НКЦК

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ
ЦЕНТР КІБЕРБЕЗПЕКИ

CYBER DIGEST

Огляд ключових подій у світі
кібербезпеки за жовтень 2022

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

Підготовлено за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України»

Створення цієї публікації стало можливим завдяки підтримці американського народу, наданій через Агентство США з міжнародного розвитку (USAID). Погляди авторів, висловлені у цій публікації, не обов'язково відображають погляди USAID або Уряду США.

ЗМІСТ

ОСНОВНІ ТЕНДЕНЦІЇ

Міжнародні партнери України продовжують робити висновки з триваючої світової кібервійни. Частину з них вже оприлюднили представники американських та британських кібервідомств. Вони відзначають значні спроможності України для захисту та швидкого відновлення. Помітним фактором триваючого протиборства стає роль приватного сектору, який швидше реагує на зміну ситуації і саме їх інформація допомагає державним органам бути ефективнішими. російські хакерські групи все частіше атакують цілі за межами України (як державні органи, так і приватні компанії), які пов'язані із українським спротивом російській агресії.

Триваюча світова кібервійна впливає на більш широкий контекст питань, ніж власне кібербезпека окремих суб'єктів. Вона вже впливає на дискусію щодо майбутніх правил поведінки в інтернеті (перспектив розвитку Декларації майбутнього інтернету), зміну ландшафту загроз та ескалації кіберактивності. А також частково впливає на внутрішньополітичну ситуацію в самій рф, що набуває форм своєрідної кіберопозиції до режиму путіна. Деякі російські хакери починають розв'язувати кібервійну всередині своєї країни.

США продовжують заходи спрямовані на посилення кібербезпеки федеральних мереж. Протягом жовтня впроваджено нову обов'язкову директиву. Під егідою Кіберкомандування США проведено заходи із поліпшення координації дій різних суб'єктів та посилено заходи з розробки Національної стратегії збільшення кількості кіберфахівців (на фоні даних про нестачу 700 тис. таких фахівців лише в США і 3,7 млн у всьому світі). Ключові кібербезпекові відомства США (CISA, NSA, FBI) продовжують відстежувати зловмисну кіберактивність, випускаючи попередження про нові загрози та інструкції щодо зменшення ризиків їх реалізації. У фокусі уваги залишаються три питання: віруси вимагачі, попередження атак проти ланцюжків постачання та використання SBOM для зменшення загроз в стратегічній перспективі.

Триває дискусія про проблеми збору та розкриття інформації про кібератаки та можливі загрози недержавним суб'єктам. Дослідники кажуть про необхідність принципового вирішення проблеми збору необхідної статистики, а також розширення обов'язків розвідувальний спільноти щодо попередження цивільного сектору про кіберзагрози. Це питання піднімає і керівник NSA в контексті російсько-української кібервійни, вказуючи, що приватні компанії швидше реагують на інциденти та мають більш оперативну інформацію ніж урядові структури.

Європейські країни зіштовхуються з новими проблемами та шукають шляхи вирішення більш традиційних. Зокрема, диверсії на «Північному потоці» поставило перед Францією питання захисту підводних кабелів, що забезпечують інтернет на європейському континенті. Великобританія надала нові рекомендації приватному сектору щодо більш ефективного убезпечення від загроз пов'язаних із ланцюжком постачання. ENISA у жовтні сконцентрувалась на питаннях кібербезпеки медичної сфери (яка все частіше потерпає від вірусів-вимагачів). Євродепутати занепокоєні можливістю посилення присутності китайської технологічної компанії в аеропорту Страсбургу.

Постквантовий світ у фокусі уваги дослідників. Корпорація RAND та ENISA оприлюднили свої оцінки пов'язані із постквантовою криптографією та оцінкою зусиль урядів в цьому напрямку. NIST продовжує активність щодо розробки стандартів для цього нового виміру проблеми. Ключовою загрозою залишається можливість прихованого створення першого квантового комп'ютера та використання його потужностей для розшифровки раніше вкрадених секретних даних.

Через низку нищівних кібератак, яких останнім часом зазнали кілька країн НАТО (Чорногорія та Албанія, як останні приклади) актуальності набуває питання застосування 5 статті договору НАТО у кіберпросторі. На сьогодні не визначена ані межа, за якою наступає відповідь Альянсу, ані спосіб, у який Альянс має реагувати. Це питання поступово актуалізується у порядку денному міжнародного діалогу у сфері кібербезпеки.

У жовтні актуалізувались питання транскордонного обміну даними. Одночасно з аналізом наявних практик такого обміну відбулось декілька подій в цій сфері. Зокрема, підписано Рамковий підхід до конфіденційності даних між ЄС і США, набрав чинності договір між США та Великою Британією щодо доступу до електронних даних.

Атаки проти критичної інфраструктури продовжуються. Зростають загрози для окремих критичних галузей – наприклад компанії нафтогазового сектору особливо вразливі до кібератак (NIST вже створює профіль кібербезпеки для організацій такого типу). Ці загрози реалізуються на фоні нестачі фахівців з кібербезпеки у всіх сферах, часто неготовності власників інвестувати у збільшення фахівців (а не лише інструменти детекції) і психологічного вигорання наявних фахівців, які перевантажені завданнями.

Зловмисники продовжують поліпшувати свої техніки та змінювати інструментарій атак. Вони вдаються до ґрунтовної модифікації старих зловмисних програм (надаючи їм нові функції), створюють все більше сервісних інструментів для інших зловмисників (MaaS – зловмисне програмне забезпечення як послуга, RaaS – програми вимагачі як послуга), або (як у випадку з китайськими хакерами) вдаються до використання старих і відомих вразливостей, які так і не були виправлені фахівцями з безпеки в організаціях.

Значну увагу до себе привертає російське хакерське угруповання Killnet, яке активізувалося останнім часом. У жовтні ця група провела цілу серію атак проти урядових сайтів США та Болгарії, а також сайтів 14 американських аеропортів, але всі не мали помітного успіху. Дослідники не знайшли доказів його зв'язку з російськими державними органами, а, також, не вважають його значною загрозою, адже угрупування практикує переважно DDos атаки, які роблять атаковані сайти недоступними для користувачів. Як внутрішня структура сайтів, так і конфіденційні дані, залишаються неушкодженими. Разом з тим, угрупування веде активну діяльність в інформаційній сфері. Воно має власний телеграм-канал, де публікує заяви серед іншого про те, що його атаки є помстою за підтримку України у війні проти РФ.

Значну увагу до себе привертає російське хакерське угруповання Killnet, яке активізувалося останнім часом. У жовтні ця група провела цілу серію атак проти урядових сайтів США та Болгарії, а також сайтів 14 американських аеропортів, але всі не мали помітного успіху. Дослідники не знайшли доказів його зв'язку з російськими державними органами, а, також, не вважають його значною загрозою, адже угрупування практикує переважно DDos атаки, які роблять атаковані сайти недоступними для користувачів. Як внутрішня структура сайтів, так і конфіденційні дані, залишаються неушкодженими. Разом з тим, угрупування веде активну діяльність в інформаційній сфері. Воно має власний телеграм-канал, де публікує заяви серед іншого про те, що його атаки є помстою за підтримку України у війні проти РФ.

Загострюється конкуренція між США та Китаєм за майбутнє інтернету та лідерство у сфері новітніх технологій. Стратегія національної безпеки США, яка була опублікована цього місяця, вказує на те, що США розглядають світ під кутом конкуренції між авторитарними та демократичними країнами та планують просувати своє бачення інтернету та норм поведінки у кіберпросторі. Практичними кроками у цьому напрямку стали рішення щодо обмеження доступу Китаю до американських новітніх технологій та продовження роботи у напрямку обміну даними та встановлення спільних правил для штучного інтелекту між демократичними країнами.

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

КІБЕРКОМАНДУВАННЯ США ПОВІДОМИЛО ПРО ПРОВЕДЕННЯ НОВОЇ ОПЕРАЦІЇ В КІБЕРПРОСТОРІ

17 жовтня Кіберкомандування США оприлюднило інформацію, що в період з 3 по 14 жовтня 2022 року вони провели оборонну операцію в кіберпросторі.
Мета операції – покращити взаємодію CYBERCOM із партнерами. «Операція була безперервною діяльністю, спрямованою на посилення стійкості інформаційної мережі Міністерства оборони (DODIN) та інших допоміжних систем», – сказав контрадмірал ВМС США Метью С. Парадайз, заступник директора з операцій J-3. Кіберкомандування США. Операція проходила одночасно в різних мережах Міністерства оборони та в усьому світі за участю партнерів-учасників.

ФБР США ТА CISA ВИПУСТИЛИ ПУБЛІЧНЕ ОГОЛОШЕННЯ, В ЯКОМУ ЗАПЕВНЯЮТЬ, ЩО КІБЕРАТАКИ НЕ ЗАВАДЯТЬ ВИБОРАМ В США

4 жовтня ФБР США та CISA заявили, що станом на дату їх повідомлення у них немає жодної інформації, яка б свідчила, що кіберактивність коли-небудь перешкоджала зареєстрованому виборцю проголосувати, скомпрометувала цілісність будь-яких поданих бюлетенів або вплинула на точність інформації про реєстрацію виборців. «Будь-які спроби, які відстежували ФБР і CISA, залишалися локалізованими та були заблоковані або успішно пом'якшені з мінімальним порушенням виборчих процедур або без порушень».

ПОСОЛ З ОСОБЛИВИХ ДОРУЧЕНЬ З ПИТАНЬ КІБЕРПРОСТОРУ ТА ЦИФРОВОЇ ПОЛІТИКИ НЕЙТ ФІК ПРОВІВ ПЕРШУ ПРЕСКОНФЕРЕНЦІЮ

6 жовтня Посол з особливих доручень з питань кіберпростору та цифрової політики Нейт Фік виступив перед журналістами. Серед іншого він заявив, що на сьогодні не спостерігається широкої ескалації з використанням кіберзасобів за межами України з боку росіян. Він висловив думку, що причиною цьому є єдність членів НАТО у протистоянні рф та ефективне кіберстримування. Здатність України протистояти російським кібератакам Фік пояснив ефективною комунікацією між виробниками програмного забезпечення, постачальниками обладнання, урядом США, урядом України та НАТО. Фік є першим посадовцем, який обіймає цей новостворений пост в Державному департаменті США. Він склав присягу 4 жовтня.

США ПРИЙНЯЛИ НОВУ СТРАТЕГІЮ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

12 жовтня США оприлюднили нову Стратегію національної безпеки. Серед іншого, документ містить невеликий розділ, присвячений питанням кібербезпеки. Згадавши заходи, які США вже вживають у цій сфері, автори документа визначають такі інтереси та завдання: «Як відкрите суспільство Сполучені Штати однозначно зацікавлені у зміцненні норм, які пом'якшують кіберзагрози та підвищують стабільність у кіберпросторі. Ми прагнемо стримувати кібератаки з боку державних і недержавних суб'єктів і будемо рішуче відповідати усіма відповідними державними інструментами на ворожі дії в кіберпросторі, включно з тими, які порушують життєво важливі функції держави або шкодять критичній інфраструктурі. Ми продовжуватимемо заохочувати дотримання схвалених Генеральною Асамблеєю ООН принципів відповідальної поведінки держав у кіберпросторі, які визнають, що міжнародне право застосовується як онлайн, так і офлайн».

Напередодні Білий дім опублікував перелік заходів, які вживає адміністрація Байдена-Харріс у сфері кібербезпеки. Серед них: зміцнення безпеки критичної інфраструктури, протидія атакам вимагачів, співпраця з союзниками та партнерами з метою забезпечення безпечнішого кіберсередовища та інші.

CISA ВПРОВАДЖУЄ ДОДАТКОВІ ЗАХОДИ З БЕЗПЕКИ ФЕДЕРАЛЬНИХ МЕРЕЖ

3 жовтня CISA опублікувала Обов'язкову оперативну директиву (BOD) 23-01 «Покращення видимості активів і виявлення вразливостей у федеральних мережах», яка наказує федеральним цивільним агентствам краще обліковувати наявні активи в їх мережах. Це продовження політики попередження кібератак аналогічних кібератаці SolarWinds. Мета Директиви – встановити базові вимоги для всіх федеральних цивільних агенцій виконавчої влади (FCEB) щодо визначення активів і вразливостей у їхніх мережах і надання даних CISA через визначені проміжки часу. Директиви обов'язкова для державних установ та рекомендована і для приватного сектору.

УПРАВЛІННЯ НАЦІОНАЛЬНОГО КІБЕРДИРЕКТОРА (ONCD) США РОЗРОБЛЯЄ НАЦІОНАЛЬНУ СТРАТЕГІЮ ЩОДО РОЗВИТКУ РОБОЧОЇ СИЛИ В КІБЕРПРОСТОРІ

3 жовтня Управління національного кібердиректора США повідомило про те, що з липня 2022 року веде активну роботу з розробки Національної стратегії розвитку робочої сили, навчанні та освіті в кіберпросторі, а також цифровій обізнаності. Ця стратегія має на меті розв'язати проблему нестачі близько 700 000 кіберфахівців, яких потребує США для забезпечення власної кібербезпеки. У жовтні Управління звернулось до всіх зацікавлених сторін щодо надання пропозицій (за запропонованою схемою) до цієї стратегії.

НАЦІОНАЛЬНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ ВЕЛИКОБРИТАНІЇ ВИПУСТИВ НАСТАНОВИ З БЕЗПЕКИ ЛАНЦЮЖКІВ ПОСТАЧАННЯ ДЛЯ СЕРЕДНІХ ТА ВЕЛИКИХ ПІДПРИЄМСТВ

20 жовтня Національний центр кібербезпеки (NCSC) Великобританії спільно з приватним сектором підготував та оприлюднив настанови (керівництво) для середніх та великих компаній приватного сектору, які мають складну структуру постачальників IT-послуг. Документ описує типові відносини з постачальниками та способи, за допомогою яких організації піддаються вразливості та кібератакам через ланцюг постачання. Крім того, він визначає основні кроки, які допоможуть організаціям оцінити наявний підхід до ланцюга постачання. Поява документа стала результатом опитування уряду Великої Британії щодо порушень безпеки за 2022 рік. Відповідно до нього, більша частина великих і малих компаній передають IT та кібербезпеку третім сторонам. Проте лише 13% компаній оцінили ризики, пов'язані з постачальниками.

ФРАНЦІЯ ЗАНЕПОКОЄНА ФІЗИЧНОЮ БЕЗПЕКОЮ ПІДВОДНИХ ІНТЕРНЕТ-КАБЕЛІВ

У статті від 13 жовтня видання Politico досліджує зусилля Франції щодо убезпечення підводних кабелів, що забезпечують інтернет-зв'язок між континентами (Франція є головною точкою входу в Інтернет у континентальній Європі – до її берегів підходить 30 кабелів). Диверсії проти «Північного потоку» підсилили ці страхи та призвели до низки кроків з боку французького уряду. У бюджеті Франції на 2023 рік закладено 3,1 млн євро на захист підводної інфраструктури. Також Париж вже інвестував 11 млн євро в придбання двох безпілотних підводних апаратів для захисту інфраструктури (вони почнуть працювати на початку наступного року).

УРЯД СИНГАПУРУ ПОСИЛЮЄ ПОЛІТИКУ КІБЕРБЕЗПЕКИ ТА ПЛАНУЄ ДЕЛЕГУВАТИ БІЛЬШЕ ОБОВ'ЯЗКІВ З КІБЕРБЕЗПЕКИ САМИМ КОРИСТУВАЧАМ

Під час свого виступу 18 жовтня на конференції, міністр-координатор з питань національної безпеки Сінгапуру Тео Чі Хеан озвучив нові пріоритети політики кібербезпеки Сінгапуру. Вони включають п'ять напрямків: посилення навичок кібергігієни громадян, встановлення вимог щодо дотримання кращих практик кіберзахисту основними суб'єктами електронної комерції, захист критичної інформаційної інфраструктури, протидія вірусам-вимагачам та посилення міжнародної співпраці.

ДЕПУТАТИ ЄВРОПАРЛАМЕНТУ ЗВЕРНУЛИСЬ ДО АЕРОПОРТУ СТРАСБУРГУ З ПРОХАННЯМ СКАСУВАТИ КОНТРАКТ З КИТАЙСЬКОЮ КОМПАНІЄЮ

10 жовтня троє депутатів Європарламенту звернулись до адміністрації аеропорту Страсбург з пропозицією скасувати нещодавно підписаний контракт на постачання обладнання для сканування багажу, виготовленого китайською компанією Nuctech. Вказана компанія частково належить владі КНР та просуває технології, що пов'язані з аерокосмічною галуззю. У 2020 році компанія була внесена до чорного списку Бюро промисловості та безпеки США.

Водночас обладнання Nuctech було перевірено та схвалено французьким авіаційним органом DGAC. Депутатів непокоїть впровадження підконтрольних Китаю технологій в місті, яке є офіційною резиденцією Європейського парламенту, а також Ради Європи та Європейського суду з прав людини.

КЕРІВНИКА СЛУЖБИ КІБЕРБЕЗПЕКИ НІМЕЧЧИНИ ЗВІЛЬНЕНО ЧЕРЕЗ ЙМОВІРНІ ЗВ'ЯЗКИ З РОСІЄЮ

Міністр внутрішніх справ Німеччини Ненсі Фейзер 18 жовтня звільнила главу відділу кібербезпеки Арне Шенбома через повідомлення, що він має зв'язки з людьми, причетними до російської розвідки. Занепокоєння Фейзер щодо Шенбома, який шість років очолював Федеральне відомство з інформаційної безпеки, виникло через його постійні контакти з організацією під назвою Рада кібербезпеки Німеччини.

Понад десять років тому Шенбом допоміг створити цю організацію, яка об'єднує експертів з державних установ і приватного сектору. Але після російського вторгнення в Україну Рада зазнала критики через повідомлення, що один із її членів пов'язаний із Кремлем.

2. МІЖНАРОДНА ТА МІЖДЕРЖАВНА ВЗАЄМОДІЯ В КІБЕРПРОСТОРІ

НА ПОСАДУ ГОЛОВИ МІЖНАРОДНОГО СОЮЗУ ЕЛЕКТРОЗВ'ЯЗКУ ОБРАНО ПРЕДСТАВНИЦЮ США

Під час Повноважної конференції Міжнародного союзу електрозв'язку (МСЕ), що відбулась в Бухаресті наприкінці вересня, 139 країн підтримали обрання американки Дорін Богдан-Мартін на посаду голови МСЕ. Вона обійматиме цю посаду протягом наступних чотирьох років. За її опонента росіянина Рашида Ісмаїлова свої голоси віддали 25 країн.

Зазначаючи свої пріоритети на посаді, пані Богдан-Мартін заявила, що необхідно багато зробити: від протидії зловмисній кіберактивності та підвищення стійкості до сприяння інвестиціям у захищену телекомунікаційну інфраструктуру та забезпечення загального доступу до Інтернету у такий спосіб, щоб просувати права людини. Результати виборів Голови МСЕ вважаються важливими з точки зору бачення напрямків подальшого розвитку мережі Інтернет.

ПРЕЗИДЕНТ БАЙДЕН ПІДПИСАВ ВИКОНАВЧИЙ УКАЗ ПРО ВПРОВАДЖЕННЯ РАМКОВОГО ПІДХОДУ ДО КОНФІДЕНЦІЙНОСТІ ДАНИХ МІЖ ЄС І США

7 жовтня Президент Байден підписав виконавчий наказ, яким запроваджується Рамковий підхід до конфіденційності даних між ЄС та США. Виконавчий наказ посилює і без того суворий набір обмежень щодо порушення конфіденційності та громадянських свобод з боку радіотехнічної розвідки США.
Про домовленість щодо розробки такого підходу президент Байден і президент Європейської комісії Фон дер Ляєн оголосили у березні 2022 року. Указ має розблокувати трансатлантичний обмін даними та зняти застереження, які було висловлено Європейським судом щодо попередньої угоди під назвою EU-U.S. Privacy Shield framework.

НАБУВ ЧИННОСТІ ДОГОВІР МІЖ США ТА ВЕЛИКОЮ БРИТАНІЄЮ ЩОДО ДОСТУПУ ДО ЕЛЕКТРОННИХ ДАНИХ

3 жовтня набув чинності договір між США та Великою Британією щодо Доступу до електронних даних з метою запобігання тяжким злочинам. Він стане першою угодою такого роду, яка дозволить слідчим кожної з країн отримати кращий доступ до життєво важливих даних для боротьби з серйозними злочинами відповідно до стандартів щодо конфіденційності та захисту громадянських свобод.
Згідно з Угодою, постачальники послуг в одній країні можуть відповідати на вимоги та законні запити щодо електронних даних, видані іншою країною, при цьому не боятись порушити обмеження на транскордонне розкриття інформації.

АЛБАНІЯ РОЗГЛЯДАЛА МОЖЛИВІСТЬ ЗАСТОСУВАННЯ СТАТТІ 5 ДОГОВОРУ НАТО ЧЕРЕЗ КІБЕРАТАКУ ІРАНУ

За словами Прем'єр-міністра Албанії Еді Рами, його країна зазнала настільки нищівної кібератаки з боку Ірану цього року, що його уряд навіть розглядав можливість застосування статті 5 договору НАТО, в якій йдеться, що атака на одну країну є атакою на всі країни альянсу. І хоча тої межі, після якої має відбутися колективна відповідь членів НАТО на кібератаку на сьогодні ще не визначено, Рама вважає, що атака на Албанію була дуже близькою до неї. Зрештою, було прийнято рішення уникнути ескалації та не антагонізувати впливових членів Альянсу.

США ЗРОБИЛИ НАСТУПНИЙ КРОК У ПРОЦЕСІ ФОРМУВАННЯ ТРАНСАТЛАНТИЧНИХ ПРАВИЛ ЩОДО ШТУЧНОГО ІНТЕЛЕКТУ

4 жовтня Білий дім опублікував Проект Біллю про права для штучного інтелекту. Документ містить принципи на яких, на думку адміністрації, має базуватися штучний інтелект (AI) та довідник «Від принципів до практики», що включає детальні кроки реалізації цих принципів у процесі технологічного проектування.

Тепер лідери США та ЄС зможуть порівняти та узгодити свої підходи до AI на наступній зустрічі Ради ЄС–США з торгівлі та технологій, яка відбудеться на початку грудня. Її результатом має стати «спільна дорожня карта щодо інструментів оцінки та вимірювання AI для надійного AI та управління ризиками», – йдеться в документі, опублікованому POLITICO. Європейська комісія запропонувала своє бачення наприкінці вересня у Директиві про відповідальність у сфері AI.

США УСКЛАДНЮЮТЬ КИТАЮ ДОСТУП ДО ЧІПІВ

7 Жовтня Білий дім опублікував давно очікувані експортні правила, мета яких перекрити доступ Китаю до передових чіпів, а також до засобів виробництва чіпів попередніх поколінь. Представники адміністрації заявили, що хочуть заблокувати доступ Народно-визвольної армії та внутрішнього апарату спостереження Китаю до передових можливостей у сфері комп'ютерних технологій, які вимагають використання передових напівпровідників.

Багато років тому Китай прийняв доктрину цивільно-військового злиття, яка фактично дозволяє передавати будь-яку технологію в Китаї на військові потреби. В результаті, чіпи, інструменти та програмне забезпечення, які є необхідними для виробництва предметів цивільного використання – від телефонів до самопілотованих автомобілів – допомагають Китайській військовій промисловості, зокрема сприяють розробці зброї масового знищення. США запровадили ці заходи в односторонньому порядку і на сьогодні ведуть перемовини з партнерами, щоб переконати їх приєднатися до своєї ініціативи, яка становить різку зміну у політиці США відносно продажу технологій до Китаю.

ВІДБУВСЯ TALLINN DIGITAL SUMMIT

10-11 жовтня у Таллінні відбувся Tallinn Digital Summit, основною темою якого стала trusted connectivity, або мережеві зв'язки, базовані на довірі. Талліннський форум – це щорічний захід, організований Прем'єр-міністром Естонії, який збирає однодумців і лідерів цифрових країн, міжнародних організацій і приватного сектору для вирішення найнагальніших проблем на шляху до пов'язаного цифрового майбутнього. До саміту Атлантична рада підготувала аналітичний звіт щодо trusted connectivity та шляхів її досягнення.

У СИНГАПУРІ ПРОЙШЛА МІЖНАРОДНА КОНФЕРЕНЦІЯ ВИСОКОГО РІВНЯ З ПИТАНЬ КІБЕРБЕЗПЕКИ

З 18 по 20 жовтня у Сингапурі відбувся захід високого рівня Singapore International Cyber Week 2022. У заходах взяли участь представники багатьох країн (в т.ч. рф) – представником України був Заступник Голови ДССЗЗІ Віктор Жора. Під час круглого столу 19 жовтня представник країни-агресора наголошував на важливості «міжнародної співпраці» і що росію несправедливо звинувачують у численних кібератаках не маючи достатніх для того доказів. Він відстоював думку, що це спрямовані зусилля США для дискредитації рф та її зусиль у міжнародних організаціях (таких як ООН). Представник США в межах іншого круглого столу підкреслив наявність довгострокових загроз для тих держав, які покладаються на китайське високотехнологічне обладнання або планують використовувати підводні кабелі, прокладені КНР.

