Державна служба спеціального зв'язку
та захисту інформації України

РОСІЙСЬКІ КІБЕР-ОПЕРАЦІЇ

Аналітика за ІІ півріччя 2024 року

ЗМІСТ

Передмова

Євгенія Наконечна
керівниця Державного центру
кіберзахисту Держспецзв'язку

2024 рік приніс Україні чергові випробування у сфері кібербезпеки. Ми щодня постаємо перед новими викликами: з одного боку, знайомі загрози від російських хакерських угруповань, пов'язаних з гу гш зс рф (гру) та фсб, з іншого — нові гравці, які діють ще агресивніше та більш автоматизовано. Кількість критичних інцидентів дещо зменшилася, але складність атак і ресурси, необхідні для їх відбиття, зросли в рази.

Залишається актуальною загроза ворожих атак проти енергетичної інфраструктури України та об'єктів критичної інфраструктури, які нерідко передують ракетним ударам.

Ми зосереджуємося на проактивному захисті, щоб унеможливити реалізацію деструктивних атак, але ворог постійно шукає нові слабкі місця. Його мета — не тільки завдати технічної шкоди, а й паралізувати роботу критичних сфер життєдіяльності, впливати на громадянське суспільство через залякування, дезінформацію та інформаційно-психологічні спецоперації (ІПСО). Атака на державні реєстри у грудні 2024 виявилася такою ж критичною, як і атака на найбільшого українського телеком-провайдера в грудні 2023. Це ще раз демонструє, що країна може мати широкий спектр «больових точок», які необхідно ретельно аналізувати, щоб забезпечити якісний кіберзахист і стійкість перед сучасними загрозами.

Наша основна мета — не просто реагувати на загрози, а випереджати їх. Ми щодня проводимо величезну роботу з виявлення присутності противника в мережах держустанов та критичної інфраструктури, посилюючи їхній захист. Але ефективна кібероборона — завжди спільна справа, тому міжнародна підтримка, обмін досвідом і технологіями залишаються ключовими для зміцнення нашої стійкості. Разом ми не лише захищаємо Україну, а й робимо кіберпростір безпечнішим для всієї Європи.

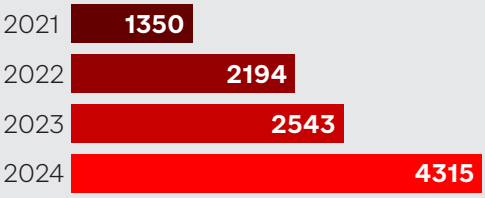
СТАТИСТИКА CERT-UA

СТАТИСТИКА CERT-UA

У другому півріччі 2024 року фахівці CERT-UA зафіксували значне зростання кількості кіберінцидентів. Пік активності припав на жовтень та листопад, коли ворожі хакери здійснили низку кампаній масового розповсюдження ШПЗ. Загалом кількість кіберінцидентів протягом другої половини 2024 року зросла на понад 48% порівняно з попереднім півріччям. Якщо подивитися на показники за підсумками календарного року, зростання кількості кіберінцидентів є ще помітнішим і становить майже 70%.

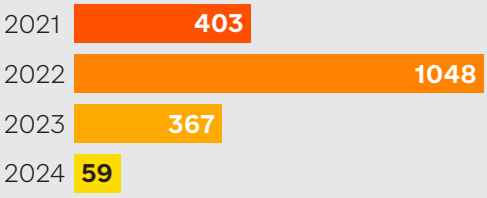
КІЛЬКІСНІ ПОКАЗНИКИ ОПРАЦЬОВАНИХ ІНЦИДЕНТІВ

Загальна кількість зареєстрованих кіберінцидентів



Зростання кількості кіберінцидентів свідчить про готовність російських спецслужб активніше використовувати кіберкомпонент як елемент ведення гібридної війни.

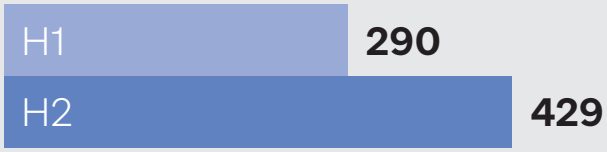
Кількість кіберінцидентів критичного та високого рівнів



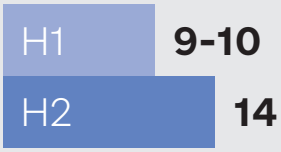
Завдяки налагодженій взаємодії з міжнародними партнерами та їхній підтримці вдалося суттєво знизити рівень деструктивного впливу кібератак у відношенні українських об'єктів.

ЗРОСТАННЯ КІЛЬКОСТІ ЗАРЕЄСТРОВАНИХ ІНЦИДЕНТІВ У ДРУГОМУ ПІВРІЧЧІ 2024 РОКУ

У СЕРЕДНЬОМУ ЗА МІСЯЦЬ



У СЕРЕДНЬОМУ ЗА ДЕНЬ



Як видно з графіків, зберігається тенденція до зростання загальної кількості кіберінцидентів. Водночас інцидентів високого та критичного рівнів стає дедалі менше.

