відстежується за ідентифікатором – UAC-0149.

РОСІЙСЬКІ ХАКЕРИ АТАКУВАЛИ ВІДОМІ УКРАЇНСЬКІ МЕДІА

ворожі хакери здійснили чергову атаку на низку українських медіа та розмістили на їхніх ресурсах фейкову інформацію. До Урядової команди реагування на комп'ютерні надзвичайні події CERT-UA, що діє при Держспецзв'язку, звернулися представники Української правди, Liga.net, Апострофу та Телеграфу. Наразі проводяться дослідження вказаного інциденту.

УРАЖЕНО ПОНАД 2000 КОМП'ЮТЕРІВ – CERT-UA ВЖИЛА ЗАХОДІВ ЩОДО АТАКИ НА УКРАЇНСЬКЕ ДЕРЖАВНЕ ПІДПРИЄМСТВО

CERT-UA надала практичну допомогу державному підприємству. Комп'ютери компанії зазнали масового ураження шкідливою програмою DIRTYMOE (PURPLEFOX), що надає віддалений доступ до уражених пристроїв. Урядова команда CERT-UA провела дослідження отриманих зразків шкідливих програм, встановила особливості функціонування інфраструктури управляючих серверів і виявила більше ніж 2000 уражених комп'ютерів в українському сегменті мережі Інтернет. Описана активність відстежується за ідентифікатором UAC-0027. Більше деталей про атаку на сайті Урядової команди CERT-UA: https://cert.gov.ua/article/6277422

8. ПЕРША СВІТОВА КІБЕРВІЙНА

РОСІЙСЬКІ ШПИГУНИ ВИДАЮТЬ СЕБЕ ЗА ЗАХІДНИХ ДОСЛІДНИКІВ

1 лютого видання The Record повідомило про викриття кампанії зломів, в якій хакери російських розвідувальних служб видають себе за дослідників та науковців, щоб отримати доступ до облікових записів електронної пошти їх колег. Техніка атакуючих полягає у створенні автентичних на вигляд статей, щоб заманити жертв проханням дати відгук, потім вкрасти дані їх облікових записів. Secureworks та Mandiant незалежно проаналізували кібератаку та підтвердили її походження. За нею стоїть спонсорована державою група загрози, яку називають Iron Frontier, Calisto, Coldriver або Star Blizzard/Seaborgium, і вважають такою, що працює на російські розвідувальні служби.

США МАЮТЬ ПРИДІЛИТИ ОСОБЛИВУ УВАГУ КІБЕРБЕЗПЕЦІ МОЛДОВИ НА ФОНІ СИТУАЦІЇ В УКРАЇНІ – CSIS

2 лютого Лія Кіфф з американського дослідницького центру CSIS опублікувала розгорнутий матеріал щодо кіберзагроз, з якими стикається Молдова та можливої політики США щодо цієї країни. Матеріал підкреслює важливість надання кібербезпекової допомоги з боку США аби не допустити масштабних кібератак та порушення виборчого процесу. Матеріал підкреслює, що Молдова має максимально врахувати досвід України аби ліпше підготуватись до деструктивної російської кіберактивності. Це включає розвиток державно-приватного партнерства, боротьбу з завербованими інсайдерами в уряді та протидію операціям впливу.

КАМПАНІЯ STEADY#URSA АТТАСК ПРОТИ УКРАЇНСЬКИХ ВІЙСЬКОВИХ

Команда Securonix Threat Research спостерігає за поточною кампанією, яка, ймовірно, пов'язана з Shuckworm і спрямована на українських військових (відстежується Securonix Threat Research як STEADY#URSA). Шкідливе навантаження доставляється через стислі файли, можливо, через фішингові електронні листи. Багато зразків, які виявила команда, містили багатослівні слова про українські міста та військову термінологію. Атака, ймовірно, пов'язана з Shuckworm, оскільки він містить кілька ексклюзивно використовуваних TTP, ексклюзивних для групи, про яку повідомлялося в попередніх кампаніях проти українських військових.

САЙТ МІНОСВІТИ НЕ ПРАЦЮЄ ЧЕРЕЗ КІБЕРАТАКУ РОСІЯН

7 лютого Міністерство освіти України повідомило, що його сайт не працював через атаку російських хакерів. Деталі інциденту не повідомлялись.

США ЙМОВІРНО ЗДІЙСНИЛИ КІБЕРАТАКУ НА ІРАНСЬКИЙ ШПИГУНСЬКИЙ КОРАБЕЛЬ

15 лютого NBC News повідомило, що Сполучені Штати здійснили кібератаку на іранський військовий корабель у Червоному морі. Корабель збирав розвідувальні дані про вантажні судна. Операція мала на меті перешкодити здатності корабля ділитися розвідданими з бойовиками Хуси в Ємені. Атака була здійснена в межах протидії діяльності бойовикам Хуси в Ємені.

ВОРОГ ПЛАНУВАВ ДРУГУ ХВИЛЮ КІБЕРАТАКИ НА КИЇВСТАР, ЯКА МОГЛА «ОБНУЛИТИ» БАЗОВІ СТАНЦІЇ – СБУ

7 лютого начальник департаменту кібербезпеки СБУ Ілля Вітюк повідомив, що після хакерської атаки проти мобільного оператора «Київстар», яка відбулася у грудні 2023 року, ворог планував другу хвилю, яка могла «обнулити» всі базові станції. Вітюк наголосив, досі триває розслідування і триватиме ще дуже довгий час, тому що під час атаки було знищено сотні серверів, а тисячі комп'ютерів повністю витерто.