3. ЗЛОВМИСНА АКТИВНІСТЬ: ОЦІНКИ, ЗАГРОЗИ, МЕТОДИ ПРОТИДІЇ

ІНЦИДЕНТ КІБЕРБЕЗПЕКИ З АВСТРАЛІЙСЬКОЮ СТРАХОВОЮ ФІРМОЮ MEDIBANK

13 жовтня австралійська страхова компанія медичного спрямування Medibank заявила, що була змушена перевести деякі свої системи в автономний режим через незвичну активність в її внутрішніх мережах. Деталі активності не розкривались. Компанія заявила, що немає наразі ніяких підтверджень, що персональні дані користувачів були скомпрометовані чи вкрадені. Компанія є однією з найбільших в Австралії – кількість клієнтів сягає 3,7 млн осіб.

ФБР ПОПЕРЕДЖАЄ ПРО ОПЕРАЦІЇ ЗЛАМУ ТА ВИТОКУ ІНФОРМАЦІЇ З БОКУ ІРАНСЬКОЇ КІБЕРГРУПИ

20 жовтня ФБР опублікувало попередження про активність іранського кіберугрупування Emennet Pasargad. Ця група тісно пов'язана з іранським урядом і здебільшого орієнтована на цілі, які пов'язані з Ізраїлем. Водночас вони активізували свою діяльність і проти США.

Група відома тим, що досліджує свої цілі перед атакою, головним чином націлюючись на вебсайти, на яких працює PHP-код або які мають зовнішні доступні бази даних MySQL, використовує інструменти тестування на проникнення з відкритим кодом. Вкрадені дані поширюються через власні спеціалізовані вебсайти, Telegram і на форумах кіберзлочинців. Часто використовують новинні організації для посилення інформаційного тиску на жертви. Матеріал ФБР містить опис тактик, прийомів і процедур (TTP), пов'язаних з Emennet, а також рекомендації для організацій щодо зменшення ризику, пов'язаного з групою.

ХАКЕРИ СУТТЄВО УДОСКОНАЛЮЮТЬ СТАРЕ ШКІДЛИВЕ ПЗ ПОВНІСТЮ ЗМІНЮЮЧИ ЙОГО ПРИЗНАЧЕННЯ – MANDIANT

Фахівці кібербезпекової компанії Mandiant відмічають тенденцію зростання кількості випадків, коли зловмисники істотно доопрацьовують старе шкідливе ПЗ при цьому повністю змінюючи його призначення. Як приклад наводиться вірус Ursnif, який вперше було застосовано ще у 2006 році, та чиїм основним призначенням була крадіжка банківських даних. Однак тепер на базі нього було створено новий вірус – LDR4 який використовується в атаках вірусів-вимагачів.

РОСІЙСЬКІ ХАКЕРИ АТАКУВАЛИ САЙТИ БОЛГАРСЬКОЇ ВЛАДИ

18 жовтня DDoS-атака на певний час паралізувала роботу онлайн представництва президентського офісу, Міністерства оборони, Міністерства внутрішніх справ, Міністерства юстиції та Конституційного суду Болгарії. Доступ до сайтів було відновлено відносно швидко, але ще протягом деякого часу вони працювали із затримками.
Відповідальність за напад взяло на себе російське хакерське угруповання KillNet, яке заявило, що атака є покаранням «за зраду росії та постачання зброї Україні». Про атаку угруповання повідомило на своєму Telegram-каналі. Болгарська влада заявила, що їй вдалось встановити особу одного з нападників. Він проживає у місті Магнітогорськ рф. У прокуратурі Болгарії заявили, що до рф буде направлено прохання про екстрадицію, хоча надія на те, що його буде екстрадовано, доволі невисока.

NSA, CISA ТА FBI РОЗКРИВАЮТЬ НАЙПОПУЛЯРНІШІ CVE, ЯКІ ВИКОРИСТОВУЮТЬ СПОНСОРОВАНІ КИТАЄМ ХАКЕРСЬКІ ГРУПИ

6 жовтня три відомства оприлюднили огляд найбільш популярних CVE (всі – вже раніше відомі) до яких найчастіше вдаються хакерські групи, які безпекові органи США вважають пов'язаними із китайським урядом. З вказаних 20 вразливостей 16 є критичними і дуже небезпечними. Всі урядові агенції мають вжити запропоновані в документі заходи для зменшення ризиків їх кібербезпеці.

NSA, CISA ТА FBI ОПУБЛІКУВАЛИ РЕЗУЛЬТАТИ СПІЛЬНОГО РОЗСЛІДУВАННЯ КІБЕРАТАКИ НА ПІДПРИЄМСТВА ОБОРОННОГО КОМПЛЕКСУ У СІЧНІ 2022 РОКУ

4 жовтня всі три організації опублікували результати спільного розслідування серії кібератак в період з листопада 2021 року по січень 2022 року проти низки організацій, що належать до оборонно-промислового комплексу. Метою зловмисників була крадіжка чутливої інформації. Особливістю кібератак було використання зловмисниками набору відкритих інструментів Impacket. Оприлюднені результати висвітлюють основні техніки зловмисників та дають рекомендації щодо уникнення таких атак у майбутньому.

KILLNET АТАКУВАЛИ САЙТИ 14 АМЕРИКАНСЬКИХ АЕРОПОРТІВ

10 жовтня хакерське об'єднання Killnet атакувало сайти 14 найбільших американських аеропортів. За оприлюдненими даними атака обмежилась виключно DDoS-сайтів цих установ. Помітних наслідків для аеропортів ці атаки не мали, хоча користувачі певний час не могли отримувати актуальну інформацію про прибуття чи відбуття літаків.
Розслідування інциденту займається FBI та CISA. Хоча не повідомлялось про інші можливі наслідки цієї кібератаки (наприклад як маскування для іншого типу атаки), окремі американські сенатори забажали від FBI та CISA більш докладної інформації про інцидент.

ДОСЛІДНИЦЬКА КОМАНДА REASONLABS РОЗКРИЛА ГЛОБАЛЬНЕ БАГАТОМІЛЬЙОННЕ ШАХРАЙСТВО З КРЕДИТНИМИ КАРТКАМИ ОНЛАЙН

Дослідники компанії ReasonLabs розкрили схему, за якою зловмисники створили мережу фейкових сайтів для дорослих. Вони купили інформацію щодо викрадених кредитних карток у dark web та знімали невеликі щомісячні платежі, як плату за підписку на ці сайти. Дослідники зазначають, що ця глобальна схема шахрайства з кредитними картками працює з 2019 року, і вже стала інструментом для отримання десятків мільйонів доларів від десятків тисяч сімей і окремих осіб. Дослідники знайшли докази того, що кримінальний синдикат, який стоїть за цією мережею, має російське походження.

ПІВНІЧНОКОРЕЙСЬКІ ХАКЕРИ ВИКОРИСТОВУЮТЬ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ З ВІДКРИТИМ ВИХІДНИМ КОДОМ ДЛЯ КІБЕРАТАК

Групи аналізу загроз Microsoft разом із LinkedIn Threat Prevention and Defense повідомляють, що «дуже оперативна, деструктивна та вправна група», пов'язана з Північною Кореєю, використовує програмне забезпечення з відкритим кодом у кампаніях соціальної інженерії проти співробітників організацій у багатьох галузях, включаючи медіа, оборону та аерокосмічну промисловість, а також IT-послуги в США, Великобританії, Індії та Росії.

Дослідники з великою долею вірогідності атрибутували ці атаки угрупованню Zinc, пов'язаному з Lazarus, яке також відстежується під назвою Labyrinth Chollima. З детальним описом операції можна ознайомитися за лінком.

ПОПЕРЕДЖЕННЯ: У ЛОГОТИПІ MICROSOFT ПРИХОВАНО ШПИГУНСЬКЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Дослідники Symantec повідомили, що спостерігають за шпигунським угрупуванням Witchetty (воно ж LookingFrog), яке поступово оновлює набір інструментів. Воно використовує нове шкідливе програмне забезпечення для атак на Близькому Сході та в Африці. Серед нових інструментів групи є бекдор-троян (Backdoor.Stegmap), який використовує малопоширену стеганографічну техніку, коли зловмисний код ховається в зображенні. Серед зображень, які були використані угрупуванням останнім часом – старий логотип Microsoft.

ЗЛОЧИНЦІ КОРИСТУЮТЬСЯ ЗЛОВМИСНИМИ ФАЙЛОВИМИ ЗАСТОСУНКАМИ У ФОРМАТІ HTML

Дослідники з Trustwave SpiderLabs протягом останнього місяця помітили зростання шкідливих вкладень HTML у фішингових електронних листах. Більшість цих вкладень відкриває фішингову сторінку для викрадення облікових даних користувачів, яка видає себе за портал входу. Дослідники відзначають, що деякі з цих файлів вводять адресу електронної пошти користувача у поле входу на фішинговій сторінці, щоб створити враження, що користувач вже здійснював вхід у систему. Зловмисники також використовують техніку HTML smuggling, щоб уникнути виявлення фільтрами безпеки електронної пошти.

FACEBOOK ВИЯВИВ 400 ПРОГРАМ ДЛЯ ANDROID ТА IOS, ЯКІ КРАДУТЬ ОБЛІКОВІ ДАНІ КОРИСТУВАЧІВ

7 жовтня Meta Platforms повідомила, що виявила понад 400 шкідливих програм для Android та iOS, які, за її словами, були націлені на онлайн-користувачів з метою викрадення їхніх даних для входу в Facebook.

42,6% зловмисних додатків були редакторами фотографій, за ними йшли бізнес-утиліти (15,4%), телефонні утиліти (14,1%), ігри (11,7%), VPN (11,7%) і програми для стилю життя (4,4%). Цікаво, що більшість додатків для iOS представлялися інструментами керування рекламою для Meta та її дочірньої компанії Facebook. Окрім приховування шкідливої природи як набору, на перший погляд, нешкідливих програм, оператори схеми також публікували підроблені відгуки, які були розроблені, щоб компенсувати негативні відгуки користувачів, які раніше завантажували програми.

LOFYGANG РОЗПОВСЮДИЛА МАЙЖЕ 200 ШКІДЛИВИХ ПАКЕТІВ NPM ДЛЯ ВИКРАДЕННЯ ДАНИХ КРЕДИТНИХ КАРТОК

7 жовтня дослідники компанії Checkmarks повідомили, що вони виявили майже 200 шкідливих пакетів NPM із тисячами інсталяцій, пов'язаних із групою «LofyGang». Ця група діє понад рік та націлена на викрадення інформації про кредитні картки, оновлення Discord «Nitro», облікові записи потокових служб (наприклад, Disney+), облікові записи Minecraft тощо. Надалі вони продають вкрадену інформацію. Більше деталей у звіті Checkmarks.

ХАКЕРИ ВКРАЛИ ЩОНАЙМЕНШЕ 100 МІЛЬЙОНІВ ДОЛАРІВ ІЗ БЛОКЧЕЙНУ, ПОВ'ЯЗАНОГО З BINANCE

6 жовтня найбільша у світі криптовалютна біржа Binance втратила щонайменше 100 мільйонів доларів через хакерську атаку. За словами генерального директора Binance Чанпена Чжао, хакери скористалися вразливістю в BSC Token Hub, мосту, який полегшує передачу активів між двома блокчейнами Binance – BNB Beacon Chain та BNB Smart Chain. Експлойт у BSC Token Hub дозволив хакерам виробити два мільйони цифрових токенів Binance вартістю приблизно 570 мільйонів доларів. В інтерв'ю CNBC Чжао сказав, що жоден користувач не втратив свої гроші, оскільки хакери намагалися викачати лише ці додаткові токени.

ЕВОЛЮЦІЯ ТАКТИКИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ BAZARCALL

У звіті, опублікованому 6 жовтня, дослідники компанії Trellix описали еволюцію підходів кампанії BazarCall. Її особливістю є те, що вона користується не шкідливими посиланнями або вкладеннями в імейлах, а телефонними дзвінками. Користувача оманою заохочують набрати номер нібито технічної підтримки. Після цього його з'єднують з реальними людьми на іншому кінці, які потім надають покрокові інструкції щодо встановлення шкідливого програмного забезпечення на свої пристрої.

BUDWORM: ШПИГУНСЬКА ГРУПА ЗНОВ ТАРГЕТУЄ ОРГАНІЗАЦІЇ В США

13 жовтня компанія Symantec повідомила, що за її спостереженнями протягом останніх шести місяців шпигунська група Budworm здійснила атаки на низку стратегічно важливих цілей, зокрема на уряд однієї з країн Близького Сходу, багатонаціонального виробника електроніки та законодавчий орган штату США. Остання атака є першим випадком за кілька років, коли Symantec спостерігає інтерес з боку Budworm до американської організації. Разом із зазначеними вище цілями високого рівня група також здійснила атаку на лікарню в Південно-Східній Азії.

ЗАСТЕРЕЖЕННЯ ДЛЯ КОРИСТУВАЧІВ WHATSAPP: НЕБЕЗПЕЧНИЙ МОБІЛЬНИЙ ТРОЯН РОЗПОВСЮДЖУЄТЬСЯ ЧЕРЕЗ ШКІДЛИВУ МОДИФІКАЦІЮ МЕСЕНДЖЕРА

Дослідники Kasperskiy Lab виявили зловмисну групу, яка розповсюджує мобільний троян, який викрадає дані через підроблену версію WhatsApp. В результаті встановлення цієї неофіційної модифікації відомого месенджера з неофіційних джерел, користувачі ризикують викраденням їх облікових даних у месенджері WhatsApp.