Зареєстровані інциденти за рівнем критичності	H1 2024	H2 2024	Зміна за період
Критичні	3	1	-67%
Високі	45	10	-78%
Середні	1670	2457	+47%
Низькі	21	108	+414%
Загалом	1739	2576	+48%

На 77% менше інцидентів критичного та високого рівнів:

Кількість інцидентів	H1 2024	H2 2024	Зміна за період
Критичного та високого рівнів	48	11	77%

Також на 112% більше кіберінцидентів з розповсюдження ШПЗ
На 63% більше кіберінцидентів із зараження ШПЗ*

Кількість інцидентів, пов'язаних з ШПЗ	H1 2024	H2 2024	Зміна за період
Розповсюдження	531	1123	112%
Зараження	196	320	63%

Зростання кіберінцидентів, пов'язаних із зараженням ШПЗ, більшою мірою пов'язано зі збільшенням кількості шкідливих розсилок та збільшенням видимості, а меншою мірою — зі зміною ТТП*

У другому півріччі 2024 року найчастіше об'єктами кібератак ставали державні органи та сектор безпеки та оборони.

СЕКТОР БЕЗПЕКИ ТА ОБОРОНИ

H1 2024 276
H2 2024 +82% 502

УРЯДОВІ ОРГАНІЗАЦІЇ

H1 2024 473
H2 2024 +41% 665

МІСЦЕВІ ОРГАНИ ВЛАДИ

H1 2024 542
H2 2024 +53% 831

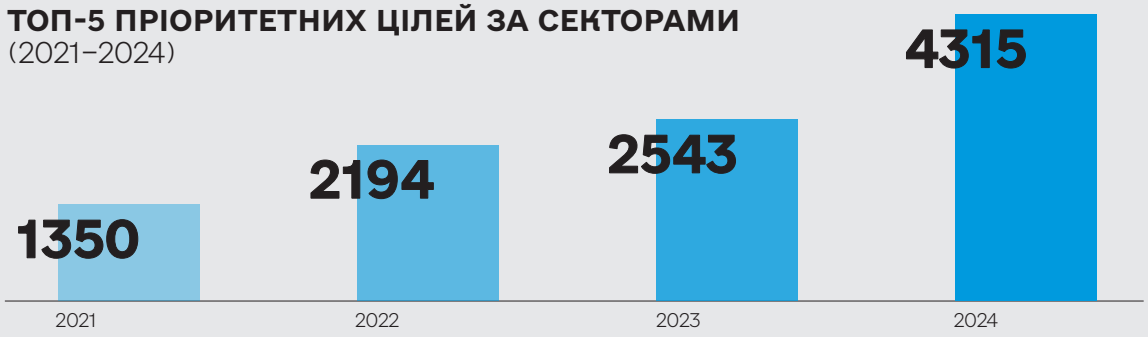
ЕНЕРГЕТИЧНИЙ СЕКТОР

H1 2024 124
H2 2024 127 +2%

ТЕЛЕКОМ ТА IT-СЕКТОР

H1 2024 19+7
H2 2024 33+4 +42%

ТОП-5 ПРІОРИТЕТНИХ ЦІЛЕЙ ЗА СЕКТОРАМИ
(2021–2024)



2021	2022	2023	2024
20% Урядові організації та місцеві органи влади	**26%** Урядові організації та місцеві органи влади	**25%** Урядові організації та місцеві органи влади	**58%** Урядові організації та місцеві органи влади
16% Сектор безпеки та оборони	**14%** Сектор безпеки та оборони	**7%** Сектор безпеки та оборони	**18%** Сектор безпеки та оборони
6% Комерційний сектор	**6%** Комерційний сектор	**5%** Комерційний сектор	**6%** Енергетичний сектор
6% Фінансовий сектор	**5%** Фінансовий сектор	**4%** Енергетичний сектор	**3%** Комерційний сектор
3% Енергетичний сектор	**5%** Енергетичний сектор	**4%** Телеком-компанії та інтернет-провайдери	**2%** Заклади освіти

Дані сформовано на основі аналітики інцидентів, опрацьованих ВИКЛЮЧНО Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA та SOC Державного центру кіберзахисту Держспецзв'язку*.

КЛЮЧОВІ ВИСНОВКИ ТА ІНСАЙТИ ЗА ДРУГЕ ПІВРІЧЧЯ 2024 РОКУ

КЛЮЧОВІ ВИСНОВКИ ТА ІНСАЙТИ ЗА ДРУГЕ ПІВРІЧЧЯ 2024 РОКУ

Загальні тенденції

2024 рік відзначився варіативністю підходів до кібератак як нових, так і відомих хакерських груп. Збільшення кількості інцидентів на 48% порівняно з попереднім півріччям призвело до значного зростання навантаження на роботу команди реагування та підвищення витрат часу на обробку загроз.

Складність атак, які ми розслідували, та рівень чутливості об'єктів, на які вони були спрямовані, залишаються високими. Ворог застосовує дедалі витонченіші методи, комбінуючи різні тактики для досягнення своїх цілей, що ускладнює виявлення та нейтралізацію загроз на ранніх етапах.

У багатьох випадках ми не можемо розкривати важливі деталі щодо постраждалих організацій, виявлених векторів атак та специфіки наших розслідувань. Публічне розголошення цих даних може призвести до адаптації противником своїх методів та ускладнення подальшої роботи з виявлення та запобігання подібним атакам.