РОСІЙСЬКІ ХАКЕРИ АТАКУЮТЬ УКРАЇНУ ДЕЗІНФОРМАЦІЄЮ ТА ЗБИРАННЯМ ОБЛІКОВИХ ДАНИХ

Дослідники кібербезпеки зі словацької компанії ESET виявили нову операцію впливу, націлену на Україну, яка використовує спам для поширення дезінформації, пов'язаної з війною. ESET пов'язує цю діяльність із загрозливими діячами, що мають відношення до росії. Операція Texonto, якою була кодова назва всієї кампанії, не була приписана конкретному загрозливому актору, хоча деякі її елементи, зокрема фішингові атаки, збігаються з COLDRIVER, який має історію збирання облікових даних через фальшиві сторінки входу. Детальніше про операцію – у звіті компанії.

ПОВ'ЯЗАНИЙ З РОСІЄЮ TAG-70 НАЦІЛЮЄТЬСЯ НА ЄВРОПЕЙСЬКІ УРЯДОВІ ТА ВІЙСЬКОВІ ПОШТОВІ СЕРВЕРИ В РАМКАХ НОВОЇ ШПИГУНСЬКОЇ КАМПАНІЇ

19 лютого компанія Recorded Future повідомила, що викрила зловмисників, які діють в інтересах Білорусі та росії, пов'язаних з новою кампанією кібершпигунства. Ця кампанія, ймовірно, скористалася з вразливостей міжсайтових сценаріїв (XSS) на серверах вебпошти Roundcube для націлювання на понад 80 організацій. Компанія відстежує це хакерське угруповання під назвою Threat Activity Group 70 (TAG-70).

Кампанія, виявлена компанією Recorded Future, тривала з початку жовтня 2023 року до середини місяця з метою збору розвідданих про політичну та військову діяльність Європи. Атаки збігаються з додатковою активністю TAG-70 проти урядових поштових серверів Узбекистану, які були виявлені в березні 2023 року.

У ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ РОСІЙСЬКОГО УРЯДУ ЗАПРОВАДЖЕНО БЕКДОР ДЛЯ РОЗГОРТАННЯ ЗЛОВМИСНОГО ПЗ KONNI RAT

В інсталятор для інструменту, який, ймовірно, використовується Консульським відділом міністерства закордонних справ росії, був запроваджений бекдор для доставки трояна віддаленого доступу під назвою Konni RAT (він же UpDog).

За висновками німецької компанії з кібербезпеки DCSO, ця активність пов'язана з діяльністю Корейської Народно-Демократичної Республіки (КНДР), націленою на росію.

УКРАЇНСЬКІ ХАКЕРИ АТАКУВАЛИ СЕРВЕРИ РФ І ОТРИМАЛИ ДОСТУП ДО ПОНАД 5 ТБ ІНФОРМАЦІЇ

Стратком ЗСУ поінформував, що 25 лютого було зафіксовано велику хакерську атаку на сайти рф. У результаті роботи групи хакерів UA25 було вивантажено 5 терабайтів особистої і корпоративної конфіденційної інформації.

9. РІЗНЕ

МАТЕРИНСЬКА КОМПАНІЯ ЯНДЕКС ПРОДАСТЬ СВІЙ РОСІЙСЬКИЙ БІЗНЕС ЗА $5,2 МЛРД

Материнська компанія групи Яндекс, що базується в Нідерландах, 5 лютого повідомила, що продає свій російський бізнес місцевим інвесторам за 5,2 мільярда доларів. Попри обов'язкову знижку принаймні наполовину, яку вимагає кремль, це буде найбільший корпоративний вихід з росії з того часу, як вона вторглася в Україну два роки тому. Рух росії до повної ізоляції Інтернету – це стратегія, яка ненавмисно впливає на Яндекс. Оскільки Яндекс є технологічною компанією, що надає низку пов'язаних з Інтернетом послуг, посилення цензури може призвести до того, що Яндекс стане головною жертвою. Ця подія підкреслює агресивний підхід росії до контролю над своєю цифровою екосистемою потенційно шляхом промисловості та інновацій.

КІБЕРПОМСТА КИТАЮ – ЧОМУ КНР НЕ НАДАЄ ДОКАЗІВ СВОЇМ ЗАЯВАМ ПРО ШПИГУНСТВО З БОКУ ЗАХОДУ

12 лютого компанія Sentinel Labs оприлюднила звіт щодо звинувачень Китаю на адресу заходу у кібершпигунстві. У звіті йдеться про наступне:

- після спільної заяви США, Великобританії та ЄС у липні 2021 року щодо безвідповідальної поведінки Китаю в кіберпросторі Китай вдався до наступальної медіа-стратегії, поширюючи наративи щодо хакерських операцій США.
- деякі кібербезпекові компанії КНР координують публікацію звітів з урядовими установами та державними ЗМІ, намагаючись посилити вплив.
- звинуваченням у хакерських операціях США з боку Китаю не вистачає важливого технічного аналізу, який би підтвердив їхні твердження. До 2023 року ці звіти переповідали старі документи розвідки США, які було злито в мережу. Після середини 2023 року КНР відмовилася від технічної валідації та оприлюднює звинувачення лише в державних ЗМІ.
- медійна кампанія, орієнтована на кіберпростір, передувала спробам Міністерства державної безпеки Китаю у 2023 році розкрити дані про західне шпигунство в КНР.