4. ТЕНДЕНЦІЇ ТА ПРОГНОЗИ

UBER ВИЗНАЛИ ВИННИМ У ПРИХОВУВАННІ ІНФОРМАЦІЇ ПРО ЗЛАМ КАМПАНІЇ У 2016 РОЦІ

Збільшились випадки притягнення до відповідальності керівництва приватних компаній за неповідомлення про виток персональних даних громадян. 7 жовтня стало відомо про те, що екс-керівник служби інформаційної безпеки Uber Джо Саліван був визнаний винним у приховуванні інформації про витік персональних даних 57 мільйонів користувачів сервісу у 2016 році. Предметом обвинувачення стало те, що у 2016 році він вже допомагав Федеральній торговій комісії США (FTC) розслідувати інший витік даних в компанії у 2014 році та знаходився під присягою. Однак він не просто не повідомив про новий витік, але і намагався його приховати заплативши хакерам викуп (100 тисяч доларів) під виглядом винагороди за пошук вразливостей і спробувавши підписати з ними угоду про нерозголошення (NDA).

ENISA ОПУБЛІКУВАЛА НОВИЙ ЗВІТ ПРО ПРОБЛЕМУ ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ

19 жовтня було оприлюднено результати дослідження «Постквантова криптографія: інтегроване дослідження». Основна мета дослідження – оцінити можливості інтеграції постквантових алгоритмів в чинні протоколи, які зміни несуть постквантові алгоритми в поточні протоколи шифрування.

Автори дослідження підтверджують занепокоєння, що створення квантового комп'ютера може істотно змінити правил гри у сфері алгоритмів та шифрування. При цьому вони підкреслюють, що найімовірніше той, хто першим зробить функціональний квантовий комп'ютер, зробить це таємно і максимально довго не розкриватиме цю таємницю. Вони пропонують низку напрямків для подальших дискусій, які вважають перспективними у сфері практичного опрацювання теми квантової криптографії.

ENISA ПРОВЕЛА СЬОМУ ЩОРІЧНУ КОНФЕРЕНЦІЮ З Е-ЗДОРОВ'Я: У ФОКУСІ УВАГИ – КІБЕРЕЗПЕКА

10 жовтня Європейська агенція з кібербезпеки (ENISA) провела щорічну конференцію з питань розвитку електронної охорони здоров'я. Фокусом цьогорічного заходу стала зміна ландшафту кіберзагроз та його вплив на медичну сферу. Зокрема, констатували еволюцію атак програм-вимагачів і проблеми з кібербезпекою ланцюжків постачання. Про це свідчать інциденти, зареєстровані відповідно до директиви NIS для сектору охорони здоров'я у 2021 році. Зокрема, для 14% цих інцидентів, основна причина пов'язана з програмами-вимагачами.

КОРПОРАЦІЯ RAND ВВАЖАЄ, ЩО АМЕРИКАНСЬКОМУ УРЯДУ ТРЕБА ПОСИЛИТИ ЗАХОДИ ЩОДО ПІДГОТОВКИ ДО ПОСТКВАНТОВОГО СВІТУ

6 жовтня фахівець Корпорації RAND Майкл Вермєр оприлюднив огляд політики США щодо дій Уряду США для забезпечення національної безпеки у постквантовому світі. На його думку, американський уряд розпочав правильну комплексну кампанію щодо такої підготовки і вона охоплює всі основні складові. Це розробки відповідних стандартів зусиллями NIST, створення DHS інструкції для об'єктів критичної інфраструктури щодо підготовки до міграції на постквантову криптографію, активне включення в цей процес NSA USA.

Але він зазначає, що цих зусиль може бути недостатньо: треба більше ресурсів вкладати як в створення стандартів, так і практичну адаптацію цивільних урядових агентств до нової реальності. А також оцінити загрози від потенційної можливості зловмисників та розшифрувати за допомогою квантових систем раніше вкрадені матеріали.

ПСИХОЛОГІЧНЕ ВИГОРАННЯ СТАВИТЬ ПІД ЗАГРОЗУ ПИТАННЯ ФУНКЦІОНАЛЬНОСТІ SOC ПО ВСЬОМУ СВІТУ

12 жовтня фахівці SANS, спираючись на результати досліджень, оприлюднили матеріал щодо проблеми комплектування SOC у всьому світі. Ця проблема пов'язана зі складними та динамічними умовами роботи в таких центрах. За даними опитування Devo SOC 55% респондентів кажуть, що вони розглядали можливість піти з роботи через тиск, який вони відчувають. Середній же час пошуку нового фахівця займає від 7 місяців до 2 років. SANS звертає увагу на необхідність вжиття превентивних заходів, які б зменшили навантаження на таких фахівців.

22 УРЯДОВІ ІНІЦІАТИВИ З КІБЕРБЕЗПЕКИ 2022 РОКУ, ЯКІ ВАРТІ УВАГИ

Аналітичне видання CSO опублікувало огляд державних ініціатив у сфері кібербезпеки. До огляду увійшли пропозиції та рішення держав з усього світу, запроваджені як на національному, так і на місцевому рівнях. Автори огляду виділили 22 важливі урядові ініціативи, спрямовані на вирішення різноманітних проблем безпеки. Серед них програма Сингапуру з кібербезпекової сертифікації для визнання належної практики безпеки, пропозиція Великої Британії щодо нового кодексу практики для підвищення безпеки та конфіденційності програм, ізраїльський проект Cyber-Dome та інші.

НЕГАТИВНА МНОЖИННІСТЬ: ПРОГНОЗИ ЩОДО МАЙБУТНЬОГО ВПЛИВУ НОВИХ ТЕХНОЛОГІЙ НА МІЖНАРОДНУ СТАБІЛЬНІСТЬ ТА БЕЗПЕКУ ЛЮДИНИ

Інститут дослідження миру та безпекової політики при Гамбурзькому університеті опублікував дослідження щодо впливу 12 нових технологій на міжнародну стабільність та безпеку людини, базоване на опитуванні 30 міжнародних експертів. Занепокоєння дослідників викликає військове застосування нового покоління технологій.

Автори звіту шукали відповіді на наступні запитання: Який вплив новітні технології матимуть на стабільність перегонів озброєнь, стабільність під час криз та гуманітарні принципи до 2040 року? Які новітні технології демонструють схожість з точки зору впливу? Коли вплив цих технологій стане найгострішим?

Серед іншого, дослідники дійшли висновку, що усі дванадцять технологій послаблять або міжнародну стабільність, або безпеку людини, а половина розглянутих технологій переважно послабить (а не посилить) як стабільність, так і безпеку людини. Адже вплив усіх технологій був негативним. Детальний звіт про дослідження можна знайти за посиланням.

АНАЛІЗ ЛАНДШАФТУ КІБЕРЗАГРОЗ ВІД SECUREWORKS COUNTER THREAT UNIT

4 жовтня компанія Secureworks опублікувала аналіз кіберзагроз. За словами її головного дослідника загроз Баррі Хенслі, програми-вимагачі залишаються найпоширенішою загрозою для бізнесу, але прослідковуються помітні зміни в поведінці суб'єктів загрози та їхньому підході до кампаній. І хоча можна стверджувати, що рансомвер як послуга втрачає популярність, дослідження Secureworks чітко показує зростання кількості використання викрадачів інформації та еволюцію інструментів і противників. Загроза змінюється, але не зникає.

КОМПАНІЯ FORTINET ДОСЛІДИЛА НАЙБІЛЬШ ВИКОРИСТОВУВАНІ СПОСОБИ ДОСТАВЛЕННЯ ЗЛОВМИСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДО КОРИСТУВАЧІВ

У звіті, опублікованому 4 жовтня, компанія Fortinet дійшла висновку, що станом на початок другої половини 2022 року, фішингові атаки та компанії, які використовують різні методи зараження користувачів і організацій, продовжують залишатися головними загрозами для організацій. Щоб допомогти організаціям краще виявляти та запобігати фішинговим кампаніям, компанія описала у своєму блозі деякі з найпоширеніших деталей і методів, які використовують шкідливі файли для розгортання зловмисного програмного забезпечення.

ЗЛОВЖИВАННЯ ПІД ЧАС COVID-19: ЯК ЗЛОВМИСНИКИ ВИКОРИСТОВУВАЛИ ПАНДЕМІЮ

Дослідники компанії Proofpoint опублікували звіт, в якому описали, як пандемія COVID-19 створила середовище, найбільш зручне для зловживань від початку ери кіберзлочинності. Ним скористалися всі зловмисні угрупування – від просунутих державних груп, великих та дрібних злочинців, до дрібних шахраїв та спамерів. Усі вони намагалися використовувати вміст, пов'язаний з COVID-19, у своїх зловмисних цілях.

По суті, страх, невизначеність і сумніви, які люди у всьому світі відчували під час пандемії COVID, створили умови, за яких підготовка та уважність не спрацювали. Це дало можливість зловмисникам використовувати людські вразливості. Зі звітом можна ознайомитися за посиланням.

ФАХІВЦІ З КІБЕРБЕЗПЕКИ ПІДІЙМАЮТЬ ПИТАННЯ «ТЕМНИХ ДАНИХ»

Згідно зі спеціальним випуском звіту DealMaker Meter щодо кібербезпеки «Розуміння ризику: темна сторона даних» від провідної компанії з вивчення ризиків Donnelley Financial Solutions (NYSE: DFIN), темні дані становлять найбільший потенційний ризик для кібербезпеки і комплаєнс компаній США та Великобританії.

У звіті темні дані визначаються як дані, які компанія зібрала, але більше не потребує (від застарілої інформації про клієнтів до старих даних щодо співробітників). Корпорації часто забувають і не захищають такі дані, створюючи значні обтяження, а також спокусливі цілі для кіберзлочинців.

ЗВІТ CLOUDFLARE ПРО ЗАГРОЗИ DDOS ЗА 3 КВАРТАЛ 2022 РОКУ

12 жовтня компанія Cloudflare опублікувала звіт про загрози DDoS атак, базований на спостереженні за її глобальною мережею. Компанія повідомляє, що багатотерабітні DDoS-атаки стають все більш поширеними. У третьому кварталі Cloudflare автоматично виявила і пом'якшила численні атаки, швидкість яких перевищувала 1 Тбіт/с.

Найбільшою була DDoS-атака зі швидкістю 2,5 Тбіт/с, запущена варіантом ботнету Mirai, спрямована на сервер Minecraft, Wynncraft. Загалом, протягом третього кварталу спостерігалися такі тенденції: збільшення кількості DDoS-атак порівняно з минулим роком, більш тривалі об'ємні атаки, різке зростання кількості атак, створених ботнетом Mirai та його варіантами, різке зростання кількості атак на Тайвань і Японію.

5. КРИТИЧНА ІНФРАСТРУКТУРА

CISA ПОПЕРЕДЖАЄ ПРО НОВІ ВРАЗЛИВОСТІ В НИЗЦІ СИСТЕМ, ЯКІ ВИКОРИСТОВУЮТЬСЯ В ІНДУСТРІАЛЬНИХ КОМПАНІЯХ

18 жовтня CISA повідомило про нові вразливості у промислових системах управління (ICS) і технологіях критичної інфраструктури. Це попередження стосується продуктів Advantech (продукт R-SeeNet використовується в енергетиці, водопостачанні та водовідведенні) та Hitachi Energy (продукт APM Edge).

КОМПАНІЯ TRUSTWAVE ПРОАНАЛІЗУВАЛА ОКРЕМІ ВИМОГИ АВСТРАЛІЙСЬКОГО ЗАКОНУ ПРО БЕЗПЕКУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Австралія продовжує реформування свого законодавства щодо захисту критичної інфраструктури. 3 жовтня фахівці компанії оприлюднили аналіз поточного законодавства в цій сфері, а також звернули увагу на деякі проблеми реалізації норм щодо оцінки ризиків для таких об'єктів у розрізі оцінки ризиків від кіберзагроз. Аналіз стосується низки положень законодавчого акту щодо якого немає роз'яснення держави в частині їх реалізації (щодо відповідності стандартам кібербезпеки чи порядку забезпечення ланцюжків постачання).

NIST ОПУБЛІКУВАВ ДЛЯ ПУБЛІЧНОГО ОБГОВОРЕННЯ ПРОЕКТ ЗВІТУ ЩОДО КІБЕРБЕЗПЕКИ ОРГАНІЗАЦІЙ ЗІ СФЕРИ ПРИРОДНОГО ЗРІДЖЕНОГО ГАЗУ

17 жовтня NIST оприлюднив проект міжвідомчого звіту, що має на меті допомогти створити профіль кібербезпеки для організацій, які залучені у сфері виробництва зрідженого газу. Підхід, що базується на іншому документі NIST – Cyber Security Framework – має допомогти організаціям у цій сфері розробити адекватні профілі кібербезпеки. Звіт надає конкретні етапи та процедури (в т.ч. теми семінарів, зустрічей), завдяки яким компанії можуть налаштувати NIST Cyber Security Framework для своїх потреб.