Протягом другого півріччя 2024 року було ідентифіковано та проаналізовано близько 70 окремих кампаній, пов'язаних із масовим розповсюдженням шкідливого програмного забезпечення (ШПЗ). Водночас зафіксовано понад 750 звернень від користувачів, які стали мішенню фішингових атак. Однак фактична кількість підтверджених випадків зараження ШПЗ виявилася на 90% меншою. Це свідчить про зростання рівня кібергігієни серед організацій, з якими взаємодіє Держспецзв'язку, покращення механізмів раннього виявлення загроз та ефективну роботу команд з реагування на інциденти.

У другій половині 2024 року зафіксовано значне зростання кібератак, спрямованих на сектор безпеки та оборони, що вказує на критичність використання кіберкомпоненту у ворожих розвідувальних операціях. Основний вектор атак — шпигунство, мета якого полягає у зборі критично важливої інформації, здатної безпосередньо вплинути на оперативну ситуацію в зоні бойових дій.

Зміна тактик

Вже добре відомі нам хакерські угруповання, пов'язані з гу гш зс рф та фсб, зберігають традиційні методи атак. Натомість нові військові кіберпідрозділи демонструють вищий рівень автоматизації, агресивності та масштабу операцій. Російські хакери систематично намагаються порушити роботу об'єктів енергетичного сектору України, координуючи кібератаки із масованими обстрілами енергосистеми.

Крім того, триває системна кампанія російських хакерів проти українського комерційного сектору. Основний вектор — викрадення коштів та поширення ransomware. Масштаби таких атак досягли рекордних показників. Попри серйозність загрози, бізнес-сектор значно менш підготовлений до кібератак, ніж державні установи, та не завжди готовий відкрито ділитися інформаці-

єю про інциденти. Додаткову складність створює низький рівень довіри до державних органів, відповідальних за кібербезпеку, які суттєво підвищили ефективність роботи та якість підходів впродовж трьох попередніх років.

Інцидент із державними реєстрами

Однією з найбільш резонансних атак другої половини 2024 року стала атака у грудні на державні реєстри Міністерства юстиції України. Інцидент призвів до серйозних збоїв у роботі ключових державних сервісів, що призвело до проблем під час перетину кордону та проведення митних операцій. Масштаб наслідків продемонстрував критичну залежність процесів у державних органах від наявної цифрової інфраструктури і потребу перегляду стратегій резервування та підвищення стійкості для всіх організацій державного сектору.

Постійні виклики для критичної інфраструктури

Прямі атаки на об'єкти критичної інфраструктури (ОКІ) стали значно складнішими в реалізації. Зловмисники змушені змінювати тактику та використовувати атаки на ланцюги постачання (supply chain) як основний вектор проникнення. Передусім вони приділяють увагу компрометації постачальників спеціалізованого ПЗ, яке використовується на ОКІ, оскільки такі компанії часто не мають достатнього рівня кіберзахисту, а їхній злам відкриває хакерам нові можливості для подальшого розширення доступу до критичних систем.

Попри суттєві покращення в захисті українських енергетичних компаній та значний досвід реагування на атаки, набутий за останні 11 років, російські APT-групи продовжують діяти, використовуючи знання внутрішньої архітектури українських енергосистем, які вже були атаковані раніше. Оскільки повна перебудова OT-мереж є складним і комплексним завданням, противник здійснює спроби відновити доступ до історично скомпрометованих сегментів інфраструктури, постійно шукаючи нові точки входу. Ці точки завжди існуватимуть через динамічність та складність інфраструктури, що робить ситуацію особливо небезпечною.

Таким чином, атаки на енергетичний сектор трансформувалися у складніші та триваліші операції, реалізація яких може займати 6–8 місяців. Вони вимагають від зловмисників нових підходів до прихованого проникнення, утримання доступу та використання слабких місць у суміжних системах.

Однак, завдяки посиленій співпраці з міжнародними партнерами, розширенню мережі сенсорів моніторингу та покращенню механізмів раннього виявлення загроз, значну частину ворожих операцій вдалося ідентифікувати та нейтралізувати ще до їхньої повної реалізації. Водночас для забезпечення більш ефективного виявлення атак необхідне подальше розгортання додаткових сенсорів та аналітичних систем на об'єктах критичної інфраструктури. За цей період 2024 року ми мали певну кількість таких атак, які відповідно до NIS2 класифікуються як “near missed”, що свідчить про високий рівень загрози та необхідність подальшого зміцнення захисту.

Шпигунство та інформаційні атаки

Тривають як широкомасштабні, так і точкові атаки, спрямовані на окремих людей у Signal, Telegram та WhatsApp, з метою викрадення листування та конфіденційної інформації а також зараження мобільних пристроїв і Windows-систем імплантами для постійного стеження.

Також другу половину 2024 року характеризує зростання кібератак проти об'єктів оборонно-промислового комплексу. Ворог активно використовує всі можливі ресурси для отримання розвідданих, які можуть вплинути на хід бойових дій. Відзначено цілеспрямовані атаки на окремих військових, комп'ютери яких можуть містити інформацію щодо оперативної ситуації на фронті, складу сил і засобів, а також доступ до систем ситуаційної обізнаності. Мали місце атаки на підприємства ВПК, спрямовані на викрадення даних про новітні зразки озброєння та технології захисту, що може бути використано ворогом для розвитку власних систем озброєння.

Вразливості програмного забезпечення

Неоновлене ПЗ та інші грубі помилки системних адміністраторів — залишаються однією з ключових загроз для всіх категорій організацій. Часто тестові сервери та допоміжні системи залишаються поза увагою адміністраторів, що створює потенційні точки компрометації, які використовують зловмисники. Практика свідчить, що хакери максимально оперативно експлуатують незакриті вразливості — буквально впродовж лічених годин після їх публічного розголошення.

Висновки

2024 рік засвідчує зміну підходів у кібервійні з боку росії: підвищення автоматизації атак, фокус на supply chain, розширення масштабів кампаній шпигунства, в тому числі й на комерційний сектор. Збільшення кількості атак потребує більшої координації між державними структурами, приватними компаніями та міжнародними партнерами для забезпечення ефективного реагування та протидії загрозам.

КЕЙСИ

КЕЙСИ

Злам державних реєстрів Мін'юсту

19 грудня хакери атакували реєстри Міністерства юстиції України, фактично зупинивши роботу 14 ключових державних реєстрів.

Кібератака паралізувала значну частину господарської діяльності в країні. Фінансові операції, перевірка контрагентів, державні закупівлі та доступ до важливих державних послуг опинилися під загрозою. Кібератака спричинила масштабні перебої у критично важливих сферах:

- **Перетин кордону.** Збої у реєстрах унеможливили перевірку інформації про заборони на виїзд, що призвело до затримок та відмов у перетині кордону.
- **Розмитнення товарів.** Зупинка доступу до даних про власників юридичних осіб і транспортних засобів паралізувала митні операції, спричинивши затримки вантажів.
- **Нотаріат та операції з майном.** Відсутність доступу нотаріусів та державних реєстраторів до реєстрів нерухомості заблокувала оформлення угод купівлі-продажу, спадкування та інших операцій.
- **Паспортна служба.** Неможливість перевірки персональних даних у реєстрах ускладнила видачу паспортів, id-карток та інших документів.

Цей інцидент продемонстрував критичну залежність процесів у державних і комерційних установах від функціонування реєстрів, що потребує перегляду підходів до резервування та забезпечення безперебійної роботи.

Імплантація на телеком-провайдерах

Ми спостерігаємо продовження кампанії проти телеком-провайдерів через вразливі вебдодатки з подальшим застосуванням шпигунських PAM-модулів POEMGate для збору паролів адміністраторів та всіх інших можливих користувачів.

Імплантація та збір ключів і паролів забезпечує постійну можливість прихованого доступу в мережу телекомунікаційних провайдерів та експлуатації довіри між ними в режимі легітимного користувача без застосування будь-яких засобів, які можуть привернути увагу систем безпеки.

Інфраструктура телекомунікаційних компаній може використовуватися зловмисниками для атак на інші об'єкти, такі як легітимні IP-адреси українського сегменту. Вони привертають меншу увагу SOC-аналітиків та інших кіберфахівців.

Використання вразливостей

Одна з критичних вразливостей програмного забезпечення GeoServer вже через 20 днів з моменту публікації інформації про неї була використана зловмисниками для отримання доступу до ІКС організації, де вони були непоміченими протягом тривалого часу та проводили підготовку до здійснення деструктивної операції.

Загалом фахівці фіксують загальну тенденцію до скорочення часу від розкриття вразливості до перших спроб її експлуатації.

Хронологія від розкриття до експлуатації вразливості

Зазвичай хакерам достатньо 12 годин після публікації інформації про вразливість для виявлення пристроїв, які піддаються експлуатації. А вже за добу вони здійснюють перші спроби її експлуатації. Також приблизно за добу у відкритому доступі публікуються коди для перевірки вразливості (Proof of Concept).

Здебільшого компанії публічно розкривають інформацію про вразливості своїх продуктів разом з оновленням чи патчем, що виправляє її. Саме тому з метою запобігання успішній експлуатації вразливості необхідно своєчасно встановлювати оновлення та застосовувати патчі. Особливо це стосується публічно доступних ресурсів з мережі Інтернет.

Зокрема, протягом другого півріччя 2024 року CERT-UA зафіксувала в різних операціях використання експлойтів для кількох вразливостей, серед них:

- GeoServer — CVE-2024-36401.
- HFS HTTP File Server — CVE-2024-23692.
- Adobe Acrobat Reader — CVE-2023-21608.
- Roundcube — CVE-2023-43770.
- WinRAR — CVE-2023-38831.