В ПРОМИСЛОВОМУ ІНСТРУМЕНТІ SIEMENS ВИЯВЛЕНА «КРИТИЧНА» ВРАЗЛИВІСТЬ, ЯКА ДОЗВОЛЯЄ ВИКРАДАТИ КРИПТОГРАФІЧНІ КЛЮЧІ

Компанія Siemens опублікувала патч для усунення вразливості в одному з її найпопулярніших програмованих логічних контролерів (ПЛК) – промислових комп'ютерах, які широко використовуються у виробництві та інших галузях промисловості. За інформацією дослідників з фірми Claroty, які виявили вразливість, ця помилка дозволяла зловмисникам отримувати доступ до «міцно захищених, жорстко закодованих, глобальних приватних криптографічних ключів», вбудованих в продукти Siemens. Вони, своєю чергою, можуть використовуватися зловмисниками «для кількох розширених атак на пристрої Siemens SIMATIC і пов'язаний TIA Portal, в обхід усіх чотирьох його рівнів захисту».

СИСТЕМИ SCADA ПОРТІВ І ТЕРМІНАЛІВ США ПІД ОСОБЛИВОЮ УВАГОЮ ЗЛОВМИСНИКІВ

Згідно з дослідженням кібербезпеки портів і терміналів за 2022 рік, проведеним юридичною фірмою Jones Walker, спостерігається значне зростання кількості кібератак, спрямованих на цей сектор. І хоча переважна більшість респондентів стверджують, що вони готові протистояти кіберзагрозам, багато хто підтвердив, що минулого року зазнали зломів.

На запитання про типи систем, залучених у витік даних, 36% назвали системи диспетчерського контролю та збору даних (SCADA), а 32% назвали системи керування польовими пристроями. Крім того, SCADA було названо найбільшою «вразливістю кібербезпеки» портів і терміналів США.

ДОСЛІДНИКИ РОЗРОБИЛИ АЛГОРИТМ, ЩО МОЖЕ ДОПОМОГТИ ЗАХИСТИТИ ЕНЕРГОСИСТЕМУ ВІД ВІРУСІВ ВИМАГАЧІВ

Дослідники Університету Пердью розробили алгоритм для прийняття рішень щодо інвестицій у кібербезпеку електричної мережі, який враховує особливості поведінки людини. Для створення такого алгоритму дослідники спочатку змоделювали інвестиційну поведінку осіб, що приймають рішення, і виявили, що люди, зазвичай, не дуже добре можуть передбачити, які активи є найуразливішими до потенційних атак. На їхню думку, застосування такого алгоритму допоможе убезпечити енергетичну систему від атак вірусів вимагачів, які стають все більш широко розповсюдженими та призводять до відключення електроенергії.

БІЛИЙ ДІМ ПЛАНУЄ ВСТАНОВИТИ НОВІ ПРАВИЛА КІБЕРБЕЗПЕКИ В ТРЬОХ СЕКТОРАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Зв'язок, водопостачання та охорона здоров'я є наступними секторами критично важливої інфраструктури, з якими адміністрація Байдена планує працювати для підвищення базової кібербезпеки. Про це 13 жовтня заявила заступниця радника Білого дому з національної безпеки Енн Нойбергер. Робота, яку проводитимуть у цій сфері різні федеральні відомства, є ще одним кроком адміністрації, спрямованим на усунення прогалин у безпеці критичної інфраструктури для посилення її захисту від хакерів. Це питання актуалізувалося після торішніх гучних атак програм-вимагачів, включаючи атаку на Colonial Pipeline, яка порушила постачання палива до Східного узбережжя США.

ПОВІТРЯНИЙ РУХ БІЛЯ ДАЛЛАСА БУЛО ПЕРЕНАПРАВЛЕНО, ОСКІЛЬКИ FAA ПОМІТИЛА НЕНАДІЙНИЙ СИГНАЛ GPS

18 жовтня рейси, що направлялися в район аеропорту міста Даллас, змушені були використовувати застарілі, ускладнені маршрути, а злітно-посадкова смуга в міжнародному аеропорту Даллас-Форт-Ворт була тимчасово закрита. Авіаційна адміністрація заявила, про ненадійність сигналу GPS у тому районі. Федеральна авіаційна адміністрація повідомила, що розслідує можливі перешкоди для роботи системи глобального позиціювання. На початковому етапі розслідування ознак навмисного втручання виявлено не було.

6. АНАЛІТИЧНІ ОЦІНКИ

СВІТУ ВСЕ ЩЕ НЕ ВИСТАЧАЄ 3,4 МІЛЬЙОНА ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

20 жовтня некомерційна асоціація сертифікованих кіберфахівців (ISC) оприлюднила результати свого дослідження щодо стану забезпеченості світу кіберфахівцями. Дослідження стало наслідком опрацювання відповідей 11 779 фахівців з кібербезпеки по всьому світу протягом травня-червня 2022 року.

Дослідження показує, що на поточний момент у світі є приблизно 4,7 мільйона кіберфахівців, до яких цього року додалось ще 464 тисячі. Серед результатів: 70% вважають, що їх організаціям не вистачає фахівців з кібербезпеки. 20% співробітників заявляють, що їх організація швидше за все збільшить свій бюджет на кібербезпеку у разі виявлених порушень, однак лише 16% заявляють, що цей збільшений бюджет вплине на залучення додаткового персоналу.

ЗБІР КІБЕРСТАТИСТИКИ ЗАЛИШАЄТЬСЯ НЕВИРІШЕНОЮ ПРОБЛЕМОЮ ДЛЯ США І ЦЕ УСКЛАДНЮЄ ПОБУДОВУ ЕФЕКТИВНОГО КІБЕРЗАХИСТУ

18 жовтня з'явилась аналітична стаття Дженіфер Шор щодо проблеми збору кіберстатистики в США. Вона вказує, що попри численні спроби уряду розпочати цей процес (в т.ч. запустивши Бюро кіберстатистики) прогрес все ще незначний. Відповідно і державні органи, і багато приватних організацій змушені будувати свою кібербезпеку «в сліпу».

Вона вказує, що навіть зараз є щонайменше 20 федеральних документів, які вимагають звітування про кіберінциденти, власні бази даних є у приватних компаній, страховиків та дослідників. І основне завдання уряду зараз – знайти шлях інтеграції цих даних аби отримати більше користі для всіх суб'єктів. А для цього потрібно більше інвестиції в аналіз, обмін і публічне оприлюднення даних і синтез їх з усіма іншими доступними даними про кібербезпеку.

NIST ОПУБЛІКУВАВ РІЧНИЙ ЗВІТ ПРО СВОЇ ДОСЛІДЖЕННЯ У СФЕРІ КІБЕРБЕЗПЕКИ У 2021 ФІСКАЛЬНОМУ РОЦІ

13 жовтня NIST оприлюднив комплексний звіт про всі свої здобутки у 2021 фіскальному році в питаннях кібербезпеки. В документі надається огляд діяльності організації за вісьмома ключовими сферами: стандарти криптографії та валідація, вимірювання кібербезпеки, освіта та робоча сила, управління ідентифікацією та доступом, побудова приватності, управління ризиками, надійні мережі, надійні платформи.

SBOM ДОЗВОЛИТЬ ЗНАЧНО ПІДВИЩИТИ КІБЕРБЕЗПЕКУ ОРГАНІЗАЦІЙ ЗА МЕНШІ КОШТИ – MITRE

13 жовтня Корпорація опублікувала своє дослідження «Переваги для кібербезпеки від використання» (SBOM – Software Bill Of Material). В ньому підкреслюється, що подальше впровадження SBOM дозволить автоматизовано ідентифікувати вразливі компоненти, які сприяють інцидентам безпеки, зменшувати незаплановану та непродуктивну роботу через заплутані ланцюги постачання. Автоматизація цих заходів економить кошти, оскільки дії виконуються за менший час і з меншою кількістю помилок.

ОБОВ'ЯЗКИ РОЗВІДУВАЛЬНИХ СЛУЖБ США ЩОДО РОЗКРИТТЯ ІНФОРМАЦІЇ ПРО ЗАГРОЗИ НЕДЕРЖАВНОМУ СЕКТОРУ МАЮТЬ БУТИ РОЗШИРЕНІ – RAND

У матеріалі від 20 жовтня дослідниця Корпорації RAND Кортні Вайнбаум звертає увагу на необхідність розширити обов'язки розвідувальних служб США в частині попередження громадськості про кібератаки. Вона посилається на відповідний обов'язок повідомляти громадян, якщо їх життю загрожує небезпека і пропонує доповнити відповідну Директиву розвідувальної спільноти 191 (яка за це відповідає) нормами про нефізичні загрози.

РОЗВИТОК КІБЕРБЕЗПЕКИ КІНЦЕВИХ ТОЧОК ЗАЛИШАЄТЬСЯ ПРІОРИТЕТОМ ДЛЯ БІЛЬШОСТІ КОМПАНІЙ В ПРОЦЕСІ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ – ОПИТУВАННЯ FOUNDRY 2022 SECURITY PRIORITIES

6 жовтня було поширено результати дослідження Foundry 2022 Security Priorities, що базується на результаті опитування 900 фахівців з кібербезпеки. Майже всі опитані стикаються з проблемами браку фахового персоналу, що стає критичним при зростанні кіберзагроз.

Водночас типового рішення реакції на цю проблему не існує: 45% IT-керівників збільшують обов'язки наявного персоналу, 45% використовують технології автоматизації, а 42% доручають окремі функції безпеки стороннім підрядникам. З точки зору визначення критичних точок докладання зусиль 51% респондентів сказали, що засоби захисту кінцевих точок для співробітників компаній є їх пріоритетом.

ПОЛІТИКА УРЯДУ США ЩОДО ПРОТИДІЇ ВІРУСАМ-ВИМАГАЧАМ ДАЄ РЕЗУЛЬТАТИ, АЛЕ НЕБЕЗПЕКИ НЕ ЗНИКАЮТЬ: ОЦІНКА ПОТОЧНИХ УРЯДОВИХ ІНІЦІАТИВ

Автором інтернет-ресурсу Security Intelligence підготовлено та оприлюднено огляд поточних зусиль Уряду США у протидії вірусам-вимагачам. Він аналізує ефективність санкційної політики щодо ініціаторів атак та зважає результативність підходу за якого держава визнає виплату викупу зловмисникам цивільним злочином.

Основний висновок: вжиті зусилля дають помітні результати (хоча загальна кількість атак не зменшується, але ціна одного викупу впала майже у два рази у порівнянні з минулим роком). Однак Уряд ще зіткнеться з проблемою, коли для деяких великих, системоутворюючих компаній виплата викупу буде єдиним способом відновлення діяльності.

АТЛАНТИЧНА РАДА ОПРИЛЮДНИЛА ЗВІТ ЩОДО БЕЗПЕКИ ПРИЛАДІВ В ІНТЕРНЕТІ РЕЧЕЙ

26 вересня дослідники Atlantic Council опублікували новий звіт із рекомендаціями для політиків щодо захисту пристроїв Інтернету речей. Зосереджуючись на пристроях Інтернету речей у підключених будинках, мережевому та телекомунікаційному секторі та медичних пристроях, звіт «Мільярдна безпека: на шляху до кращої стратегії безпеки екосистеми Інтернету речей» розглядає заходи для зменшення ризиків безпеки IoT, що їх вжили чотири країни: США, Великобританія, Сінгапур та Австралія.

Дослідники стверджують, що регулятори повинні впроваджувати мінімальні стандарти безпеки для виробників пристроїв в IoT, заохочувати рівень безпеки вище мінімального рівня через державні контракти та прагнути до міжнародного узгодження стандартів IoT, таких як міжнародні рекомендації щодо поводження з розгорнутими підключеними пристроями, які не отримують оновлення безпеки.

ДОСЛІДЖЕНО СТАН КІБЕРБЕЗПЕКИ В КОМПАНІЯХ НАФТОГАЗОВОГО СЕКТОРУ - TREND MICRO

Компанія Trend Micro провела дослідження щодо стану промислової кібербезпеки в нафтогазовій сфері, обробній та енергетичній промисловості у 2022 році. На основі результатів опитування понад 900 реципієнтів у ICS у США, Німеччині та Японія були визначені ключові тенденції та проблеми галузей. Серед результатів дослідження – в нафтогазовій промисловості простої в наслідок кібератак тривають в середньому 6 днів. Також нафтогазові компанії, через особливості виробничого циклу, менше вдаються до поліпшення заходів кібербезпеки навіть після вдалих кібератак. Загальна рекомендація фахівців Trend Micro полягає у посиленні лідерства керівників компаній в питаннях кібербезпеки та посилення кібербезпекових вимог до ділових партнерів.

TREND MICRO ОПРИЛЮДНИЛО РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ЩОДО КЛЮЧОВИХ КІБЕРБЕЗПЕКОВИХ ТЕНДЕНЦІЙ ПЕРШОЇ ПОЛОВИНИ 2022 РОКУ

20 жовтня Trend Micro опублікувало перші результати свого дослідження щодо кіберзагроз першої половини 2022 року. Результати базуються на опитуванні 6297 керівників IT-безпеки у 29 країнах. Серед ключових результатів: збільшенням площі атаки (73% описують безпекову ситуацію як постійний розвиток і безлад), зростає попит на зловмисне програмне забезпечення як послугу (MaaS), модель RaaS надала хакерам доступ до інструментів та інфраструктури, які інакше були б недоступні (за першу половину цього року 1200 організацій постраждали від програм-вимагачів, що діяли по моделі RaaS), системи на базі Linux стають все цікавішою мішенню для вірусів-вимагачів.

ОСНОВНИМ ТИПОМ РИЗИКІВ В ЖОВТНІ 2022 РОКУ СТАЛО «ЗБІЛЬШЕННЯ ПРИВІЛЕЇВ» – АНАЛІЗ CROWDSTRIKE

13 жовтня аналітики кібербезпекової компанії CrowdStrike оприлюднили результати своїх досліджень щодо ризиків безпеці у жовтні 2022 року. Розподіл типів кібератак сформувався наступним чином: основним ризиком виявилась загроза «Збільшення привілеїв» (46%), друге місце за віддаленим виконанням коду (майже 24%) і на третьому – розкриття інформації (13%).

ІНДЕКС КІБЕРПОТУЖНОСТІ ДЕРЖАВ ЗА 2022 РІК ВІД HARVARD BELFER CENTER

Дослідники Белферського центру при Гарвардському університеті опублікували другий індекс кіберпотужнсті держав. Перший було опубліковано у 2020 році. Індекс є проєктом, що розвивається, і має на меті запровадити цілісний підхід до оцінки кіберпотужності держав.

Цьогорічний звіт оцінює держави за вісьмома вимірами: спостереження, оборона, розвідка, комерційний сектор, норми, фінансовий сектор, контроль за інформацією та руйнівні кіберпотужності. Автори індексу оцінили 30 держав, серед яких і Україна. Перша п'ятірка країн відповідно до індексу: США, Китай, росія, Великобританія, Австралія. Україна на 12 місці (між Німеччиною та Канадою).

Автори звіту наголошують, що через зміну балансу на міжнародній арені та геополітичні події, а також зростання впливу Китаю, особливо в кіберсфері, держави зараз, як ніколи, прагнуть формувати нові коаліції, аби ліпше забезпечити свої інтереси в глобальному кіберпросторі. Такий індекс допомагає не лише порівняти потужності країн, а й зрозуміти, які з них є близькими за підходами.

ЗАХИСТ ЕЛЕКТРОННОЇ ПОШТИ: ХТО ЦЕ РОБИТЬ НАЙКРАЩЕ?

Дослідники компанії Avanan випустили звіт за результатами аналізу понад трьох мільйонів електронних листів, щоб визначити, як Microsoft Defender та інші служби захисту протистоять найсучаснішим складним загрозам, які намагаються обійти захист. Дослідники наголошують на актуальності свого дослідження, адже причиною номер один для всіх зламів є електронна пошта. Її доля становить колосальні 90%.

СТАН З ПРОГРАМАМИ-ВИМАГАЧАМИ У ТРЕТЬОМУ КВАРТАЛІ 2022 РОКУ

19 жовтня дослідники Digital Shadows випустили звіт щодо стану програм-вимагачів у третьому кварталі 2022 року. У звіти йдеться про те, що активність програм-вимагачів сповільнилася, загальна активність знизилася на 10,5% порівняно з попереднім кварталом. Ймовірно, це пов'язано з основними подіями у другому кварталі 2022 року, зокрема з припиненням діяльності групи програм-вимагачів Conti та запуском останньої партнерської програми «LockBit 3.0». Серпень був спокійнішим місяцем для більшості груп програм-вимагачів, за винятком LockBit, але у вересні 2022 року активність знову зросла, що є можливим передвісником того, що буде відбуватися в четвертому кварталі 2022 року.

7. КІБЕРБЕЗПЕКОВА СИТУАЦІЯ В УКРАЇНІ

В Україні пройшов Місяць кібербезпеки. Незважаючи на загострення ситуації з ракетними обстрілами та атаками дронів з боку рф основні суб'єкти кібербезпеки в Україні, профільні навчальні заклади та бізнес провели багато заходів та навчальних курсів.

УКРАЇНА РОЗВИВАЄ СПІВПРАЦЮ З АГЕНТСТВОМ ЄС З МЕРЕЖЕВОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Керівник служби з питань інформаційної безпеки та кібербезпеки Апарату Ради національної безпеки і оборони України, секретар НКЦК Наталія Ткачук та заступник Голови Держспецзв'язку Віктор Жора провели робочу зустріч з директором Агентства Європейського Союзу з мережевої та інформаційної безпеки (ENISA) паном Юханом Лепасаром.

Під час зустрічі, яка відбулася у рамках візиту до штаб-квартири ENISA, організованого Cybersecurity East Project за сприяння РЄ, було обговорено перспективні напрями взаємодії та необхідність розробки дорожньої карти розвитку співробітництва. Українські фахівці наголосили, що для нашої країни налагодження практичної взаємодії з ENISA та отримання особливого статусу партнера стане надзвичайно важливим кроком на шляху євроінтеграції та необхідності гармонізації вітчизняного законодавства у сфері кібербезпеки з європейським.

УКРАЇНА ТА ЄС ПРОВЕЛИ ДРУГИЙ РАУНД ДІАЛОГУ З ПИТАНЬ КІБЕРБЕЗПЕКИ

Україна та Європейський Союз провели другий раунд Діалогу з питань кібербезпеки. На тлі невиправданої та непровокованої воєнної агресії з боку російської федерації проти України учасники Діалогу підкреслили важливість подальшого посилення своїх зусиль і співпраці для нарощування стійкості до кіберзагроз. ЄС висловив солідарність із Україною, яка нині протистоїть кіберзагрозам, спрямованим на знищення її критичної інфраструктури, та запевнив у готовності й надалі надавати підтримку. Російська федерація повинна негайно припинити цю безглузду й незаконну війну та покласти край людським стражданням.

Україна та ЄС обмінялися думками щодо поточного ландшафту загроз, серед усього – численних кібератак проти критичної інформаційної інфраструктури України, які розпочалися ще до початку повномасштабного вторгнення у лютому і тривають донині.

НКЦК СПІЛЬНО З ГЛОБАЛЬНИМ ЦЕНТРОМ ВЗАЄМОДІЇ В КІБЕРПРОСТОРІ ЗАПОЧАТКУВАВ ПЕРШУ В УКРАЇНІ НАВЧАЛЬНУ ПРОГРАМУ СТРАТЕГІЧНОГО ЛІДЕРСТВА ДЛЯ УПРАВЛІНЦІВ У СФЕРІ КІБЕРБЕЗПЕКИ

7-8 жовтня 2022 року розпочався навчальний курс «Програма стратегічного лідерства для українських управлінців у сфері кібербезпеки SJC-2022». Головною метою курсу є підвищення рівня професійної підготовленості керівників державного та приватного секторів, політиків, які залучені до створення спільних стратегічних рішень з питань кібербезпеки.

Програма розроблена Глобальним центром взаємодії в кіберпросторі спільно з кращими міжнародними експертами та за підтримки Національного координаційного центру кібербезпеки. Вона складається з шести модулів, кожен з яких є унікальним. Для навчання було відібрано 43 керівники з державного та приватного секторів, які працюють у сфері кібербезпеки. Реалізація програми стала платформою, де вони зможуть обмінюватися досвідом, розвивати стратегічне мислення та ухвалювати нелінійні/асиметричні рішення для посилення національних кібербезпекових спроможностей.

НКЦК ТА CRDF GLOBAL ПРОВЕЛИ XV ЗАСІДАННЯ НАЦІОНАЛЬНОГО КЛАСТЕРА КІБЕРБЕЗПЕКИ

27 жовтня 2022 року у м. Вінниця відбулося XV засідання Національного кластера кібербезпеки тему «Поточний стан, виклики та перспективи реалізації Стратегії кібербезпеки на місцевому рівні», організоване Національним координаційним центром кібербезпеки при РНБО спільно CRDF Global в Україні та за підтримки U.S. Department of State.

До обговорення актуальних регіональних потреб у галузі онлайн та офлайн долучилися близько 200 учасників з державного та приватного секторів, представників міжнародних інституцій та наукової спільноти. З-поміж них – представники Національного центру кібербезпеки Великобританії, Вінницької міської ради, АТ «Вінницяобленерго», Державної служби спеціального зв'язку та захисту інформації України та Вінницької ІТ-асоціації.

Учасники Кластера обговорили поточний стан реалізації Стратегії на місцевому рівні та основні виклики і загрози з урахуванням агресії рф в кіберпросторі. Запропоновано ряд ініціатив і проєктів, спрямованих на підвищення рівня кібербезпеки України та посилення взаємодії між державою, академічною спільнотою, приватним сектором тощо.

НКЦК ЗА ПІДТРИМКИ USAID ПРОВІВ КРУГЛИЙ СТІЛ ЩОДО РОЗРОБКИ НАЦІОНАЛЬНОГО ПЛАНУ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України» 17 жовтня 2022 року провів круглий стіл на тему «Готовність та стійкість до кібератак національного рівня: яким має бути Національний план реагування?».

У заході взяли участь представники всіх основних суб'єктів забезпечення кібербезпеки, Міністерства цифрової трансформації України та Міністерства закордонних справ України. Вони обговорили структуру та формат майбутнього Національного плану реагування на кіберінциденти, а також успішні кейси впровадження такого документа в провідних країнах світу. За результатами обговорення внесено пропозиції щодо наповнення та реалізації Плану з урахуванням досвіду реагування на кібератаки під час війни.

ПОНАД 400 ПРЕДСТАВНИКІВ ДЕРЖСЕКТОРУ ПРОЙШЛИ НАВЧАННЯ ЗА НАПРЯМОМ OSINT

НКЦК та CRDF Global в Україні провели триденний теоретичний та практичний семінар для представників державного сектору на тему: «OSINT – розвідка із використанням відкритих джерел». Учасники ознайомились з останніми дослідженнями у сфері OSINT та особливостями організації та проведення інформаційно-психологічних операцій у воєнний час.

У заході взяли участь понад 400 представників державного сектору. Разом із провідними експертами від української компанії Molfar та волонтерської спільноти InformNapalm вони обговорювали останні дослідження та мали змогу одразу перевірити набуті навички, виконавши низку завдань, що допомогло краще засвоїти пройдений матеріал.

МИ ВКОТРЕ ДОВЕЛИ, ЩО УКРАЇНСЬКІ КІБЕРСПЕЦІАЛІСТИ Є ОДНИМИ З НАЙКРАЩИХ У СВІТІ – СЕРГІЙ ДЕМЕДЮК

6 жовтня у Київському коледжі зв'язку з нагоди початку проведення місяця кібербезпеки відбувся урочистий захід «Кібервійна з росією: освіта в умовах нових викликів та загроз», в якому з вітальним словом виступив заступник Секретаря Ради національної безпеки і оборони України Сергій Демедюк.

«Повномасштабна війна в Україні триває вже понад сім місяців. Вона показала, що кіберскладова є важливим елементом нашої обороноздатності. Отриманий бойовий досвід ставить нашу державу в один ряд із провідними країнами світу у сфері кібербезпеки. Триває процес створення кібервійськ, які мають стати в майбутньому потужною складовою сил оборони нашої держави. Ми вкотре показали, що українські кіберспеціалісти є одними з найкращих у світі, і наш досвід, здобутий під час першої кібервійни, маємо використати для зміцнення обороноздатності, для вдосконалення практики та навчання», – сказав Сергій Демедюк.

Захід було організовано Торгово-промисловою палатою України та Київським коледжем зв'язку. У ньому взяли участь представники Апарату РНБО України, Міністерства оборони України, Держспецзв'язку та Департаменту кіберполіції НПУ, а також викладачі, аспіранти та студенти.

ЖІНОЧЕ ЛІДЕРСТВО У СФЕРІ КІБЕРБЕЗПЕКИ НЕВДОВЗІ СТАНЕ ЗВИЧНОЮ ПРАКТИКОЮ – НАТАЛІЯ ТКАЧУК

Керівник служби з питань інформаційної та кібербезпеки Апарату РНБОУ, секретар НКЦК Наталія Ткачук взяла участь у менторській програмі для дівчат спеціальності «125 Кібербезпека» та виступила на заключній конференції програми «Кар'єрні траєкторії у кібербезпеці».