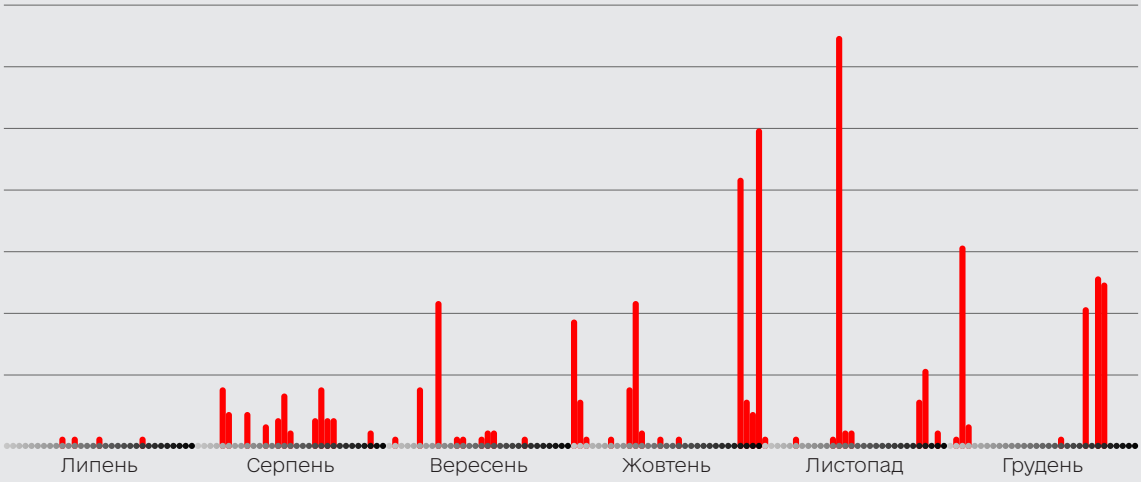
UAC-0050

У другому півріччі 2024 року тактики та техніки угруповання UAC-0050, що спеціалізується на викраденні інформації (кібершпигунстві), дещо зазнали змін. Ключовою відмінністю стало формування додаткових напрямів діяльності, а саме викрадення грошових коштів та проведення інформаційно-психологічних операцій під «брендом» Fire Cells Group.

Однією з нових особливостей стала реалізація паралельних кампаній з розповсюдження ШПЗ, зокрема на легітимних сервісах: Bitbucket, Dropbox, 4Sync, Google Drive та GitHub.

Також можна вважати, що UAC-0050 розширило перелік потенційних «жертв», розсилаючи листи дедалі більшій кількості організацій. На це, ймовірно, вплинула і зміна вектора — від кібершпіонажу до викрадення коштів.

Графік активності кластера кіберзагроз UAC-0050



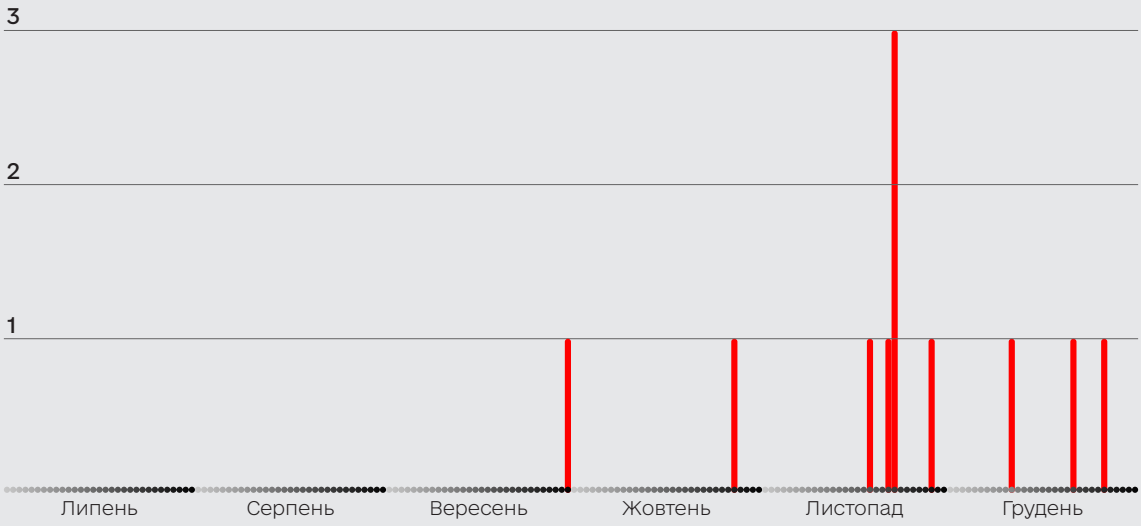
Слід зазначити, що для підвищення рівня довіри зловмисники продовжують, надсилати листи нібито від імені відомих компаній, наприклад, Нової Пошти (https://x.com/NP_official_ua/status/1871897036376748461).

UAC-0099

Активність UAC-0099 здійснюється з метою шпигунства, а перелік об'єктів заінтересованості, як і засоби реалізації зловмисного задуму, змінюються.

У листопаді–грудні 2024 року CERT-UA дослідила низку здійснених угрупованням UAC-0099 кібератак на низку державних організацій, зокрема лісництв, установ судово-медичної експертизи, а також заводів та інших установ.

Графік активності кластера кіберзагроз UAC-0099



Для доставки засобів реалізації кіберзагроз традиційно використовуються електронні листи із вкладеннями у вигляді подвійних архівів з LNK- або HTA-файлами.

У випадку успішної компрометації на ЕОМ здійснюється запуск програми LONEPAGE, яка реалізовує функціонал виконання команд. Разом з тим слід наголосити на змінах у тактиках, техніках і процедурах: якщо раніше LONEPAGE був представлений у вигляді VBS-файлу, що розміщувався в одному з каталогів комп'ютера, то в грудні описаний вище функціонал реалізується двома файлами: зашифрованим (3DES) файлом та .NET програмою, призначенням якої є розшифровка файлу та запуск отриманого PowerShell-коду в пам'яті.

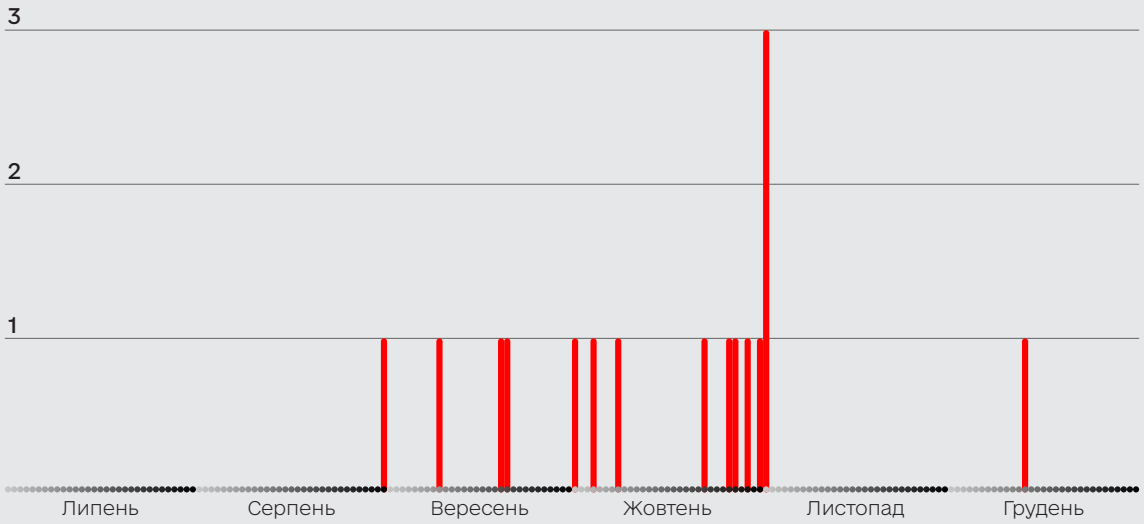
UAC-0001

У другому півріччі основним напрямом діяльності залишалося отримання доступу до поштових скриньок з використанням різноманітних технік.

Для прикладу, продовжувалися постійні фішингові кампанії, спрямовані на викрадення аутентифікаційних даних з поштових скриньок з використанням вкладень у вигляді PDF- або HTML-файлів, вміст яких копіює офіційні сторінки ресурсів ukr.net та містить посилання на фішингову вебсторінку. Проте було зафіксовано кілька кампаній, коли в тілі листа розміщувався QR-код, сканування якого спрямовує користувача на фішингову сторінку. Таким чином, хакери обходять засоби захисту електронної пошти. Незмінним залишається розміщення фішингових сторінок на сервісі Mocky.

У вересні 2024 року CERT-UA було досліджено кібератаку, під час якої зловмисники точково розіслали електронні листи, в яких містився експлойт вразливості Roundcube (CVE-2023-43770). Його успішна експлуатація могла призвести до викрадення аутентифікаційних даних та створення фільтра для переспрямування вмісту поштової скриньки жертви на електронну адресу зловмисника.

Графік активності кластера кіберзагроз UAC-0001



Враховуючи використану вразливість та індикатори кіберзагроз, активність із середнім рівнем впевненості асоційовано з діяльністю угруповання UAC-0001 (APT28).

Також восени в світі почали активно використовувати фейкові сторінки з CAPTCHA для розповсюдження ШПЗ. У жовтні ця схема була виявлена під час кібератаки на український сегмент мережі.

Так, серед органів місцевого самоврядування розповсюджувалися електронні листи з посиланням на сторінку, де відображається вікно, що імітує механізм reCAPTCHA. Дотримання описаних на сторінці інструкцій призводило до виконання PowerShell-команди, яка забезпечує завантаження і запуск шкідливих файлів, основні призначення яких — побудова SSH-тунелю, запуск програмного засобу METASPLOIT, а також викрадення та ексфільтрація аутентифікаційних та інших даних браузерів. Після аналізу використаної мережевої інфраструктури, яка перетинається з інфраструктурою, описаною вище, цю активність із середнім рівнем впевненості ми також асоціюємо з діяльністю UAC-0001.

Як вже згадувалося раніше, протягом цього півріччя ми спостерігаємо тенденцію до зростання кількості кібератак, націлених на сектор безпеки та оборони. На арені з'явилися нові кластери загроз, а ті, що були раніше, продовжують розвиватися та змінювати свої ТТП, саме тому увага в цьому розділі буде зосереджена саме на цій активності.

UAC-0020 (Vermin)

Влітку 2024 року CERT-UA зафіксувала дві цілеспрямовані кібероперації угруповання UAC-0020 (Vermin) на військових з використанням нового інструменту FIRMACHAGENT (CERT-UA#10742), яким керують співробітники силових відомств тимчасово окупованого Луганська.

https://cert.gov.ua/article/6279600

Перша кампанія була описана в звіті за перше півріччя 2024 року.

В обох випадках для збору інформації з інфікованої ЕОМ використано відомий з 2019 року інструментарій — шкідливе програмне забезпечення SPECTR. Для прикладу, ось кілька модулів цього ШПЗ:

https://cert.gov.ua/article/6280422

- **Screengrabber** — забезпечує виготовлення знімків екрана кожні 10 секунд за умови, якщо вікно програми містить такі назви: «word», «excel», «office», «signal», «whatsapp», «discord», «пошта», «диск», «disk», «wallet», «anydesk», «browser», «viewer» тощо.