Метою програми, яка реалізується Проєктом USAID Cybersecurity Activity та ініціативою Дівчата STEM, стало підвищення рівня поінформованості студентів про актуальні шляхи побудови та розвитку кар'єри у сфері кібербезпеки.

Протягом двох місяців дев'ятнадцять дівчат-менті з першого по шостий курс ЗВО, спеціальності «125-кібербезпека» отримували менторську підтримку від дев'яти успішних жінок, які працюють в кібербезпеці у державному та приватному секторі. «Я впевнена, що дуже скоро словосполучення «жінки в кібербезпеці» буде такою ж аксіомою, як «жінки в медицині» чи «жінки в науці». І аби це сталось якнайшвидше, ми повинні постійно привертати увагу суспільства до цієї теми. В Україні триває перша у світі кібервійна, і нам як ніколи потрібні нові таланти. Жінки розумні, дисципліновані, творчі, цілеспрямовані, вони не менш ніж чоловіки є ефективними IT-спеціалістами, експертами в кібербезпеці, аналітиками, керівницями та лідерками», – сказала Наталія Ткачук.

ЗА СПРИЯННЯ НКЦК ПРЕДСТАВНИКИ ОРГАНІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ РОЗПОЧАЛИ НАВЧАННЯ З ІМПЛЕМЕНТАЦІЇ ІНСТРУМЕНТАРІЮ OSINT

НКЦК спільно з Національною академією СБ України та Інститутом постінформаційного суспільства запустили навчальний курс із імплементації інструментів OSINT для представників органів сектору безпеки і оборони.

У курсі візьмуть участь близько 100 представників державних органів сектору безпеки і оборони, які опановуватимуть основні методики та принципи розвідки з відкритих джерел, інструменти та сервіси, які використовуються для OSINT, з-поміж яких Google-інструменти, пошук по фото, методи деанонімізації в мережі Інтернет, моніторинг соцмереж та месенджерів (телеграм-канали), побудова графіків взаємозв'язків тощо.

«Незважаючи на складні часи для нашої держави, саме зараз, як ніколи, маємо вибудовувати спроможності сектору безпеки і оборони із протидії загрозам з боку країни-терориста. Інформаційний та кіберпростір вже давно перетворився на поле ведення бою. І соціальні мережі, і телеграм-канали, і власне, інформація у цій війні також стають зброєю. Тож маємо випереджати ворога за якістю підготовки та вмінні давати гідну відсіч», – наголосила керівник служби з питань інформаційної та кібербезпеки Апарату РНБО України – секретар Національного координаційного центру кібербезпеки Наталія Ткачук.

НАЙБІЛЬША РОЗВІДУВАЛЬНО-АНАЛІТИЧНА КОМПАНІЯ У СВІТІ RECORDED FUTURE В ПОШУКАХ 100 СПІВРОБІТНИКІВ В УКРАЇНІ

Мінцифра та Національний координаційний центр кібербезпеки при РНБО допоможуть Recorded Future знайти нові таланти в Україні. До 2025 року компанія планує найняти до 100 співробітників, серед яких розробники ПО, інженери, аналітики тощо. Наразі в Україні вже працює 40 співробітників компанії.

ДЕРЖСПЕЦЗВ'ЯЗКУ СТАНЕ УПОВНОВАЖЕНИМ ОРГАНОМ ІЗ ПИТАНЬ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Верховна Рада ухвалила в цілому проєкт Закону «Про внесення змін до деяких законів України щодо формування та реалізації державної політики у сфері захисту критичної інфраструктури». Він визначає, що функції уповноваженого органу з питань захисту критичної інфраструктури України виконуватиме Держспецзв'язку.

Документ – закономірний крок держави в напрямку посилення стійкості критичної інфраструктури країни. Попередній варіант законодавства передбачав створення окремого органу, який відповідатиме за ці завдання. Реалізація ухвалених змін дасть можливість без створення нового органу забезпечити формування та реалізацію державної політики у сфері критичної інфраструктури і зекономити державні кошти.

CERT-UA ПОПЕРЕДЖАЄ ПРО РОЗСИЛАННЯ ШКІДЛИВИХ ЕЛЕКТРОННИХ ЛИСТІВ ВІД ІМЕНІ СТРУКТУР СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ

Фахівці Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA 21 жовтня виявили факт розповсюдження електронних листів, начебто від імені пресслужби Генштабу ЗСУ. У повідомленнях містилося посилання на завантаження «наказу», перейшовши за яким, жертва потрапляла на сторінку з повідомленням про необхідність оновлення програмного забезпечення (PDF Reader). Натискання на кнопку «ЗАВАНТАЖЕННЯ» призводить до завантаження шкідливої програми RomCom.

Проведений командою CERT-UA аналіз шкідливої активності дає можливість асоціювати її з діяльністю групи Tropical Scorpius (Unit42) aka UNC2596 (Mandiant), яка відповідальна за розповсюдження шкідливого ПЗ Cuba Ransomware.

ЗАВДЯКИ ЧАТ-БОТУ СБУ ЗНИЩЕНО СОТНІ ОДИНИЦЬ ВОРОЖОЇ ТЕХНІКИ І НАВІТЬ ДЕКІЛЬКОХ ГЕНЕРАЛІВ – ІЛЛЯ ВІТЮК

Телеграм-бот @stop_russian_war_bot, створений СБУ на початку повномасштабного вторгнення рф, отримав більше 100 тис. повідомлень від українців. Це дозволило знищити сотні одиниць ворожої техніки і навіть ліквідувати декількох російських генералів.

«Через наш бот надійшло понад 100 тис. повідомлень про переміщення ворога! Ми уточнювали та перевіряли цю інформацію через агентурні можливості, операторів БПЛА та дронів, порівнювали з даними з супутників і пересилали до артилерії ЗСУ. В результаті – багато сотень результативних влучань по великим колонам техніки, знищено не одного генерала рф», – повідомив Ілля Вітюк.

З ПОЧАТКУ ВІЙНИ СБУ НЕЙТРАЛІЗУВАЛА МАЙЖЕ 3,5 ТИС. КІБЕРАТАК НА ОРГАНИ ВЛАДИ ТА ОБ'ЄКТИ ІНФРАСТРУКТУРИ

З початку повномасштабного вторгнення нейтралізовано майже 3,5 тис. кібератак на електронні системи центральних органів влади та об'єкти критичної інфраструктури України. З них 1650 кіберзагроз виявлено в режимі «реального часу» за допомогою Системи управління подіями інформаційної безпеки, що створена на базі СБУ.

Встановлено, що переважна більшість російських атак мали на меті або знищити цифрові сервіси, або дестабілізувати роботу стратегічно важливих підприємств енергетичної та транспортної галузей. До організації і проведення таких диверсій причетні російські спецслужби та підконтрольні їм хакерські угруповання.

КІБЕРПОЛІЦІЯ ІДЕНТИФІКУВАЛА ПОНАД 14500 ВІЙСЬКОВОСЛУЖБОВЦІВ РФ, ЯКІ БРАЛИ УЧАСТЬ У БОЙОВИХ ДІЯХ НА ТЕРИТОРІЇ УКРАЇНИ – ЮРІЙ ВИХОДЕЦЬ

«Наші працівники змінили вектор роботи на протидію кібератакам на державні органи та приватний сектор, виявлення та реагування на антиукраїнську пропаганду в інтернеті, ідентифікацію колаборантів, розробку систем та механізмів для збору інформації з відкритих джерел про військовослужбовців рф», – повідомив Юрій Виходець.

Він розповів, що наразі працівники кіберполіції вже ідентифікували понад 14500 військовослужбовців рф, які брали участь у бойових діях на території України. Також зафіксовано участь 170 членів незаконних збройних формувань у бойових діях та фінансуванні війни. Спільно з іншими суб'єктами кібербезпеки попереджено майже 400 кібератак на українські інформаційні ресурси, а також проведено заходи щодо ліквідації їх наслідків.

Загалом із початку воєнного стану працівники підрозділу провели понад 1400 обшуків. За цей час правоохоронці виявили близько 800 фактів онлайн-шахрайства, викрили 23 педофіли, які безпосередньо створювали та розповсюджували протиправний контент за участю дітей. Від їх дій постраждало 48 дітей.

КІБЕРПОЛІЦІЯ СПІЛЬНО ІЗ ВОЛОНТЕРАМИ ЗАБЛОКУВАЛА 14 ТИСЯЧ ВОРОЖИХ РЕСУРСІВ

Майже 750 тисяч людей об'єднав проєкт «МРІЯ», створений для ліквідації каналів російських пропагандистів та осіб, які підтримують війну. З початку повномасштабного вторгнення проєкт «МРІЯ» змінив профіль і став спільним проєкт із волонтерами та громадянами для протидії інтернет-пропаганді ворога.

Найбільша сила цієї спільноти — це підписники, завдяки їм, вдається успішно блокувати та протидіяти російській агресії в інтернеті. Наразі проєкт об'єднав майже 750 тисяч людей, які заблокували більше 14-ти тисяч ворожих ресурсів, котрі розповсюджують дезінформацію та пропаганду. Загальна аудиторія цих ресурсів становить близько 67 мільйонів підписників.

КІБЕРПОЛІЦІЯ ВИКРИЛА МАСШТАБНУ МЕРЕЖУ БОТОФЕРМ, ЩО ПОШИРЮВАЛА ФЕЙКИ ТА ПРОПАГАНДУ ПРО ВІЙНУ В УКРАЇНІ

Ботоферма нараховувала понад 50 тисяч ботів у соціальних мережах та поштових сервісах. Спільно з Головним слідчим управлінням Нацполіції встановлено чотирьох організаторів мережі ботоферм.

Для реалізації злочинної схеми фігуранти залучали громадян рф та жителів тимчасово окупованих територій України. Виконавці отримували оплату за створені акаунти у російських рублях через заборонені в Україні електронні платіжні системи. Фейкові сторінки використовувалися для поширення недостовірної інформації щодо війни, виправдання окупації українських територій та пропаганди у вигляді дописів та коментарів у соцмережах. Правопорушники генерували майже 3 тисячі фейкових акаунтів на тиждень. Загалом мережа ботоферм налічувала більше 50 тисяч ботів. Крім цього, фігуранти здійснювали рекламування фішингових шахрайських сторінок.

Під час проведених обшуків вилучено майже 35 тисяч SIM-карт різних мобільних операторів України та інших держав, а також комп'ютерну техніку, мобільні телефони та документацію. Розслідується кримінальне провадження за ч. 3 ст. 361 Кримінального кодексу України. Фігурантам загрожує до восьми років позбавлення волі.

ПЕРЕБОЇ З ІНТЕРНЕТОМ ПІД ЧАС РАКЕТНИХ УДАРІВ

За даними Bitdefender та інших, у деяких районах України під час російських ракетних ударів 10 жовтня відбулися збої в Інтернеті, в основному пов'язані з перебоями в електропостачанні та фізичними порушеннями зв'язку. «Дані Cloudflare свідчать про зниження доступності Інтернету на 35%, оскільки численні вибухи спричинили перебої в електропостачанні. Cloudflare повідомила, що перебої в Інтернеті спричинили явне падіння трафіку після 06:15 10 жовтня у Харкові (приблизно на 80% менше трафіку), Львові (приблизно на 60% падіння), а також, меншою мірою, в столиці України Києві». Послуги електропостачання та зв'язку були в основному відновлені. Українські чиновники віддають належне Starlink через важливу роль у швидкому відновленні інтернет послуг, повідомляє Reuters.

ДЕРЖСПЕЦЗВ'ЯЗКУ НАГАДУЄ ПРО ПРОСТІ ПРАВИЛА БЕЗПЕКИ В МЕРЕЖІ ІНТЕРНЕТ

Найпростіший спосіб поширити шкідливе програмне забезпечення чи скерувати користувача на шкідливий сайт, що краде персональні дані – повідомлення із вкладеними файлами та посиланнями. Такі повідомлення зловмисники можуть надсилати на електронну скриньку, в приватні повідомлення у соціальних мережах та месенджерах, в SMS, чатах тощо.

Допис із посиланням на шахрайський сайт може бути розміщено навіть у місцевому новинному паблiку чи групі. У таких випадках часто використовують спекуляції на тему соціальних виплат начебто від держави для внутрішньо переміщених осіб та українців, які постраждали під час війни. Тому варто дотримуватись рекомендацій.

ДЕРЖСПЕЦЗВ'ЯЗОК ІНФОРМУЄ ЩОДО СПЕЦІАЛЬНОСТЕЙ З КІБЕРБЕЗПЕКИ

Україна зараз як ніколи раніше потребує фахівців із кібербезпеки та кіберзахисту, які зможуть чинити гідний опір ворогу на кіберфронті. У межах Місяця кібербезпеки в Україні Держспецзв'язку створила спеціальний сайт – https://cybermonth.cip.gov.ua, на якому можна знайти корисну інформацію з кібербезпеки для всіх груп користувачів інтернету, в тому числі – тих, хто планує зробити кібербезпеку своєю професією.