- **FileGrabber** — забезпечує копіювання файлів з визначених директорій та з визначеними розширеннями в іншу папку.

- **Usb** — має схожий до FileGrabber функціонал, але копіює файли зі знімних (USB) носіїв.
- **Social** — здійснює викрадення конфігураційних (автентифікаційних) даних месенджерів.
- **Browsers** — здійснює викрадення даних (автентифікаційних даних, даних сесій, історії) Інтернет-браузерів.

Обидві атаки, судячи з тематики листів, спрямовані на Сили оборони України. У першому випадку у вкладеннях до листа нібито містились технічні характеристики турелі «Вовчок». У листах з другої кампанії містилося посилання начебто на перелік військовополонених, що вибувають з Курської області.

Для ексфільтрації даних, зібраних за допомогою SPECTR, у цих кампаніях зловмисники використали різні методи. В одному випадку — це легітимна утиліта SyncThing, що призначена для синхронізації файлів між кількома пристроями. За її допомогою синхронізували вміст директорії %APPDATA%\sync\Slave_Sync\, до якої копіювалися викрадені файли, та передавали дані на хост зловмисників. В іншому — нова шкідлива програма FIRMACHAGENT, призначена для вивантаження цієї ж директорії за допомогою протоколу HTTP.

UAC-0180: «поліглоти» атакують оборонні підприємства (CERT-UA#10375)

На початку другого півріччя 2024 року CERT-UA виявила спробу кібератаки угруповання UAC-0180. Хоч активність хакерів цієї групи має широку географію, його учасники не полишають спроб отримання несанкціонованого доступу до ЕОМ співробітників оборонних підприємств та Сил безпеки і оборони України.

https://cert.gov.ua/article/6280099

Слід зазначити про широкий та постійно оновлюваний арсенал шкідливих програм, які вони використовують в своїх кібератаках. Це ШПЗ розроблено з використанням різних мов програмування, включно з: C (ACROBAIT), Rust (ROSEBLOOM, ROSETHORN), Go (GLUEEGG), Lua (DROPCLUE).

Отже, в липні CERT-UA отримала інформацію щодо розповсюдження серед українських оборонних підприємств електронних листів з тематикою закупівлі БпЛА та вкладенням у вигляді ZIP-файлу, що містить PDF-документ з посиланням.

За посиланням завантажується файл «adobe_acrobat_fonts_pack.exe», який є шкідливою програмою GLUEEGG, розробленою з використанням мови програмування Go. Вона призначена для розшифрування та запуску завантажувача DROPCLUE, розробленого з використанням мови програмування Lua.

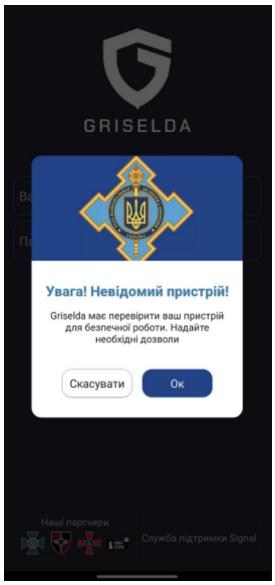
Останній забезпечує завантаження та відкриття документа-приманки «UA-2024-07-04-010019-a-open.pdf», а також EXE-файлу «font-pack-pdf-windows-64-bit». Він запускає BAT-файл, який своєю чергою за допомогою штатної утиліти «curl.exe» здійснить завантаження і встановлення MSI-файлу легітимної програми для віддаленого управління ЕОМ ATERA, що надає хакерам доступ до ЕОМ.

Мобільні імпланти під виглядом «військових» програм

Ведення сучасної війни неможливе без використання сучасних технологій управління боєм, розвідки та ситуаційної обізнаності. При цьому для користування спеціальними військовими системами застосовуються мобільні пристрої. Відтак зловмисники докладають чималих зусиль для компрометації смартфонів та планшетів військовослужбовців з метою викрадення аутентифікаційних даних (які використовуються для доступу до інформаційних систем) та передачі GPS-координат пристроїв, що може мати безпосередні негативні наслідки для життя особового складу.

https://cert.gov.ua/article/6280563

Так, у вересні 2024 року було виявлено кібератаки, пов'язані з розповсюдженням шкідливих програм для мобільних пристроїв, які імітують додатки військових систем GRISELDA (автоматизована система внесення, обробки та передачі інформації з використанням штучного інтелекту) та системи стеження «Очі».



За допомогою месенджера Signal хакери розповсюджували посилання (у випадку з GRISELDA — на копію офіційного вебсайту проєкту, а у випадку з системою «Очі» — на Google Drive), де було розміщено APK-файли.

Слід зауважити, що «мобільної версії» додатка GRISELDA не існує, а на сайті-підробці було розміщене шкідливе програмне забезпечення HYDRA, функціонал якого серед іншого передбачає можливість викрадення даних сесій (HTTP Cookie), контактів, кейлогінг тощо.

Щодо системи «Очі». APK-файл, окрім штатного функціоналу оригінальної програми, містив сторонній код, за допомогою якого здійснювалося викрадення логіна та пароля користувача, а також встановлення та передача GPS-координат пристрою. Ми припускаємо, що зловмисники здійснили модифікацію легітимної програми, додавши сторонній JAVA-клас та реалізувавши його виклик у відповідних блоках коду.

Для відстеження активності, пов'язаної з модифікацією програми «Очі», створено ідентифікатор UAC-0210.

«Запрошення на конференцію» від UAC-0185 (UNC4221) (CERT-UA#12414)

Активність угруповання UAC-0185 (UNC4221) здійснюється щонайменше з 2022 року. Кіберзловмисники спеціалізуються на викраденні облікових даних месенджерів Signal, Telegram, WhatsApp та військових систем DELTA, ТЕНЕТА, «Кропива». Водночас більш обмежено проводяться кібератаки, що мають на меті отримання несанкціонованого віддаленого доступу до ЕОМ співробітників підприємств оборонно-промислового комплексу, а також Сил оборони України з використанням програм для віддаленого управління ЕОМ, зокрема MESHAGENT та ULTRAVNC.

https://cert.gov.ua/article/6281632

У грудні 2024 року хакери здійснили розсилку електронних листів нібито від імені Українського союзу промисловців та підпри-

ємців (УСПП) із запрошенням на конференцію, присвячену тематиці переходу продукції ОПК України на технічні стандарти НАТО, що проводилася у Києві 05.12.2024 у змішаному форматі.

У листі містилося гіперпосилання «Вкладення містить важливу інформацію для вашої участі.», з якого завантажувався файл-ярлик «лист_02-1-437.lnk». Його відкриття призводило до завантаження і запуску за допомогою штатної утиліти mshta.exe файлу «start.hta», що містить JavaScript-код, призначений для запуску двох PowerShell-команд, одна з яких здійснить завантаження і відкриття файлу-приманки у вигляді нібито листа УСПП, а друга — завантаження файлу «Front.png», що є ZIP-архівом, в якому розміщені три файли: «Main.bat», «Registry.hta» та «update.exe», видобування вмісту архіву до каталогу «%LOCALAPPDATA%\Microsoft\EdgeUpdate\Update\» і запуск BAT-файлу «Main.bat».

Останній забезпечить переміщення файлу «Registry.hta» в каталог автозапуску, його виконання, а також видалення з комп'ютера частини завантажених файлів.

Насамкінець «Registry.hta» запустить «update.exe», який класифіковано як програму віддаленого керування MESHAGENT.

Кібератака UAC-0125 з використанням тематики «Армія+»

У серпні 2024 року було запущено додаток «Армія+», призначений для цифровізації документообігу у Збройних Силах України. Хакери не оминули цей додаток. Наприкінці 2024 року CERT-UA отримала інформацію про виявлення низки вебресурсів, які імітують офіційну сторінку додатка «Армія+» та опубліковані за допомогою сервісу Cloudflare Workers.

https://cert.gov.ua/article/6281701

На таких вебсайтах пропонувалося завантажити нібито програму Армія+ для операційної системи Windows. Слід зазначити, що офіційний додаток доступний лише для мобільних пристроїв Android та iOS.

Встановлено, що файл підробленого додатка («ArmyPlusInstaller-v.0.10.23722.exe») є інсталятором, який, окрім .NET файлу-приманки «ArmyPlus.exe», містить файли інтерпретатора Python, архів з файлами програми Tor, а також PowerShell-скрипт «init.ps1».

У випадку відкриття файлу «ArmyPlusInstaller-v.0.10.23722.exe» буде здійснено запуск файлу-приманки, а також PowerShell-скрипта, призначенням якого є:

- встановлення на ЕОМ жертви OpenSSH-сервера;
- генерація пари RSA-ключів;
- додавання публічного ключа до файлу «authorized_keys» для автентифікації;
- надсилання приватного ключа за допомогою «curl» на сервер зловмисників (TOR-адреса);
- публікація прихованого SSH-сервісу за допомогою Tor.

У такий спосіб створюється технічна можливість для віддаленого прихованого доступу до комп'ютера жертви.

Згадана активність відстежується CERT-UA за ідентифікатором UAC-0125 та з достатнім рівнем впевненості асоціюється з кластером UAC-0002 (APT44 aka Sandworm).

ПОПЕРЕДНІ ЗВІТИ

Для розуміння цілісної картини трансформацій у сфері кіберопе-рацій під час повномасштабної війни, ознайомтеся з попередні-ми аналітичними звітами за такими посиланнями:

Англійською

Russia’s Cyber Tactics H2’2022-EN

Russia’s Cyber Tactics H1’2023-EN

Russia’s Cyber Tactics H2’2023-EN

Russia’s Cyber Tactics H1’2024-EN

Українською

Russia’s Cyber Tactics H1’2023-UA

Russia’s Cyber Tactics H2’2023-UA

Russia’s Cyber Tactics H1’2024-UA

Контакт-центр для ЗМІ

press@cip.gov.ua

Залишайтеся на зв'язку

https://x.com/SSSCIP

https://x.com/_CERT_UA

https://www.linkedin.com/company/dsszzi

https://www.linkedin.com/company/cert-ua

https://www.facebook.com/dsszzi

https://www.facebook.com/UACERT

Державна служба спеціального зв'язку
та захисту інформації України

РОСІЙСЬКІ КІБЕРОПЕРАЦІЇ

Аналітика за ІІ півріччя 2024 року