8. ПЕРША СВІТОВА КІБЕРВІЙНА

КЕРІВНИК NSA ОЗВУЧИВ ШІСТЬ СВОЇХ ОСНОВНИХ ВИСНОВКІВ РОСІЙСЬКО-УКРАЇНСЬКОЇ КІБЕРВІЙНИ

18 жовтня керівник NSA USA Роб Джойс виступив на конференції Mandiant Worldwide Information Security Exchange (mWISE) де поділився своїми основними висновками з російсько-української кібервійни: кібервійна супроводжується поєднанням як руйнівних кібероперацій, так і актами кібершпигунства.

Приватні компанії швидше реагували на зміну ситуації і саме їх інформація допомагала державних органам буде ефективнішими. Розвідувальні органи краще навчились працювати з отриманими даними, «очищати» їх для більшої цінності при прийнятті рішень. Україна продемонструвала високий рівень стійкості та навичок відновлення після інцидентів. Згуртованість недержавного сектора забезпечує ліпшу безпеку в таких конфліктах, а резервне копіювання даних у хмару – ліпшу стійкість. Іноземні компанії часто не розуміють, наскільки вони пов'язані із іноземними партнерами (в даному випадку – з українськими).

ВІЙНА РФ ПРОТИ УКРАЇНИ: ХРОНОЛОГІЯ КІБЕРАТАК

Дослідницька служба Європейського парламенту опублікувала довідку щодо війни рф проти України у кіберпросторі. Матеріал містить короткий хронологічний опис атак, що їх зазнає Україна, починаючи з 2014 року, а, також, опис відповіді міжнародної спільноти та позицію Європейського парламенту з цього питання.

ОЧІЛЬНИЦЯ БРИТАНСЬКОГО НАЦІОНАЛЬНОГО ЦЕНТРУ КІБЕРБЕЗПЕКИ (NCSC) ПРО ВИСНОВКИ З КІБЕРКОНФЛІКТУ В УКРАЇНІ

Виступаючи під час події, присвяченої кібервиміру російсько-української війни, організованої Chattem House, очільниця Національного центру кібербезпеки (NCSC) Лінді Камерон наголосила на важливій ролі захисту. Після вторгнення 24 лютого росія веде постійну зловмисну кіберкампанію проти України та її союзників, але її безуспішність показує, що можна захиститися від кібератак, навіть з боку деяких із найдосконаліших і наполегливих зловмисників, заявила вона.

Якщо український кіберзахист і дає нам ширший урок – для військової теорії та за її межами – він полягає у тому, що в кібербезпеці захисник має широкий вибір. У багатьох випадках ви можете вибрати, наскільки ви можете бути вразливими до атак.

«Ключовим у такій ситуації є прагнення до довгострокової стійкості», –сказала Кемерон. «Побудова стійкості означає, що нам не обов'язково потрібно знати, де або як загроза проявить себе наступного разу. Натомість ми знаємо, що більшість загроз не зможуть зламати наш захист. А якщо це станеться, ми зможемо швидко й повністю відновитися».

ФІНСЬКА РОЗВІДКА ПОПЕРЕДЖАЄ, ЩО З ВЕЛИКОЮ ЙМОВІРНІСТЮ РОСІЯ ВЗИМКУ ВДАСТЬСЯ ДО КІБЕРАТАК

У відкритому Огляді національної безпеки за 2022 рік, опублікованому наприкінці вересня, Служба безпеки Фінляндії стверджує, що традиційний підхід росії до збору розвідданих із використанням шпигунів із дипломатичним прикриттям «став значно складнішим після того, як рф розпочала свою агресивну війну в Україні, оскільки багато російських дипломатів були виселені з Заходу». Загроза корпоративного шпигунства з боку росії також зростає, оскільки санкції вимагають запуску високотехнологічного виробництва для заміни імпорту із Заходу.

ГРОМАДЯНИ РФ РОЗВ'ЯЗУЮТЬ КІБЕРВІЙНУ ПРОТИ УРЯДУ ЗСЕРЕДИНИ КРАЇНИ

2 жовтня українське англомовне видання KyivPost повідомило, що з ним зв'язалися хакери, які називали себе членами Національної республіканської армії (NRA), яка являє собою організацією громадян рф, які прагнуть повалення режиму путіна. Представники NRA заявили, що за допомогою віруса-вимагача, атакували компанію Unisoftware, серед клієнтів якої ФНС, Мінфін рф і Центробанк росії. Вони повідомили, що атака стала наслідком політики, що її проводить президент путін, посилаючи «наших юнаків гинути в несправедливій війні проти України».

РОСІЙСЬКЕ ХАКЕРСЬКЕ УГРУПОВАННЯ KILLNET АТАКУВАЛО ВЕБСАЙТИ ОРГАНІВ ДЕРЖАВНОГО УПРАВЛІННЯ США

5 жовтня російське хакерське угруповання Killnet взяло на себе відповідальність за атаки на урядові сайти штатів Колорадо, Кентуккі, Міссісіпі та ін. Ці дії є частиною кампанії політично мотивованих атак на країни, що підтримують Україну, яка інтенсифікувалася після 24 лютого 2022 року. В результаті DDos атаки доступ до сайтів був нерегулярним протягом дня 5 жовтня, але до вечора його переважно було відновлено. Експерти з кібербезпеки вважають Killnet загрозою низького рівня, адже його учасники відключають сайти від мережі, але не руйнують їх інфраструктуру. Разом з тим, привертає на себе увагу комунікаційна складова мережі. Відповідь CISA https://twitter.com/CISAJen/status/1580171703908331520

СТРАХОВИЙ ГІГАНТ LLOYD'S OF LONDON РОЗСЛІДУЄ КІБЕРАТАКУ

5 жовтня страховий гігант Lloyd's of London повідомив, що експерти з кібербезпеки компанії «виявили незвичайну активність у своїй мережі». Компанія не розкриває деталей того, що відбулося, але тимчасово відключила зовнішні зв'язки своєї системи та повідомила партнерів та клієнтів про проблему. Журналісти наголошують, що компанія була одним з лідерів у запровадженні санкцій проти російської федерації у відповідь на її агресію проти України.

УГРУПОВАННЯ «ANONYMOUS RUSSIA» АТАКУВАЛО САЙТ БРИТАНСЬКОЇ СЛУЖБИ ВНУТРІШНЬОЇ БЕЗПЕКИ MI5

30 вересня служба внутрішньої безпеки Великої Британії MI5 внаслідок DDoS-атаки ненадовго відключила свій публічний вебсайт. Фахівці схарактеризували атаку як примітивну та короткочасну. Обслуговування було швидко відновлено, і MI5 каже, що жодних даних не було втрачено чи розкрито. Відповідальність взяла на себе номінальна хактивістська група, яка називає себе «Anonymous russia», яка заявляє, що є російським підрозділом міжнародного хакерського угруповання Anonymous.

КРИПТОВАЛЮТИ ПІДЖИВЛЮЮТЬ ВТОРГНЕННЯ РОСІЇ В УКРАЇНУ

Дослідники виявили, що від початку повномасштабного вторгнення росії в Україну групи, які підтримують російську армію в Україні, зібрали криптовалюти на суму щонайменше 4 мільйони доларів. Відповідно до аналізу, проведеного компаніями з відстеження криптовалют Chainalysis, Elliptic і TRM Labs, а також дослідниками найбільшої у світі криптовалютної біржі Binance, до одержувачів належать воєнізовані групи, які пропонують боєприпаси та обладнання, військові підрядники та виробники зброї.

Цей потік коштів, часто спрямований до угрупувань, що офіційно знаходяться під санкціями, не має жодних ознак зменшення та може навіть прискорюватися. І хоча ці потоки можливо відстежувати, блокувати їх доволі важко, через санкції, накладені на біржі криптовалют, або тому, що вони знаходяться у рф та не мають запобіжників проти кримінального відмивання грошей. Деякі з використовуваних бірж знаходяться в Китаї та Індії.

СВІТ МАЄ БУТИ ГОТОВИЙ ДО ЕСКАЛАЦІЇ КІБЕРКОНФЛІКТІВ ВНАСЛІДОК КІБЕРПРОТИБОРСТВА МІЖ РОСІЄЮ ТА УКРАЇНОЮ, ЩО ТРИВАЄ

CyberPeace Institute провів 17 жовтня у Женеві захід, присвячений обговоренню кібербезпекової ситуації навколо України. Основний спікер заходу – представник НАТО Крістіан-Марк Ліфлендер – підкреслив, що Україна стикаючись зі значними кіберзагрозами змогла показати нову якість взаємодії держави та приватного сектора.

Водночас представник Міжнародного комітету Червоного Хреста Бальтазар Штехелін зауважив, що акцент на Україні не повинен відвертати увагу від інших кібератак, в т.ч. – на МКЧХ який все ще відчуває наслідки кібератаки початку 2022 року. Також Ніколь Перлрот, автор книги «Ось як вони кажуть мені, що настав кінець світу» зауважила, що успіхи України проти Росії підвищують ризик кібератак у відповідь: «З кожним днем, з кожною перемогою українців рівень загрози зростає».

НОВА КОМПАНІЯ ВІРУСІВ ВИМАГАЧІВ «PRESTIGE» СПРЯМОВАНА НА ЦІЛІ В УКРАЇНІ ТА ПОЛЬЩІ

Починаючи з 11 жовтня скоординована кампанія програм-вимагачів була спрямована на транспортний та логістичний сектори в Україні та Польщі. Центр аналізу загроз компанії Microsoft повідомив, що спостерігає за шкідливим програмним забезпеченням, яке називає себе «Prestige ranusomeware» у повідомленні, залишеному на пристроях жертви.

«Атаки, що протягом години спрямовувалися на всіх жертв по черзі», розпочались 11 жовтня. Корпорація Майкрософт заявила, що все ще проводить розслідування та поки що не приписує цю кампанію відомим зловмисним угрупованням. Однак Майкрософт зазначила, що є схожість з іншими атаками, включаючи руйнівні вайпери, які атакували Україну та її союзників після початку російського вторгнення.

ЧИ ЗМІНИТЬ ВІЙНА В УКРАЇНІ ІНТЕРНЕТ?

Дослідники Грегорі Тревертон та Парі Есфандіарі з Центру стратегічних і міжнародних досліджень (CSIS) розмірковують на тему впливу війни в Україні (в т.ч. її кіберскладової) на майбутнє інтернету взагалі. Вони вказують, що необхідність держав визначатись у моральній площині цього конфлікту змінює баланс і у підходах до самого майбутнього інтернету та моделі управління ним. Вони вказують на зростаючу роль Декларації майбутнього інтернету (від 28 квітня 2022 року) як документу, що може стати аналогом Загальної декларації прав людини для майбутніх міжнародних та національних нормативних актів що стосуються відносин в інтернеті.

У РФ ЗАЯВИЛИ ПРО РІЗКЕ ЗРОСТАННЯ КІЛЬКОСТІ НЕПРАВДИВИХ ПОВІДОМЛЕНЬ ПРО ТЕРАКТИ

З початку 2022 року в росії у вісім разів зросла кількість хибних повідомлень про теракти, що готуються. Різкий стрибок розпочався після старту спецоперації в Україні, заявив 19 жовтня голова МВС рф Володимир Колокольцев. Передбачувано, Колокольцев звинуватив у цій тенденції Україну, заявивши, що переважна більшість колцентрів, з яких надходять фальшиві повідомлення, знаходять на її території.

9. РІЗНЕ

АМЕРИКАНСЬКИЙ УРЯД ОТРИМАЄ ПЗ ЯКЕ ДОЗВОЛЯЄ ОБМАНЮВАТИ КІБЕРЗЛОВМИСНИКІВ ТА СКЕРОВУВАТИ ЇХ ДО ПАСТОК

6 жовтня стало відомо, що компанія CounterCraft підпислало контракт з Адміністрацією загальних служб США вартістю 26 мільйонів доларів в межах якого надасть всім урядовим агенціям (включаючи Пентагон) доступ до платформи Deception. Платформа створює автоматизовані «цифрові навігаційні крихти», щоб змусити хакерів подумати, що вони проникають у справжні комп'ютерні мережі. Платформа дозволить урядовим установам у режимі реального часу отримувати інформацію про зловмисників і їх цілі, скеровуючи їх у невірну сторону.

ПЕНТАГОН ГОТУЄТЬСЯ ДО УКЛАДАННЯ КОНТРАКТУ НА 9 МЛРД ДОЛАРІВ ДЛЯ ПОБУДОВИ ІНТЕГРОВАНОЇ ХМАРНОЇ СИСТЕМИ УПРАВЛІННЯ ВІЙСЬКАМИ

Пентагон продовжує обрання підрядника для створення Joint Warfighter Cloud Capability (JWCC) – спільного простору управління військами, що має забезпечити постійне під'єднання військ в різних регіонах світу. Платформа має забезпечувати роботу зі всіма рівнями секретності інформації (в т.ч. – особливо секретної). Як підрядників розглядаються чотири компанії: Amazon, Google, Microsoft і Oracle.